



Jozef Záhora (ed.)

Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní

**TEORETICKÉ A PRAKTICKÉ PROBLÉMY VYUŽÍVANIA
INFORMAČNO-TECHNICKÝCH PROSTRIEDKOV
V TRESTNOM KONANÍ**

Jozef Záhora (ed.)

TEORETICKÉ A PRAKTICKÉ PROBLÉMY VYUŽÍVANIA INFORMAČNO-TECHNICKÝCH PROSTRIEDKOV V TRESTNOM KONANÍ

Zborník príspevkov z vedeckej konferencie
s medzinárodnou účasťou konanej dňa 23. marca 2017

leges

Vzor citácie:

Záhora, J. (ed.): Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní. Praha: Leges, 2017, 288 s.

Zostavil:

prof. JUDr. Jozef Záhora, PhD.

Recenzenti:

doc. JUDr. Dezider Bango, CSc.

doc. JUDr. Marek Fryšták, Ph.D.

Programový výbor:

prof. JUDr. Jaroslav Ivor, DrSc.

prof. JUDr. Jiří Jelínek, CSc.

prof. JUDr. Jozef Záhora, PhD.

doc. JUDr. Peter Polák, PhD.

KATALOGIZACE V KNIZE – NÁRODNÍ KNIHOVNA ČR

Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou konanej dňa 23. marca 2017 / Jozef Záhora (ed.). – Praha : Leges, 2017
ISBN 978-80-7502-206-6

343.13 * 347.94

– trestní řízení

– dokazování (právo)

– informačně-technické prostředky

– sborníky konferencí

343 – Trestní právo [16]

Táto práca bola podporovaná Agentúrou na podporu výskumu a vývoja na základe Zmluvy č. APVV-15-0272.

This work was supported by the Slovak Research and Development Agency under the contract No. APVV-15-0272.



**AGENTÚRA
NA PODPORU
VÝSKUMU A VÝVOJA**

Vydalo Nakladatelství Leges, s. r. o., Lublaňská 4/61, Praha 2,
v roce 2017 jako svou 407. publikaci.

Edice Teoretik

Vydání první

Návrh obálky Michaela Vydrová

Rukopis neprošel jazykovou úpravou. Za odbornou a jazykovou stránku
příspěvků odpovídají autoři.

Sazba Gradis

Tisk powerprint, s. r. o.

www.knihyleges.cz

© Paneurópska vysoká škola n. o., 2017

ISBN 978-80-7502-206-6

Obsah

Obsah	5
Predhovor	9
Program	11
<i>JUDr. Jaroslav Málik, JUDr. Františka Jakubíková</i>	
Niektoré aspekty využívania informačno-technických prostriedkov Policajným zborom pri odhaľovaní a objasňovaní trestnej činnosti	15
<i>JUDr. Miroslava Bálintová</i>	
Zásah do práva na súkromie použitím informačno-technických prostriedkov vo svetle rozhodovacej činnosti Európskeho súdu pre ľudské práva	24
<i>prof. JUDr. Ján Svák, DrSc.</i>	
Ústavné hranice využívania informačno-technických prostriedkov v trestnom konaní	31
<i>prof. JUDr. Jiří Jelínek, CSc.</i>	
Odposlech a záznam telekomunikačného provozu v České republice – záruky přezkoumání zákonnosti příkazu k odposlechu	37
<i>prof. JUDr. Ivan Šimovček, CSc.</i>	
Zákonné limity zabezpečovania informácií dôležitých pre trestné konanie	44
<i>prof. JUDr. Jozef Čentěš, PhD.</i>	
Vývoj právnej úpravy oznámenie údajov o telekomunikačnej prevádzke v trestnom konaní	53
<i>doc. JUDr. Sergej Romža, PhD.</i>	
Príslušnosť súdu na rozhodovanie o použití informačno-technických prostriedkov	62
<i>prof. Ing. Miroslav Lisoň, PhD., JUDr. Michal Marko, PhD.</i>	
Prostriedky operatívnej techniky – kategória kreovanej teórie kriminálno-policajného poznania	69
<i>prof. JUDr. Jaroslav Ivor, DrSc.</i>	
Monitorovanie obydľia kamerovým systémom a jeho využitie pre účely trestného konania	82
<i>doc. JUDr. Alexander Nett, CSc.</i>	
K problematice příkazu ke zjištění údajů o uskutečněném telekomunikačním provozu podle § 88a trestního řádu	91
<i>JUDr. Miroslav Růžička, Ph.D.</i>	
K aplikačním problémům týkajícím se odposlechu, zjišťování údajů z telekomunikačního provozu a sledování osob a věcí v České republice	98
<i>prof. Ing. Vladimír Smejkal, CSc., LL.M, prof. JUDr. Ing. Viktor Porada, DrSc., Dr.h.c.</i>	
Možnosti a limity využitií informačně-technických prostředků při vyšetřování kybernetické kriminality	118

doc. JUDr. Lucia Kurilovská, PhD., Ing. Stanislav Šišulák, PhD.

Použitie inštitútu agenta pri odhaľovaní a objasňovaní kriminality v kybernetickom prostredí	134
---	------------

doc. JUDr. Peter Polák, PhD., JUDr. Marek Talapka

Prípustnosť využitia dôkazov získaných použitím informačno-technických prostriedkov pre účely trestného konania	145
--	------------

JUDr. Jaroslav Rapčan, PhD., JUDr. Adrián Vaško

Informačno-technické prostriedky využívané v účelovo realizovaných procesoch OPC	159
---	------------

PhDr., JUDr. Jozef Medelský, PhD.

Historický exkurz odpočúvania a záznamu telekomunikačnej prevádzky	168
---	------------

JUDr. Marcela Tittlová, PhD.

Teoretické a praktické problémy odpočúvania a záznamu telekomunikačnej prevádzky v trestnom konaní	182
---	------------

JUDr. Miloš Deset, PhD.

Vybrané ústavné a trestno-procesné aspekty vyhotovovania obrazových, zvukových alebo obrazovo-zvukových záznamov	198
---	------------

JUDr. Remig Kubička

Informačno-technické prostriedky v trestnom konaní – analýza niektorých aspektov aktuálnej právnej úpravy s dôrazom na interpretačné problémy	209
--	------------

JUDr. Nina Vančíková

Príkaz na odpočúvanie a záznam telekomunikačnej prevádzky podľa § 115 Trestného poriadku	221
---	------------

JUDr. Juraj Chylo PhD.

Odpočúvanie a záznam telekomunikačnej prevádzky a oznámenie údajov o telekomunikačnej prevádzke	239
--	------------

Mgr. Barbora Tallová

Využitie trestno-procesného inštitútu odpočúvanie a záznam telekomunikačnej prevádzky pri dokazovaní trestnej činnosti právnických osôb	247
--	------------

Mgr. Monika Širilová

Aktuálne problémy vyhotovovania obrazových, zvukových alebo obrazovo-zvukových záznamov v trestnom konaní	261
--	------------

JUDr. Michal Aláč, PhD.

Osobitosti použitia ITP v pôsobnosti Slovenskej informačnej služby	268
---	------------

prof. JUDr. Jozef Záhora, PhD.

Využitie informácií získaných prostredníctvom ITP v „netrestnej veci“	276
--	------------

Contents

Contents	7
Preface	9
Conference Programme	11
<i>JUDr. Jaroslav Málik, JUDr. Františka Jakubíková</i>	
Some Aspects of the Use of Information-technology by Police Force in Detecting and Clarification Crime	15
<i>JUDr. Miroslava Bálintová</i>	
Interference with the Right to Privacy Using Means of Secret Surveillance in the Light of Case-law of the European Court of Human Rights	24
<i>prof. JUDr. Ján Svák, DrSc.</i>	
Constitutional Limits of Using Information-technology in Criminal Proceeding	31
<i>prof. JUDr. Jiří Jelínek, CSc.</i>	
The Interception and Recording of Telecommunications in the Czech republic – the Legal Guarantees of the Reviewing of the Interception Order	37
<i>prof. JUDr. Ivan Šimovček, CSc.</i>	
Legal Limits Provision of Information Relevant to Criminal Proceedings	44
<i>prof. JUDr. Jozef Čentéš, PhD.</i>	
The Legislation Development of Notification the Telecommunications Operation in Criminal Proceedings	53
<i>doc. JUDr. Sergej Romža, PhD.</i>	
Jurisdiction of Courts to Decide Using of Informational-technical Means	62
<i>prof. Ing. Miroslav Lisoň, PhD., JUDr. Michal Marko, PhD.</i>	
Means of the Operative Technology – Category of the Developed theory of Criminal and Police Cognition	69
<i>prof. JUDr. Jaroslav Ivor, DrSc.</i>	
Monitoring of Dwellings by Video Surveillance System and its Use for the Purpose of Criminal Proceeding	82
<i>doc. JUDr. Alexander Nett, CSc.</i>	
Problems of the Order to Ascertain Data on Telecommunication Traffic in Accordance with Section 88a of the Criminal Procedure Code	91
<i>JUDr. Miroslav Růžička, Ph.D.</i>	
Application Problems of Interception of Telecommunications, Ascertain Data on the Telecommunications and Surveillance of Persons and Items in the Czech Republic	98
<i>prof. Ing. Vladimír Smejkal, CSc., LL.M., prof. JUDr. Ing. Viktor Porada, DrSc., Dr.h.c.</i>	
Possibilities and Limits of Using Information-technical Means in the Investigation of Cyber Crime	118

<i>doc. JUDr. Lucia Kurilovská, PhD., Ing. Stanislav Šišulák, PhD.</i> The use of Agent's Institute in Crime Detection and Investigation in Cyber Environment	134
<i>doc. JUDr. Peter Polák, PhD., JUDr. Marek Talapka</i> Admissibility of Evidence Obtained by the Use of Information Technology for the Purposes of Criminal Proceeding	145
<i>JUDr. Jaroslav Rapčan, PhD., JUDr. Adrián Vaško</i> Information and Technical Means Used in Purpose Oriented Processes of Operative and Search Activity	159
<i>PhDr. JUDr. Jozef Medelský, PhD.</i> Historical Review of the Legislation of the Eavesdrop and Telecommunication Recording	168
<i>JUDr. Marcela Tittlová, PhD.</i> Theoretical and Practical Problems of Interception and Recording of Telecommunications in Criminal Proceedings	182
<i>JUDr. Miloš Deset, PhD.</i> Selective Constitutional and Criminal Procedural Aspects of Getting the Video, Audio or Video-audio Records	198
<i>JUDr. Remig Kubička</i> Information Technical Means in Criminal Proceedings – an Analysis of Some Aspects of Current Legislation with an Emphasis on Interpretation Problems	209
<i>JUDr. Nina Vančíková</i> Order on the Interception and Recording of the Communications Pursuant to Section 115 of the Code of Criminal Procedure	221
<i>JUDr. Juraj Chylo PhD.</i> Interception and Recording of Telecommunications and Notification of Communication Data	239
<i>Mgr. Barbora Tallová</i> The Use of Wiretapping and Recording Telecommunications in Proving the Crime of Legal Entities	247
<i>Mgr. Monika Širilová</i> Actual Problems of Making Video, Audio or Video-audio Recordings in Criminal Proceedings	261
<i>JUDr. Michal Aláč, PhD.</i> Particularities of Use Information Technical Means within the Scope of the Slovak Intelligence Service	268
<i>prof. JUDr. Jozef Záhora, PhD.</i> Using of Information Obtained by Technical Means in a “Non-criminal Case”	276

Predhovor

Preface

Informačno-technické prostriedky (ďalej len „ITP“) je možné charakterizovať ako osobité, špecifické, ofenzívne a spravodajským spôsobom vykonávané trestno-procesné inštitúty, ktoré majú v trestnom konaní povahu dôkazných prostriedkov. Ich použitím, pri dodržaní všetkých zákonných podmienok, na ktoré sa ich použitie viaže, je možné získať informácie, ktoré môžu byť dôkazom v trestnom konaní. Dôležitosť týchto trestno-procesných inštitútov je potrebné vidieť aj v tom, že mnohé z relevantných druhov trestnej činnosti nie je možné odhaliť, dokázať a ich páchatelov usvedčiť iným spôsobom, než za pomoci ich využitia. Práve spravodajský, teda utajený spôsob ich využitia, smeruje k tomu, že sa v trestnom konaní získajú také informácie, ktoré budú vykazovať určitý stupeň vierohodnosti, určitý stupeň objektívnosti.

Záujem na riešení a celkovo kontrole relevantných druhov kriminality viedol k tomu, že do určitej miery sa obetujú niektoré základné ľudské práva a teda povoľujú sa zásahy do týchto ľudských práv s ohľadom na potrebu odhalenia relevantných trestných činov a zistenia ich páchatelov. Všeobecne je pre ITP charakteristické, že do oblasti základných ľudských práv zasahujú pomerne intenzívne. Je možné spomenúť nielen právo na súkromie, ale aj právo na rodinný život, právo na ochranu tajomstva prepravovaných správ, právo na ochranu obydlia.

Určenie miery, do ktorej je ešte možné zasahovať do týchto ľudských práv s ohľadom na právo i povinnosť štátu stíhať trestné činy a týmto spôsobom chrániť spoločnosť a jej členov, je značne problematické. V každom prípade podlieha hodnoteniu z hľadiska viacerých kritérií, okrem iného aj z hľadiska proporcionality tohto zásahu. V mnohých prípadoch sa však obvinení či obžalovaní z tých najzávažnejších trestných činov, v súvislosti s odhaľovaním a dokazovaním ktorých sa využívajú ITP, dovoľávajú ochrany svojich dotknutých práv a to práve s ohľadom na zákonnosť využitia týchto prostriedkov, nutnosť, resp. nevyhnutnosť ich použitia a už vyššie spomenutú proporcionalitu resp. legitimitu ich použitia vo vzťahu k predmetnému zásahu.

Právna úprava ITP, ich použitie v trestnom konaní a viaceré aplikačné problémy predstavujú veľmi aktuálnu otázku. O aktuálnu otázku ide práve s ohľadom na problematiku ich využívania na podklade nedôslednej a nesystematickej právnej úpravy (trestno-procesnej i mimo-procesnej), čo vedie ku komplikáciám v súvislosti s odhaľovaním a dokazovaním trestnej činnosti. Trestno-procesná úprava vykazuje viaceré nedostatky, ktoré komplikujú proces odhaľovania i dokazovania trestnej činnosti prostredníctvom týchto ITP.

Vzhľadom na uvedené a skutočnosť, že problematika odhaľovania a dokazovania trestnej činnosti prostredníctvom ITP nie je dostatočne teoreticky spracovaná, riešiteľský kolektív Fakulty práva Paneurópskej vysokej školy sa podujal spracovať výskumnú úlohu *„Zvyšovanie efektívnosti odhaľovania a dokazovania trestnej činnosti prostredníctvom informačno-technických prostriedkov“*, ktorá po príslušnom hodnotiacom procese bola podporená Agentúrou na podporu výskumu a vývoja na základe zmluvy č. APVV-15-0272. Konferencia si kladie za cieľ vytvoriť priestor na vedeckú rozpravu o aktuálnych problémoch využívania ITP v trestnom konaní a pri pokúsiť sa identifikovať relevantné teoretické a aplikačné problémy.

Sme radi, že na konferencii okrem záujemcov z akademického prostredia z právnických fakúlt a ďalších vysokých škôl zo Slovenska a Českej republiky, participujú aj účastníci z Kancelárie zástupcu Slovenskej republiky pred Európskym súdom pre ľudské práva, Najvyššieho súdu

Českej republiky, Najvyššieho štátneho zastupiteľstva Českej republiky, Spoločnosti pre trestné právo a kriminológiu, ale aj ďalší odborníci z radov sudcov, prokurátorov, polície a advokátov.

Preto veríme, že cieľ konferencie sa podarilo naplniť, bolo identifikovaných viacero teoretických a praktických problémov, ktorým bude v rámci ďalšieho riešenia venovaná náležitá pozornosť. S týmito výsledkami budú riešitelia vedeckovýskumného projektu pracovať, postupne sa budú snažiť prinášať riešenia a v spolupráci s príslušnými orgánmi ich implementovať do praxe.

Program

Conference Programme

celoštátnej konferencie s medzinárodnou účasťou „Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní“

organizovanej v rámci riešenia vedecko-výskumnej úlohy „Zvyšovanie efektívnosti odhaľovania a dokazovania trestných činov prostredníctvom informačno-technických prostriedkov“ podporovanej APVV na základe zmluvy č. APVV-15-0272.

23. marca 2017, miestnosť Aula Maxima, Tomášikova 20, 821 02 Bratislava

08 ³⁰ –09 ⁰⁰ h	prezentácia účastníkov	
09 ⁰⁰ –09 ¹⁰ h	otvorenie konferencie	
Blok I. 09 ³⁰ –11 ⁰⁰ hod.	plk. JUDr. Jaroslav Málik 1. viceprezident Policajného zboru	Niektoré aspekty využívania informačno-technických prostriedkov Policajným zborom pri odhaľovaní a objasňovaní trestnej činnosti
	JUDr. Miroslava Bálintová spoluzástupkyňa SR pred ESEP	Zásah do práva na súkromie použitím ITP vo svetle rozhodovacej činnosti ESEP
	prof. JUDr. Ján Svák, DrSc. Fakulta práva PEVŠ Bratislava	Ústavné hranice využívania informačno-technických prostriedkov v trestnom konaní
	prof. JUDr. Jiří Jelínek, CSc. Právnická fakulta UK Praha	Odposlech a záznam telekomunikačného provozu v České republice – záruky přezkoumání zákonnosti příkazu k odposlechu
	prof. JUDr. Ivan Šimovček, CSc. Právnická fakulta Trnavskej univerzity	Zákonné limity zabezpečovania informácií dôležitých pre trestné konanie
	prof. JUDr. Jozef Čentěš, PhD. Právnická fakulta UK Bratislava	Vývoj právnej úpravy oznámenia údajov o telekomunikačnej prevádzke v trestnom konaní
	doc. JUDr. Sergej Romža, PhD. Právnická fakulta UPJŠ, Košice	Príslušnosť súdu na rozhodovanie o použití ITP
	prof. Ing. Miroslav Lisoň, PhD. Akadémie Policajného zboru	Prostriedky operatívnej techniky – kategória kreovanej teórie kriminálno-policajného poznania
	Diskusia	
11 ⁰⁰ –11 ²⁰ h	Coffee break	

Blok II. 11²⁰–13⁰⁰ hod.	<i>prof. JUDr. Jaroslav Ivor, DrSc.</i> Fakulta práva PEVŠ Bratislava	Monitorovanie obydla kamerovým systémom a jeho využitie pre účely trestného konania
	<i>doc. JUDr. Alexander Nett, CSc.,</i> Právnická fakulta UP Olomouc	K problematice příkazu ke zjištění údajů o uskutečněném telekomunikačním provozu podle § 88a tr. ř.
	<i>JUDr. Miroslav Růžička, Ph.D.</i> Nejvyšší státní zastupitelství ČR	K aplikačním problémům týkajícím se odposlechu, zjišťování údajů z telekomunikačního provozu a sledování osob a věcí v České republice
	<i>prof. Ing. Vladimír Smejkal, CSc., LL.M.,</i> Moravská vysoká škola Olomouc, <i>prof. JUDr. Ing. Viktor Porada, DrSc.,</i> <i>Dr.h.c.,</i> Vysoká škola finanční a správní	Možnosti a limity využitia informačno-technických prostriedkov pri vyšetrovaní kybernetickej kriminality
	<i>doc. JUDr. Lucia Kurilovská, PhD.,</i> <i>plk. Ing. Stanislav Šišulák, PhD.,</i> Akadémia PZ v Bratislave	Inštitút agenta pri odhaľovaní kriminality v kybernetickom priestore
	<i>doc. JUDr. Peter Polák, PhD.,</i> <i>JUDr. Marek Talapka</i> Fakulta práva PEVŠ Bratislava	Prípustnosť využitia dôkazov získaných použitím informačno-technických prostriedkov pre trestné konanie
	<i>JUDr. Peter Šamko</i> Krajský súd v Bratislava	Súkromné nahrávky iných osôb získané utajeným spôsobom a možnosti ich využitia v trestnom konaní
	<i>JUDr. Jaroslav Rapčan, PhD.,</i> <i>JUDr. Adrián Vaško</i> Akadémia PZ v Bratislave	Informačno-technické prostriedky využívané v účelovo realizovaných procesoch OPČ
	Diskusia	
13¹⁰–14¹⁰ h	Obed	

Blok III. 14²⁰ – 16⁰⁰ hod.	<i>PhDr. JUDr. Jozef Medelský, PhD.</i> Akadémia PZ v Bratislave	Historický exkurzus odpočúvania a záznamu telekomunikačnej prevádzky
	<i>JUDr. Marcela Tittlová, PhD.</i> Fakulta práva PEVŠ Bratislava	Teoretické a aplikačné problémy odpočúvania
	<i>JUDr. Miloš Deset, PhD.</i> Právnická fakulta, Trnavskej univerzity	Vybrané ústavné a trestno-procesné aspekty vyhotovovania obrazových, zvukových alebo obrazovo-zvukových záznamov v trestnom konaní
	<i>JUDr. Remig Kubička</i> Okresná prokuratúra Bratislava IV.	Informačno-technické prostriedky v trestnom konaní – analýza niektorých aspektov aktuálnej právnej úpravy s dôrazom na interpretačné problémy
	<i>JUDr. Nina Vančíková</i> Fakulta práva PEVŠ Bratislava	Príkaz na odpočúvanie a záznam telekomunikačnej prevádzky
	<i>JUDr. Juraj Chylo PhD.</i> Okresná prokuratúra Bratislava II	Odpočúvanie a záznam telekomunikačnej prevádzky a oznámenie údajov o telekomunikačnej prevádzke
	<i>Mgr. Barbora Tallová</i> Fakulta práva PEVŠ Bratislava	Využitie trestno-procesného inštitútu odpočúvanie a záznam telekomunikačnej prevádzky pri dokazovaní trestnej činnosti právnických osôb
	<i>Mgr. Monika Širilová</i> Fakulta práva PEVŠ Bratislava	Aktuálne problémy vyhotovovania obrazových, zvukových alebo obrazovo-zvukových záznamov v trestnom konaní
	<i>JUDr. Ing. Henrich Gaulieder</i> Fakulta práva PEVŠ Bratislava	Preskúmanie zákonnosti príkazu na odpočúvanie a záznam telekomunikačnej prevádzky ako nový inštitút v trestnom procese
	<i>JUDr. Michal Aláč, PhD.</i> Právnická fakulta, Trnavskej univerzity	Osobitosti použitia ITP v pôsobnosti Slovenskej informačnej služby
	<i>prof. JUDr. Jozef Záhora, PhD.</i> Fakulta práva PEVŠ Bratislava	Využitie informácií získaných prostredníctvom ITP v „netrestnej veci“
	Diskusia	
16⁰⁰ h	Záver konferencie	

Niektoré aspekty využívania informačno-technických prostriedkov Policajným zborom pri odhaľovaní a objasňovaní trestnej činnosti

Some Aspects of the Use of Information-technology by Police Force in Detecting and Clarification crime

Jaroslav Málík¹

Františka Jakubíková²

Abstrakt: Predkladaný článok poukazuje na aplikačné problémy spravidla praktického charakteru, s ktorými sa príslušníci Policajného zboru stretávajú v súvislosti s odhaľovaním a objasňovaním najzávažnejších trestných činov využitím informačno-technických prostriedkov ako moderných a ofenzívnych prostriedkov odhaľovania a objasňovania najzávažnejších trestných činov. Keďže ide o tak invazívny prostriedok získavania informácií a v určitom prípade aj zaškoľovania vecí dôležitých pre trestné konanie, článok na úvod predstavuje ústredné základné právo, ktoré je jeho využitím narušené, vrátane jeho právnej úpravy s dôrazom na rozmer poskytovaný Dohovorom o ochrane ľudských práv a základných slobôd, ďalej analyzuje zakotvenie tohto inštitútu v zákone č. 301/2005 Z. z. Trestný poriadok ako aj zákone č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním), ktoré stručne komparuje a napokon vzhľadom na citlivosť tejto témy poskytuje aj strohý náčrt zásadných aplikačných problémov praktického charakteru, ktoré zainteresovaným útvarom Policajného zboru v súvislosti s týmto inštitútom vzniknú.

Abstract: The article illustrates practical problems with application which the policemen are meeting with according to detection, clarification and investigation of most serious crimes using information technology means as modern and offensive means of detection and clarification of most serious crimes. As regards the fact that information technology means represent such invasive means of reaching new information, in the beginning the article describes elemental basic right which is by their usage violated, including its legislation emphasizing the side given by European Convention on the Protection of Human Rights and Fundamental Freedoms, then it analysis and shortly compares Code of criminal procedure and Act. No. 166/2003 Coll. about protection of privacy before interception and in the end as regards the sensitivity of these questions the article offers short illustration of main practical problems of their application which the interested police units deal with.

Kľúčové slová: právo na súkromie, informačno-technické prostriedky, odhaľovanie, objasňovanie.

Key words: information technology means, creating of video, audio or audio-visual recordings, right to privacy.

V dnešnej postmodernej dobe intenzívne rastie význam informačných technológií. Informatizácia spoločnosti a s tým spojená informačná moc sa stávajú zbraňou v rukách jednotlivcov, dokonca účinnejšou než sú zbrane konvenčné, ktorá postupne ohrozuje základné ľudské práva a slobody. Záleží preto na tom, aby zmienené prostriedky mali správnych držiteľov, slúžili ušľachtilým cieľom a boli vždy pod nezávislou verejnou kontrolou.

¹ Plk. JUDr. Jaroslav Málík, 1. viceprezident Policajného zboru, Prezídium Policajného zboru, Pribinova 2, 812 72 Bratislava.

² Kpt. JUDr. Františka Jakubíková, Prezídium Policajného zboru, Pribinova 2, 812 72 Bratislava.

Stav a povaha súčasnej kriminality, najmä pokiaľ ide o jej vysoko organizované a utajované formy, jednoznačne poukazujú na skutočnosť, že odhaľovanie, objasňovanie a vyšetrovanie týchto najzávažnejších trestných činov a samozrejme aj ich efektívna kontrola či prevencia ich ďalšieho výskytu sú v súčasnej a budúcej spoločnosti nerozlučne spojené s využívaním moderných, ofenzívnych a svojou povahou aj do základných ľudských práv a slobôd silne zasahujúcich inštitútov.

Keďže základom úspešného odhalenia, objasnenia trestného činu a zistenia jeho páchatela sú v prvom rade informácie, je zrejmé, že v tomto prípade ide o inštitúty, ktorých elementárnym cieľom je práve zabezpečiť informácie. Za takéto považujeme aj informačno-technické prostriedky (ďalej len „ITP“), ktoré sú charakteristické silným stretom so súkromím jednotlivca spolu s jeho všetkými zložkami (domová sloboda či tajomstvo prepravovaných správ a ochrana osobných údajov).

S ohľadom na stret ITP so základnými ľudskými právami a slobodami a hlavne teda s už zmieneným právom na súkromie, je potrebné, aby trestno-právne úpravy právneho štátu veľmi dôsledne vymedzovali podmienky, za ktorých splnenia je možné takéto prostriedky v konkrétnych prípadoch a voči určitým osobám využiť a zároveň pravidlá, za ktorých by sa takéto zásahy zákonne realizovali.

Na jednej strane sa pomocou nich stanovujú garancie pred svojvoľným využívaním prostriedkov či využívaním na základe neodôvodnených podnetov a informácií a na strane druhej sa tak vytvára určitá hranica medzi zásahmi do práva na súkromie, ktoré sú ešte považované za prípustné a tými, ktoré naopak už prípustnými nie sú.

Na úvod je nutné zdôrazniť, že základným predpokladom fungovania každého demokratického štátu je vzťah medzi štátnou mocou a občanom, v rámci ktorého je zabezpečená ochrana občana pred štátnou mocou a jej podriadenie zákonu. Základné práva a slobody môžu byť obmedzené len zo zákonom presne vymedzených dôvodov a v nevyhnutnej miere a ochrana je možná len do tej miery, kým chránené právo či sloboda nie je obmedzené druhým právom či slobodou.

Na tomto mieste si dovoľíme krátko predstaviť legislatívny rámec tak nevyhnutného ľudského práva v demokratickej spoločnosti, akým právo na súkromie určite je. Začnime základným zákonom štátu, a síce zákonom č. 460/1992 Zb. Ústava Slovenskej republiky (ďalej len „Ústava SR“), ktorý sa na úpravu základných práv a slobôd sústreďuje hneď vo svojej druhej hlave, pričom konkrétne právo na nedotknuteľnosť osoby a jej súkromia je obsiahnuté v jej druhom oddieli v článku 16 ods. 1 ako základné ľudské právo.

Podľa článku 16 ods. 1 Ústavy SR, cit.: *„Nedotknuteľnosť osoby a jej súkromia je zaručená. Obmedzená môže byť len v prípadoch ustanovených zákonom“*.

Ústava prevzala ochranu súkromia v takej podobe ako ju poznala a zakotvila Listina základných práv a slobôd. V tejto súvislosti je samozrejme nutné pripomenúť, že právo na súkromie nemožno vnímať len ohraničene z pohľadu jednotlivého ustanovenia Ústavy SR ale aj s prihliadnutím na ďalšie články tohto základného zákona štátu, kam boli práve zložky práva na súkromie upravené v Listine základných práv a slobôd inkorporované (napr. článok 19, článok 21 či článok 22 Ústavy SR). Ústava SR tak v štyroch článkoch poskytuje ochranu, ktorú zaručujú medzinárodné dohovory na danú tému jedným ustanovením. Niektorí teoretici preto konštatujú zbytočnú rozkúskovanosť ochrany práva na súkromie, ktorá môže spôsobiť problémy s ich výkladom a samozrejme praktickým využitím.

V súčasnej dobe sa však od doslovného výklad článku 16 a článku 19 Ústavy SR upúšťa a vychádza sa z myšlienky, že cit.: *„...čl. 16 ods. 1 a čl. 19 ods. 2 chránia hodnoty súkromnoprávnej povahy v jedinom a jednotnom systéme vytvorenom podľa požiadavky kompatibility s ochranou*

ľudského práva na súkromie“ (Drgonec, 2012, s. 329). „Systematika ústavy nie je taká, aby sa nevyhnutne interpretovala tak, že každým jej ustanovením sa osobe priznáva osobitné právo alebo sloboda“ (Nález Ústavného súdu Slovenskej republiky, PL. ÚS 43/95). „Ústavou vytvorená ochrana práva na súkromie sa vnútorne diferencuje. Jednotlivými ustanoveniami sa zaručuje ochrana súkromia v rôznych životných situáciách“ (Nález Ústavného súdu Slovenskej republiky, I. ÚS 13/00).

Právo na súkromie je plodom anglo-amerického právneho systému.³ Je faktom, že ústavy tzv. vyspelých západných krajín Európy ho v polovici minulého storočia ešte nepoznali. V americkej právnej teórii je právo na súkromie vnímané ako „...antitotalitné právo, teda ... základné právo, ktoré má chrániť jednotlivca pred jeho nadmerným formovaním zo strany spoločnosti“ (Drgonec, 2012, s. 326). Práve tento antitotalitný rozmer sa prejavil najmä v súvislosti s jeho významom po politických zmenách v roku 1989.

Z pohľadu medzinárodnoprávného zakotvenia práva na súkromie, ktoré je vychádzajúc z Ústavy SR súčasťou slovenského právneho poriadku, hovoríme v prvom rade o Všeobecnej deklarácii ľudských práv, kde je uvedené právo zmieňované v jej článku 12, ďalej o článku 8 Dohovoru o ochrane ľudských práv a základných slobôd či o článku 17 Medzinárodného paktu o občian-ských a politických právach.

Ústava SR vo svojom článku 16 ods. 1 teda konštatuje, že nedotknuteľnosť osoby a jej súkromia môže byť obmedzená, ale len v prípadoch ustanovených zákonom. Dohovor o ochrane ľudských práv a základných slobôd zase vo svojom článku 8 uvádza tri podmienky, ktoré musia byť v prípade obmedzenia práva na súkromie naplnené. Vymedzuje, že v prvom rade musí ísť o súlad so zákonom, ďalej, že takýto krok je nevyhnutný v demokratickej spoločnosti a zároveň musí ísť o ochranu jedného z taxatívne vymedzených záujmov – „...národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom a zločinnosti, ochrany zdravia alebo morálky alebo ochrany práv a slobôd iných“ (článok 8 ods. 2 Dohovoru o ochrane ľudských práv a základných slobôd). Základným účelom daného ustanovenia je ochrana jednotlivcovho práva na súkromný a rodinný život pred svojvoľným zásahom verejnej moci, pričom chráni viacero oblastí – „... súkromie telefonických rozhovorov, zhromaždené a uschované informácie osobnej povahy, intímny život, atď.“ (Drgonec, 2012, s. 318). Európsky súd pre ľudské práva sa otázkou práva na súkromie zaoberal v množstve rôznych prípadov, no napokon ho ne-definoval, cit.: „Súd nepokladá za možné ani nutné pokúsiť sa o vyčerpávajúcu definíciu pojmu“.

Keďže za splnenia zákonom predpokladaných podmienok sú v týchto prípadoch dovolené určité zásahy, nejde o práva absolútne. S ohľadom na trestno-právny kontext sú zásahy do základných ľudských práv a slobôd možné iba v takých prípadoch a v takom rozsahu, aký je nevyhnutný na účely odhaľovania a dokazovania konkrétnych trestných činov.

Na tomto mieste treba pripomenúť základné zásady trestného konania ako nosné piliere celého trestného procesu a jeho organizácie. Spomedzi všetkých má v tejto súvislosti najväčší význam zásada primeranosti a zdržanlivosti⁴ upravená v § 2 ods. 2 zákona č. 301/2005 Z. z. Trestný poriadok (ďalej len „Trestný poriadok“), ktorá spočíva v tom, že síce „...trestné právo procesné umožňuje zásahy do nich [rozumej – základné práva a slobody]...“ (Čentíš a kol., 2014, s. 4), ale tieto musia byť uskutočňované len v takom rozsahu „...v akom to odôvodňuje účel trestného konania“ (Čentíš, 2014, s. 4). Zásada je „...prejavom nového, humánnejšieho ponímania trestného

³ Vzniklo v Spojených štátoch amerických na prelome 19. a 20. storočia a bolo odvodené od ústavného práva na riadny súdny proces.

⁴ Podľa § 2 ods. 2 Trestného poriadku cit.: „Do základných práv a slobôd osôb v prípadoch dovolených zákonom možno zasahovať len v miere nevyhnutnej na dosiahnutie účelu trestného konania, pričom treba rešpektovať dôstojnosť osôb a ich súkromie.“

procesu“ (Ivor a kol., 2006, s. 59) a väčšinou teoretikov je radená medzi všeobecné zásady trestného konania, pričom sa vzťahuje na všetkých zúčastnených na procesných úkonoch. Trestný poriadok ďalej v § 55 čiastočne rozoberá jej obsah, podľa ktorého orgány činné v trestnom konaní, súd ako aj ďalšie osoby príslušné vykonávať úkony trestného konania musia pri ich výkone so zúčastnenými zaobchádzať v súlade s účelom trestného konania, pričom vždy musia rešpektovať ich dôstojnosť a ústavou zaručené základné práva a slobody.

Európsky súd pre ľudské práva k použitiu informačno-technických prostriedkov skonštatoval, že tieto sú zo strany štátu tolerovateľné len v prípade, ak sú nevyhnutné pre ochranu demokratických inštitúcií. Dôležitými sú dva momenty, a síce vývoj techniky v oblasti špionáže a následne kontrašpionáže a súčasne rozmach terorizmu, tieto v podstate „nútiť“ štát z dôvodu vzniknutej hrozby kontrolovať jednotlivcov utajeným spôsobom. V demokratickom štáte je potrebné vytvoriť priestor pre aplikáciu tajného dohľadu za istých výnimočných podmienok (Drgonec, 2012). Podľa Európskeho súdu pre ľudské práva akékoľvek zásahy do súkromného života či korešpondencie (ako napríklad odpočúvanie či iné formy sledovania telefonických rozhovorov) sú závažnými zásahmi a musia prebiehať podľa presnej úpravy. Vnútroštátne právo je zákonite povinné poskytnúť dostatočnú ochranu jednotlivcovi pred svojvoľnými zásahmi do jeho práva na súkromie, a teda presne vymedziť, kedy k nemu môže dôjsť. Z judikatúry súdu vyplýva, že nedostatočná domáca právna úprava bola v mnohých prípadoch dôvodom, pre ktorý súd vyslovil nesúlad s Dohovorom (napr. Kopp vs. Švajčiarsko, Cosme Valenzuela Contreras vs. Španielske kráľovstvo, atď.).

Po návrate k vnútroštátnej právnej úprave je nutné uviesť, že k použitiu ITP môže dôjsť len na základe dvoch právnych predpisov, a to zákona č. 301/2005 Z. z. Trestný poriadok (ďalej len „Trestný poriadok“) a zákona č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) (ďalej len „zákon o ochrane pred odpočúvaním“) samozrejme formou realizácie oprávnenia príslušníka Policajného zboru vymedzeného v § 36 zákona č. 171/1993 Z. z. o Policajnom zbore.

Na doplnenie prameňov práva pri úprave ITP je potrebné uviesť, že konkrétny mechanizmus realizácie informačno-technických úkonov prostredníctvom ITP vzhľadom na strohú právnu úpravu obsiahnutú vo vyššie uvedených zákonoch obsahuje nariadenie ministra vnútra Slovenskej republiky č. 30/2012 o používaní informačno-technických prostriedkov. Toto však práve z dôvodu citlivosti samotného konania a utajovaného spôsobu výkonu informačno-technických úkonov podlieha stupňu utajenia, a preto sa ním ďalej zaoberať nebudeme.

Úprava ITP obsiahnutá v Trestnom poriadku sa vzťahuje na realizáciu informačno-technických úkonov počas celého trestného konania, avšak z praktického pohľadu výkonných zložiek Policajného zboru sa zriedkavo využíva v postupe pred začatím trestného stíhania. Práve pre túto úvodnú etapu ako teda časť „policajného“ odhaľovania a objasňovania trestnej činnosti je typická ich realizácia na základe zákona o ochrane pred odpočúvaním.

Podľa § 10 ods. 21 Trestného poriadku sa ITP rozumejú „...elektrotechnické, rádiatechnické, fototechnické, optické, mechanické, chemické a iné technické prostriedky a zariadenia alebo ich súbory použité utajovaným spôsobom pri odpočúvaní a zázname prevádzky v elektronických komunikačných sieťach (ďalej len „odpočúvanie a záznam telekomunikačnej prevádzky“), obrazových, zvukových alebo obrazovo-zvukových záznamov alebo pri vyhľadávaní, otváraní a skúmaní zásiek, ak sa ich použitím zasahuje do základných ľudských práv a slobôd.“

Na spracúvanie takto získaných informácií, ich evidenciu, dokumentáciu a ukladanie sa vzťahujú osobitné predpisy, pričom prevádzkovatelia verejných telefónnych sietí, poskytovatelia elektronických telekomunikačných sietí, elektronických telekomunikačných služieb, poštových

podnik, dopravcovia a iní zasielateľia a ich zamestnanci sú povinní pri ich použití poskytnúť nevyhnutnú súčinnosť informačno-technických prostriedkov a zároveň sa nemôžu dovolávať povinnosti mlčanlivosti podľa osobitných zákonov.

Medzi ITP v zmysle Trestného poriadku zahŕňame tri inštitúty:

- vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov podľa § 114 Trestného poriadku,
- odpočúvanie a záznam telekomunikačnej prevádzky podľa § 115 Trestného poriadku a napokon
- zadržanie podľa § 108 Trestného poriadku a otvorenie zásielok podľa § 109 Trestného poriadku (Čentéš a kol., 2014).

Ďalším zákonným prameňom práva v tomto prípade je zákon o ochrane pred odpočúvaním, v ktorom je upravená aj ich hmotnoprávna stránka.

§ 2 ods. 1 zákona o ochrane pred odpočúvaním obsahuje definíciu ITP, ktorá po poslednej novele uvádza, že tieto predstavujú najmä elektrotechnické, rádiotechnické, fototechnické, optické, mechanické, chemické a iné prostriedky a zariadenia alebo ich súbory používané utajovaným spôsobom pri vyhľadávaní, otváraní, skúmaní a vyhodnocovaní poštových zásielok a iných dopravovaných zásielok, ďalej získavaní obsahu správ prenášaných prostredníctvom elektronických komunikačných sietí, vrátane odpočúvania telefónnej komunikácie a napokon pri vyhotovovaní obrazových, zvukových, obrazovo-zvukových alebo iných záznamov.

Zákon sa rovnako vyjadruje k subjektom, ktoré takéto prostriedky môžu používať, cit. „...Policajný zbor, Slovenská informačná služba, Vojenské spravodajstvo, Zbor väzenskej a justičnej stráže a Colná správa ... v rozsahu podľa osobitných predpisov“ (§ 2 ods. 2 zákona o ochrane pred odpočúvaním). Zakazuje sa ich použitie nepovolánymi – orgány územnej samosprávy, súkromnými bezpečnostnými službami, inými fyzickými alebo právnickými osobami.

Podmienkou pre využitie informácií získaných použitím ITP ako dôkazu v trestnom konaní je podľa tohto zákona vyhotovenie písomného záznamu s uvedením údajov o mieste, čase a zákonnosti použitia ITP, ku ktorému orgán štátu priloží záznam a jeho doslovný prepis.

§ 3 ods. 1 zákona vymedzuje účel použitia ITP, cit.: „*Informačno-technický prostriedok možno použiť len vtedy, ak je to v demokratickej spoločnosti nevyhnutné na zabezpečenie ochrany ústavného zriadenia, vnútorného poriadku a zahraničnopolitických záujmov štátu, bezpečnosti a obrany štátu, získavanie informácií zo zahraničných zdrojov, predchádzanie a objasňovanie trestnej činnosti alebo na ochranu práv a slobôd iných...*“.

Definícia ITP v § 2 zákona je výsledkom už zmieňovanej poslednej novely účinnej od 1. 1. 2016, ktorá zaviedla aj novinku, princíp subsidiarity použitia dotknutých prostriedkov podľa § 3 ods. 1 posl. veta cit.: „*ak dosiahnutie účelu inak by bolo neúčinné alebo podstatne sťažené*“.

Celkovo z pohľadu vzájomnej komparácie oboch zákonných úprav možno uviesť, že obe úpravy ITP sú na mnohých miestach čo do lehôt a podmienok ich aplikácie obdobné, v niektorých prípadoch je úprava v zákone prísnejšia, inde nie, ale mechanizmus zachováva rovnaký.

Za všetky prvky spomenieme napríklad, že podľa zákona o ochrane pred odpočúvaním hovoríme o písomnom súhlase zákonného sudcu vydanom na základe žiadosti orgánu „... štátu, ktorý zamýšľa použiť informačno-technický prostriedok na uplatnenie svojej zákonom ustanovenej pôsobnosti (§ 2 ods. 2)“ (§ 4 ods. 4 zákona o ochrane pred odpočúvaním), v prípade Trestného poriadku ide už o písomný príkaz vydaný na základe návrhu. Rovnako v oboch prípadoch je táto činnosť vykonávaná nevyhnutne potrebný čas, na ktorý je vydaný príkaz či súhlas, najdlhšie však po dobu 6 mesiacov s možnosťou aj opakovaného predĺženia najviac na 6 mesiacov v prípade zákona o ochrane pred odpočúvaním, čo je trojnásobne dlhšie než v prípade trestno-procesnej úpravy, ktorá hovorí o najviac 2 mesiacoch. V oboch prípadoch sú stanovené zá-

onné podmienky pre situácie, ktoré neznesú odklad, v zásade ide opätovne o úpravu obdobnú. V oboch zákonoch platí nutnosť skúmať dôvody vykonávania tejto aktivity počas celej doby jej vykonávania.

V úvode sme hovorili o nevyhnutnosti kontroly takýchto aktivít zodpovedajúcich subjektov. Realizácia ITP by mala byť podrobená prísnej kontrole. Poslednou novelou zákona o ochrane pred odpočúvaním, zákonom č. 404/2015 Z. z. s účinnosťou od 1. 1. 2016, bol v súvislosti so zabezpečením takejto kontroly do zákona § 8a zavedený aj nový inštitút kontroly používania ITP Národnou radou Slovenskej republiky, resp. jej komisiou zriadenou na takýto účel.

Konštatujeme, že novela je výrazným prelomom k zvýšeniu kontroly používania ITP a významným spôsobom posilnila kontrolnú právomoc zákonodarného orgánu nad používaním ITP orgánmi výkonnej moci. Komisia Národnej rady Slovenskej republiky vykonáva v zmysle jeho dikcie kontrolu používania ITP vo všeobecnosti raz ročne, ale aj kedykoľvek z vlastného podnetu či z podnetu príslušného výboru alebo napokon v neposlednom rade na základe podnetu občana, ak sa domnieva, že sa ITP používajú voči nemu. Je samozrejmé, že výkonom takto nastavenej parlamentnej kontroly používania ITP však nie je dotknuté právo každého jednotlivca na súdnu alebo inú právnu ochranu.

Pokiaľ ide o upotrebitelnosť dôkazov získaných využitím ITP podľa zákona o ochrane pred odpočúvaním v ďalšom trestnom konaní prikláňame sa k judikatúre, ktorá takto získané dôkazy hodnotí ako dôkazy získané v súlade s § 119 ods. 2 Trestného poriadku, ergo ako všetko, čo môže prispieť na náležité objasnenie veci a čo sa získalo z dôkazných prostriedkov podľa osobitného zákona. V danom prípade sa vec týka práve zmieneného zákona, pričom dodávame, že podľa § 7 ods. 2 posl. veta zákona o ochrane pred odpočúvaním cit.: *„Informácie získané použitím informačno-technického prostriedku, ktoré sa nevzťahujú na dôvody jeho použitia uvedeného v žiadosti, sa môžu použiť ako dôkaz v trestnom konaní, len ak sa týkajú trestnej činnosti, v súvislosti s ktorou možno použiť informačno-technický prostriedok“*. Z citovaného je zrejmé, že takto získaný dôkaz je využiteľný aj v prípadoch, na ktoré sa pôvodná žiadosť nevzťahovala, avšak spĺňajú podmienky pre použitie ITP. V prípade Trestného poriadku je však použiteľnosť dôkazov v iných trestných konaniach oklieštená, buď konkrétnymi požiadavkami pre použitie samotného druhu ITP alebo skutočnosťami ako je skutková podstata trestného činu, trestná sadzba za konkrétny trestný čin, subjektívna stránka skutkovej podstaty trestného činu, atď.

Ako sme už uviedli vo všeobecnosti platí, že v prípade ITP ide jednak o prostriedky, ktoré smerujú k získaniu a zaisteniu informácií a niektoré aj k zaisteniu vecí dôležitých pre trestné konanie, rovnako sa nemusíme ani sporiť o fakty, že ich uplatnením sa zasahuje do súkromného sféry jednotlivca. Takéto zásahy však z hľadiska ich posúdenia musia spĺňať tri základné podmienky:

- podmienku legality v podobe myšlienky, že zásah do súkromia osoby musí byť vykonaný vždy na základe zákona a v súlade so zákonom,
- podmienku legitimacy v podobe záujmu spoločnosti na ochrane pred trestným činom, jeho zistení a spravodlivom potrestaní pachateľa skutku a napokon
- podmienku proporcionality spočívajúcu v systéme právnych predpisov a kontroly ich dodržiavania ako adekvátnych záruk.

Z praktického hľadiska ja charakteristickým a súčasne nevyhnutným znakom všetkých druhov ITP utajený spôsob ich vykonávania, ktorý má zabezpečiť, že pre trestné konanie sa získajú skutočne objektívne, neskreslené a nepozmenené informácie potrebné jednak pre samotný proces dokazovania (objasňovania) veci a následne napomáhajúce aj v konečnom rozhodovaní.

Najmä z dôvodu tejto utajenosti ako prvku, ktorý je pripisovaný a priori policajnému štátu, je nutné dodržiavať vyššie zmienené podmienky. Z praxe je zrejmé, že ak by konkrétne osoby, kto-

rých sa ITP dotýkajú, vedeli o ich použití, zrejme by pozmenili svoje správanie tak, aby sa vyhli možnému trestnému postihu, príp. aby sami vo svojej veci neposkytli usvedčujúce dôkazy. Keďže ide o prirodzenú reakciu zainteresovaných, práve táto skutočnosť je dôvodom prečo sa prostriedky ITP zásadne vykonávajú utajeným spôsobom.

Tu je potrebné mať na zreteli, že ide o veľmi tenkú hranicu, ktorá oddeluje potenciálne obeť použitých prostriedkov ITP od prípadov ich odôvodneného využitia. V konkrétnom prípade bude zmienená hranica stanovená rozhodovacou činnosťou jednotlivých subjektov (súdov, činnosť príslušníkov Policajného zboru) a ich prístupom k výkonu ITP. Je nutné si uvedomiť, že neoprávnené využívanie uvedeného inštitútu vytvára na strane osôb dotknutých jeho výkonom právo domáhať sa ochrany svojho práva na súkromie a potenciálne aj právo na náhradu takto spôsobenej škody.

Informačno-technické úkony realizované prostredníctvom ITP na základe zákona o ochrane pred odpočúvaním alebo Trestného poriadku sú vykonávané špecializovaným útvarom Policajného zboru pod názvom úrad zvláštnych policajných činností Prezídia Policajného zboru. Príslušníci tohto útvaru sa však počas svojej činnosti stretávajú s viacerými komplikáciami. Nakoľko ide o jeden z utajených prostriedkov odhaľovania a objasňovania trestnej činnosti, budú tieto komplikácie uvádzané v niekoľkých základných myšlienkach bez konkrétnych okolností či atribútov, pričom celý „skutkový“ dej len stručne opíšeme.

Ak odhliadneme od častých administratívnych chýb, ktoré v takýchto časovo vyhrotených prípadoch aj zo strany súdu nastávajú, vyskytujú sa aj tie, ktoré spočívajú v rôznom právnom názore súdu a polície.

Ako časté administratívne pochybenie v súvislosti so slovným znením príkazu na použitie ITP vydaného súdom vidíme zjavne chybné vymedzenia času a miest použitia ITP, čo spôsobuje samozrejme ďalekosiahle komplikácie pri ich výkone, keďže miesto a čas ich vykonávania musia byť presne vymedzené, jasne, zrozumiteľne a najmä nezameniteľne s inými, nakoľko takéto narušenie súkromia inej než dotknutej osoby je v právnom štáte nemysliteľné. Rovnako nezriedkavými sú prípady, kedy príkaz obsahuje vo výrokovej časti skutočnosti týkajúce sa inej trestnej veci aká je uvedená v odôvodnení príkazu. Aj takáto chyba je častou chybou súdov, ktorá následne sťažuje výkon informačno-technického úkonu v teréne a v prípade chvatu sa rýchlo môže aj prehliadnuť.

Z pohľadu odlišných právnych názorov uvádzame príklad, v ktorom podľa nášho názoru súd konal v rozpore s ustanovením Trestného poriadku, nakoľko najprv sudca vydal príkaz podľa § 114 ods. 1 Trestného poriadku na časové obdobie 3 mesiacov, pričom v rámci predĺženia tento čas predĺžil namiesto lehoty stanovenej zákonom pre ďalšie predĺženie, a síce 2 mesiacov, na mesiace 3 s odôvodnením, že lehota stanovená v § 114 ods. 3 Trestného poriadku, t. j. prvá lehota, zostáva zachovaná.

S uvedeným názorom súdu si však dovoľíme nesúhlasiť, keďže z dikcie samotného ustanovenia § 114 ods. 3 Trestného poriadku vyplýva, že v príkaze musí byť stanovený čas vyhotovovania záznamov a tento môže trvať najdlhšie 6 mesiacov, pričom príkaz ten, kto ho vydal, môže predĺžiť, avšak vždy najviac o 2 mesiace, a to aj opakovane. Zákonodarca na tomto mieste nehovorí o sťahy časti 6-mesačnej lehoty vyčerpanej na základe príkazu a ďalšej časti 3 mesiacov vyčerpanej na základe jej predĺženia. Takýto prístup súdu je podľa nášho názoru v rozpore s platnou právnou úpravou a nezákonný, v konečnom dôsledku môže odvolací súd podniknúť na vyhlásenie takto získaných dôkazov za nezákonne získané.

Z technických problémov aplikačnej praxe, s ktorými sa polícia potýka, sú to najmä problémy v súvislosti so snahou súdov presne vymedziť plánované ITP.

Prvoradou podmienkou pri výkone informačno-technických úkonov prostredníctvom ITP je, aby špecializovaný útvar Policajného zboru predbežne posúdil, resp. zhodnotil, možnosti nasadenia ITP z hľadiska objektívnych okolností a znakov záujmového priestoru. Na základe takéhoto posúdenia je následne možné vytipovať reálne ITP použiteľné v danom prostredí tak, aby bol dosiahnutý účel ich využitia.

Je rovnako možné, že v prípade absencie predbežného posúdenia by došlo k predčasnému zmareniu účelu trestného konania, keďže by koniec-koncov z pohľadu reálnych technických možností nemuselo byť ITP vôbec realizovateľné. Aj napriek zmienenému nie je v aplikačnej praxi ojedinelým, že sa tak deje a postup zhodnotenia špecializovaným útvarom sa obchádza, pričom nie je podstatné z akého dôvodu a súd aj napriek tomu, že využitie konkrétneho ITP v danom prípade nie je predbežne zhodnotené špecializovaným úradom príkaz na jeho vykonanie vydá, čo teda môže v závere viesť k nerealizovateľnosti príkazu či súhlasu, a tým k narušeniu celého procesu odhaľovania, objasňovania a vyšetrovania skutku.

Častými sú v súdnej praxi aj požiadavky súdov na presné špecifikácie technických prostriedkov, ktoré budú použité pri vykonávaní informačno-technických úkonov už v samotnom návrhu (či podnete zo strany polície) alebo žiadosti na vydanie písomného súhlasu. Uvedenie takýchto informácií nie je z pohľadu skutočnosti, že tieto činnosti majú jasne stanovený zmysel (odhaliť, objasniť skutok, a zistiť jeho páchatela) a kvôli nemu sú vykonávané utajene, podľa nášho názoru vhodné a z hľadiska účelu celého trestného konania, dovoľme si povedať, prípustné, keďže práve „odkrytím“ takýchto dôležitých elementov by mohlo dôjsť nielen k zmareniu dotknutého trestného stíhania, ale vzhľadom na učenlivosť a technickú vyspelosť páchatelov aj mnohých ďalších. A určite by nemalo preventívny charakter, nakoľko by spôsobilo, že páchatelia budú o krok vpred.

Rovnako závažný technický problém nastane, ak súd sám v príkaze určí konkrétnych technických prostriedkov na vykonanie informačno-technického úkonu. Opätovne môže byť jeho dôsledkom konečná nerealizovateľnosť informačno-technického úkonu.

Záver

Súčasná situácia vyšetrovania najzávažnejších trestných činov si jednoznačne vyžaduje využívanie moderných a ofenzívnych prostriedkov, ktoré zasahujú aj do oblasti základných ľudských práv a slobôd a kam rozhodne zaraďujeme aj ITP. ITP predstavujú prostriedky, ktoré smerujú k zaisťovaniu informácií a vecí dôležitých pre trestné konanie, avšak súčasne silne zasahujú do súkromia jednotlivcov. Pri ich aplikácii musia byť nutne naplnené zákonné predpoklady, za ktorých je možné využitie týchto prostriedkov realizovať. V opačnom prípade pri ich nedodržaní by v trestnom konaní išlo nielen o nezákonne získané dôkazy, ktoré by sa nedali ďalej v konaní využiť, ale súčasne by na strane dotknutých osôb vytvorili priestor pre uplatnenie si práva na ochranu pred takýmito neoprávnenými zásahmi.

Práve ich zákonné použitie, dodržiavanie všetkých ustanovení zákonných či podzákonných právnych predpisov, umožní považovať takéto zásahy do súkromia jednotlivcov vystavených predmetnému druhu „tajného dohľadu“ za oprávnené.

Z pohľadu aplikačnej praxe si dovoľme dodať, že samozrejme ako pri akejkolvek ľudskej činnosti aj v prípade použitia ITP sa vyskytnú nedostatky a isté komplikácie, ktoré sú vzhľadom na citlivosť tejto témy často verejnosťou pranierované, dokonca výrazná časť pochybení môže viesť k „zneprocesneniu“ získaných dôkazov, a tým k zmareniu úsilia „policajných“ orgánov činných v trestnom konaní ako aj ostatných zainteresovaných príslušníkov Policajného zboru. Preto je

nutné z pohľadu zainteresovaných – polície, súdov a prokuratúry o výhradách či námietkach, ktoré by mohli viesť ku komplikáciám, komunikovať, a tým problémy odstraňovať tak, aby sa v praxi nevyskytovali, resp. vyskytovali v malej miere. Avšak *summa summarum* je nutné povedať, že odhliadnuc od niektorých závažností v praxi je množstvo prípadov, kde dochádza k súladu konania súdov, prokuratúry a polície, lebo v prvom rade si je vždy potrebné uvedomiť, že trestné konanie ako také nepredstavuje len aktivity vyvíjané jedným subjektom, ale ide o celý rad krokov, na ktorých sú zainteresovaní mnohí účastníci a momenty a jeho zmarenie nie je vinou jedného.

Zoznam bibliografických odkazov

Monografie / knihy

1. Čentéš, J. a kol. 2014. *Trestný poriadok – Veľký komentár*. Bratislava: Eurokódex, 2014. 943 s. ISBN 978-80-8155-021-8.
2. Drgonec J. 2012. *Ústava Slovenskej republiky. Komentár*. Bratislava: Heuréka, 2012. 1620 s. ISBN 978-80-8912-273-8.
3. Ivor, J. a kol. 2006. *Trestné právo procesné*. Bratislava: Iura Edition, 2006. 961 s. ISBN 80-8078-101-X.

Elektronické zdroje

1. <<http://www.vyvlastnenie.sk/predpisy/listina-zakladnych-prav-a-slobod/>>.
2. Európsky dohovor o ľudských právach. Dostupné na internete: <http://www.echr.coe.int/Documents/Convention_SLK.pdf>.
3. Všeobecná deklarácia ľudských práv. Dostupné na internete: <<http://www.upn.gov.sk/data/pdf/deklaracia.pdf>>.

Legislatíva

1. zákon č. 460/1992 Zb. Ústava Slovenskej republiky.
2. zákon č. 301/2005 Z. z. Trestný poriadok.
3. zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním).
4. zákon č. 404/2015 Z. z. ktorým sa mení a dopĺňa zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) v znení neskorších predpisov.
5. nariadenie ministra vnútra Slovenskej republiky č. 30/2012 o použití informačno-technických prostriedkov.

Judikatúra

1. Nález Ústavného súdu Slovenskej republiky, I. ÚS 13/00.
2. Nález Ústavného súdu Slovenskej republiky, PL. ÚS 43/95.

Zásah do práva na súkromie použitím informačno-technických prostriedkov vo svetle rozhodovacej činnosti Európskeho súdu pre ľudské práva

Interference with the Right to Privacy Using Means of Secret Surveillance in the Light of Case-law of the European Court of Human Rights

Miroslava Bálintová¹

Abstrakt: Dôsledná ochrana ľudských práv a základných slobôd vyžaduje existenciu primeraných záruk proti zneužitiu opatrení zameraných na sledovanie osôb. Európsky súd pre ľudské práva v Štrasburgu vo svojej judikatúre vyslovil viacero požiadaviek predovšetkým na kvalitu právnej úpravy umožňujúcej používanie takýchto opatrení.

Abstract: Consistent protection of human rights and fundamental freedoms require existence of appropriate guarantees against abuse of means for secret surveillance of people. The European Court of Human Rights in Strasbourg determined in its case-law several requirements concerning in particular quality of law allowing the use of such means.

Kľúčové slová: tajné sledovanie; odpočúvanie; záruky.

Key words: secret surveillance; telephone interception; guarantees.

Odpočúvanie a použitie iných opatrení na sledovanie osôb spadá pod článok 8 Dohovoru na ochranu ľudských práv a základných slobôd (ďalej len „Dohovor“), zaručujúci právo na rešpektovanie súkromného a rodinného života. Keďže v zmysle tohto článku,² konkrétne jeho druhého odseku, môže štátny orgán zasahovať do výkonu práva na rešpektovanie súkromného a rodinného života, obdobia a korešpondencie iba v prípadoch, ak je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom a zločinnosti, ochrany zdravia alebo morálky alebo ochrany práv a slobôd iných, Európsky súd pre ľudské práva (ďalej len „Súd“) pri posudzovaní prípadov týkajúcich sa použitia týchto opatrení kladie osobitný dôraz na podmienku súladu so zákonom, a teda na zlučiteľnosť vnútroštátnej právnej úpravy so zárukami článku 8 Dohovoru. V zmysle ustálenej judikatúry Súdu táto podmienka implicitne obsahuje **požiadavku, aby príslušný zákon, predstavujúci zákonný základ pre opatrenia zasahujúce do súkromia osôb, bol dostatočne prístupný dotknutej osobe, aby táto mohla predvídať dôsledky jeho aplikácie**, a aby bol zlučiteľný s princípom právneho štátu. Požiadavka právnej „predvídateľnosti“ osobitne v súvislosti s tajnými opatreniami na sledovanie, akými je aj odpo-

¹ JUDr. Miroslava Bálintová, spoluzástupkyňa Slovenskej republiky pred Európskym súdom pre ľudské práva, Ministerstvo spravodlivosti Slovenskej republiky, Župné námestie 13, 813 11 Bratislava, e-mail: miroslava.balintova@justice.sk.

² Článok 8 Dohovoru na ochranu ľudských práv a základných slobôd znie: 1. Každý má právo na rešpektovanie svojho súkromného a rodinného života, obdobia a korešpondencie. 2. Štátny orgán nemôže do výkonu tohto práva zasahovať okrem prípadov, keď je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom a zločinnosti, ochrany zdravia alebo morálky alebo ochrany práv a slobôd iných.

čúvanie, nemôže samozrejme znamenať, že jednotliviec bude spôsobilý predvídať, kedy štátne orgány pravdepodobne začnú odpočúvať jeho hovory, aby v súlade s tým mohol prispôbiť svoje správanie. Vnútroštátne právo však musí byť dostatočne jasné, pokiaľ ide o jeho znenie, aby poskytovalo jednotlivcom primerané indície o okolnostiach a podmienkach, za ktorých sú štátne orgány oprávnené uchýliť sa k takýmto opatreniam. Súd v tejto súvislosti zároveň zdôraznil **potrebu adekvátnych a účinných záruk proti zneužitiu**. Za takéto záruky v súvislosti s odpočúvaním Súd vo svojej judikatúre považoval najmä definovanie kategórií osôb, ktoré môžu byť odpočúvané, či trestných činov, v súvislosti s ktorými možno realizovať odpočúvanie, časové obmedzenie odpočúvania, kontrolu nezávislým súdnym orgánom, postupy pre vyhotovenie záznamov o obsahu odpočúvaných hovorov, úpravu podmienok uchovávania vyhotovených záznamov a nahrávok a vymedzenie okolností, za ktorých môžu alebo nemusia byť nahrávky vymazané a zvukové nosiče alebo iné záznamy zničené.³

Prípadov týkajúcich sa problematiky odpočúvania a použitia iných opatrení na sledovanie osôb je mnoho.⁴ Pokiaľ ide o Slovenskú republiku, za zmienku stojí prípad *Kvasnica v. Slovenská republika* (rozsudok z 9. júna 2009), ktorého základom bolo odpočúvanie sťažovateľa v rámci vyšetrovania rozsiahlej organizovanej trestnej činnosti finančného charakteru, ktorá mala byť spáchaná zamestnancami dcérskej spoločnosti najvýznamnejších oceliarní. Vyšetrovanie viedol špecializovaný vyšetrovací tím zriadený rozkazom ministra vnútra a zložený z policajtov patriacich k finančnej polícii. Dôvodom pre podanie žiadosti o súhlas s odpočúvaním sťažovateľovho telefónu boli predovšetkým poznatky špecializovaného vyšetrovacieho tímu o tom, že sťažovateľ nadštandardne komunikuje s jedným z obvinených, pričom však nebol jeho advokátom, a že sa snaží všemožne získavať poznatky o priebehu vyšetrovania. Súhlas s použitím informačno-technických prostriedkov voči sťažovateľovi dal sudca Krajského súdu v Bratislave. Po tom, ako sa prepisy sťažovateľových rozhovorov objavili v médiách a u tretích osôb, sťažovateľ podal viaceré trestných oznámení. Rovnako podal trestné oznámenie aj riaditeľ odboru zvláštnych úloh správy kriminálnej a finančnej polície. Vec prešetrovala inšpekčná služba ministerstva vnútra. V rámci vyšetrovania predložil sudca, ktorý dal súhlas na odpočúvanie, písomné vyjadrenie, v ktorom okrem iného uviedol, že vo všeobecnosti sú žiadosti o súhlas s odpočúvaním podávané v písomnej forme, ale sú predkladané osobne, pričom príslušník polície, ktorý žiadosť predkladá, zdôvodňuje vec ústne a ústna informácia je spravidla rozsahom širšia ako písomná žiadosť. Keďže o žiadostiach o súhlas s odpočúvaním je potrebné rozhodovať rýchlo a operatívne, sudcovia nemajú praktickú možnosť naštudovať si spis alebo overiť si, či obsah žiadosti o súhlas s odpočúvaním zodpovedá obsahu spisu. Navyše, informácie v spise sú často krát získané z neove-

³ Pozri napr. *Huvig v. Francúzsko*, rozsudok z 24. apríla 1990, ods. 32; alebo *Kruslin v. Francúzsko*, rozsudok z 24. apríla 1990, ods. 33.

⁴ Pozri napr. *Klass a ďalší v. Nemecko*, rozsudok zo 6. septembra 1978; *Malone v. Spojené kráľovstvo*, rozsudok z 2. augusta 1984; *Mersch a ďalší v. Luxembursko*, rozhodnutie z 10. mája 1985; *M. S. a P. S. v. Švajčiarsko*, rozhodnutie zo 14. októbra 1985; *Spillmann v. Švajčiarsko*, rozhodnutie z 8. marca 1988; *A. v. Francúzsko*, rozsudok z 23. novembra 1993; *Kopp v. Švajčiarsko*, rozsudok z 25. marca 1998; *Kruslin v. Francúzsko*, rozsudok z 24. apríla 1990; *Huvig v. Francúzsko*, rozsudok z 24. apríla 1990; *P. L. v. Nórsko*, rozhodnutie z 8. júna 1990; *Christie v. Spojené kráľovstvo*, rozhodnutie z 27. júna 1994; *Valenzuela Contreras v. Španielsko*, rozsudok z 30. júla 1998; *Lambert v. Francúzsko*, rozsudok z 24. augusta 1998; *Amman v. Švajčiarsko*, rozsudok zo 16. februára 2000; *Khan v. Spojené kráľovstvo*, rozsudok z 12. mája 2000; *Greuter v. Holandsko*, rozhodnutie z 19. marca 2002; *Al-Nasif v. Bulharsko*, rozsudok z 20. júna 2002; *Prado Bugallo v. Španielsko*, rozsudok z 18. februára 2003; *M. M. v. Holandsko*, rozsudok z 8. apríla 2003; *Doerga v. Holandsko*, rozsudok z 27. apríla 2004; *Aalmoes a 112 ďalších v. Holandsko*, rozhodnutie z 25. novembra 2004; *Abdulkadir Coban v. Španielsko*, rozhodnutie z 25. septembra 2006; *Weber a Saravia v. Nemecko*, rozhodnutie z 29. júna 2006; *Združenie pre európsku integráciu a ľudské práva a Ekimdzhiiev v. Bulharsko*, rozsudok z 28. júna 2007; *Kirov v. Bulharsko*, rozsudok z 22. mája 2008; *Bykov v. Rusko*, rozsudok z 10. marca 2009; *Iordachi a ďalší v. Moldavsko*, rozsudok z 10. februára 2009 a mnohé ďalšie.

riteľných zdrojov. Sudcovia sa preto musia spoľahnúť na informácie uvedené v žiadosti o súhlas s odpočúvaním, čo predpokladá istý stupeň vzájomnej dôvery orgánov činných v trestnom konaní. Sudca ďalej uviedol, že v agende týkajúcej sa odpočúvania došlo k enormnému nárastu nápadu, čo bolo spôsobené okrem iného aj vďaka medzirezortnej dohode, ku ktorej došlo na ministerstve spravodlivosti a ktorou bola rozšírená vecná príslušnosť Krajského súdu v Bratislave v tejto agende. Podľa jeho názoru by otázka vecnej príslušnosti nemala byť upravená „dohodou“ ale zákonom, čo vo vzťahu k agende odpočúvania chýbalo. Sudca uviedol, že v priebehu preverovania podozrenia z páchania rozsiahlej ekonomickej trestnej činnosti v rámci vyššie uvedenej priemyselnej skupiny boli udelené súhlasy na odpočúvanie telekomunikačnej prevádzky v troch predchádzajúcich prípadoch. Vďaka tomu mal o sťažovateľovej veci dostatočné a podrobné informácie. Sudca sa plne stotožnil s prijatým rozhodnutím, aj keď sa podozrenie voči sťažovateľovi neskôr nemuselo potvrdiť. Takáto situácia nebola zriedkavá a dochádzalo k nej v 10–20 % prípadov. Inšpekčná služba okrem toho vypočula štyroch členov vyšetrovacieho tímu, ktorí vo svojich výpovediach uviedli informácie o tom, že operatívna časť tímu nadštandardne komunikovala a nad rámec stanovených úloh spolupracovala so sťažovateľom, že sťažovateľ bol v úzkom kontakte s jedným z obvinených, že sťažovateľ bol zaplatený do viacerých obchodných transakcií v rámci skupiny, ktoré mohli poškodiť záujmy oceliarní, že návrh na povolenie odpočúvať sťažovateľov telefón sa zakladal na podozrení, že sťažovateľ sa dopustil obzvlášť závažného trestného činu podvodu a trestného činu legalizácie príjmu z trestnej činnosti, že návrh bol vypracovaný bez naštudovania spisu, že odpočúvanie bolo potrebné, pretože bez neho sa nedalo pohnúť vo vyšetrovaní, a že po odhalení odpočúvania bol spis sprístupnený viacerým funkcionárom vrátane ministra spravodlivosti, ktorý v tom čase *ad interim* vykonával aj funkciu ministra vnútra. Všetky trestné oznámenia však boli napokon odložené alebo bolo konanie o nich zastavené. Sťažovateľ pred Súdom namietal tak nesúlad realizovaných opatrení s platnou právnou úpravou, ako aj jej kvalitu, trvajúc predovšetkým na tom, že nedostatočným spôsobom upravovala záruky proti zneužitiu. Súd v tomto prípade poukázal na to, že vyhlásenia viacerých policajných funkcionárov a zainteresovaného sudcu naznačovali množstvo pochybení, pokiaľ ide o dodržanie príslušných právnych predpisov v sťažovateľovom prípade. Súd nebol presvedčený, že v sťažovateľovom prípade boli splnené všetky zákonné podmienky, napríklad nebolo preukázané, že boli dodržané záruky týkajúce sa dĺžky zásahu, že existovala nepretržitá súdna kontrola odpočúvania, že dôvody na použitie informačno-technických prostriedkov trvali, že boli prijaté opatrenia s cieľom zabrániť odpočúvaniu telefonických rozhovorov medzi sťažovateľom ako advokátom a trestne stíhanými ako jeho klientmi, že zásah obmedzil nedotknuteľnosť sťažovateľovho obydľia, súkromný charakter jeho korešpondencie a odovzdávaných informácií iba v rozsahu, ktorý bol nevyhnutný, a že takto získané informácie boli použité výlučne na dosiahnutie cieľa prípustného podľa vnútroštátnej právnej úpravy. Za týchto okolností Súd dospel k záveru, že došlo k porušeniu článku 8 Dohovoru.

Nedodržanie podmienok vnútroštátnej právnej úpravy bolo samozrejme dôvodom na konštatovanie porušenia článku 8 Dohovoru aj v mnohých iných prípadoch, z tých posledných možno spomenúť prípad *Meimanis v. Lotyšsko* (rozsudok z 21. júla 2015).

Pri posudzovaní sťažností týkajúcich sa použitia opatrení na sledovanie osôb Súd uplatňuje špecifický prístup, keď nevyžaduje, aby sťažovateľ preukázal, že skutočne k zásahu do jeho práv došlo. Uvedený prístup Súd zvolil z dôvodu, že sťažovatelia vzhľadom na povahu veci, teda utajovanie používania operatívnej techniky, nemajú vždy jasný dôkaz o tom, že boli subjektom odpočúvania či iných opatrení na sledovanie osôb. Súdu preto postačuje, ak je „rozumne pravdepodobné“, že sťažovateľ bol predmetom použitia takýchto opatrení. Súd však v tomto ohľade išiel ešte ďalej a v súvislosti s použitím týchto opatrení v podstate pripúšťa inak neprípustnú *actio po-*

pularis. Postačuje, aby vnútroštátna právna úprava umožňovala využitie opatrení na odpočúvanie a iné sledovanie osôb voči sťažovateľovi a zásah do práv pre potreby článku 8 Dohovoru tak bude predstavovať už samotná existencia takejto právnej úpravy.⁵

V prípade *Liberty a ďalší v. Spojené kráľovstvo* (rozsudok z 1. júla 2008) vzniesli sťažnosť pred Súdom jedna britská a dve írské občianskoprávne organizácie, ktoré tvrdili, že v období rokov 1990 až 1997 bola ich telefonická, faxová, e-mailová a dátová komunikácia, vrátane komunikácie, ktorá je v zmysle zákona dôverná, monitorovaná prostredníctvom zariadenia prevádzkovaného britským ministerstvom obrany. Súd preskúmal vnútroštátnu právnu úpravu a dospel k záveru, že táto neupravovala dostatočne jasne, tak aby poskytovala primeranú ochranu proti zneužitiu, rozsah alebo spôsob výkonu skutočne širokej miery voľnej úvahy, ktorú priznávala štátnym orgánom pri zachytávaní a odpočúvaní komunikácie. Predovšetkým neupravovala v podobe dostupnej verejnosti žiadny postup na selekciu, odovzdávanie, uchovávanie a zničenie zachyteného materiálu, ako to vyžaduje judikatúra Súdu. Zásah do práv sťažovateľov podľa článku 8 Dohovoru teda nebol „v súlade so zákonom“ a došlo k porušeniu tohto článku.

Súd v množstve prípadov podrobil kritike aj právne úpravy iných štátov.⁶ Z tých najaktuálnejších možno spomenúť prípad *Roman Zakharov v. Rusko* (rozsudok zo 4. decembra 2015), o ktorom rozhodovala veľká komora Súdu a dospela k záveru, že vnútroštátna právna úprava neobsahuje adekvátne a účinné záruky proti zneužitiu. Ďalším je prípad *Szabó a Vissy v. Maďarsko* (rozsudok z 12. januára 2016), ktorý sa týkal maďarskej právnej úpravy umožňujúcej tajné sledovanie osôb pre spravodajské účely s cieľom boja proti terorizmu, prijatej v roku 2011. Dotknutou právnou úpravou boli zvláštnej protiteroristickej jednotke zverené rozsiahle právomoci, vrátane ktorých mohla okrem iného bez súhlasu dotknutých osôb vykonávať tajné domové prehliadky, realizovať odpočúvanie, zadržiavať a otvárať zásielky a sledovať obsah elektronickej komunikácie. Na povoľovanie týchto opatrení boli stanovené dva rôzne režimy; ak išlo o vyšetrovanie zákonom vymedzených trestných činov, spomínané opatrenia podliehali povoleniu súdom a ak išlo o predchádzanie teroristickým činom, plnenie spravodajských úloh v záujme národnej bezpečnosti alebo záchranu maďarských občanov zajatých v zahraničí v súvislosti s ozbrojenými konfliktami alebo teroristickými činmi, vyžadovali súhlas ministra spravodlivosti. Súd po preskúmaní tejto právnej úpravy rozhodol o porušení článku 8 Dohovoru. Vytkol jej najmä to, že sa potenciálne môže dotknúť prakticky kohokoľvek v Maďarsku a vytvára v podstate priestor pre neobmedzené sledovanie značného počtu osôb. Ďalej vyjadril znepokojenie nad tým, že zákon nevyžaduje ani to, aby príslušné orgány preukázali akékoľvek skutočné alebo domnelé spojenie medzi dotknutou osobou alebo okruhom osôb a zistenou teroristickou hrozbou, v dôsledku čoho nemožno vylúčiť riziko strategického a plošného sledovania obyvateľstva. Ďalej Súd podrobil kritike aj režim povoľovania sledovania, ktorý v tomto prípade nespĺňal podmienku, aby účinná kontrola nad výkonom právomocí výkonnej moci bola aspoň v konečnom stupni a *ex ante* zverená nezávislým a nestranným súdom. Okrem toho boli príslušné orgány žiadajúce ministra o povolenie povinné žiadosť odôvodniť, avšak nie podložiť relevantnými podkladmi, ktoré by umožňovali posúdiť „striktnú nevyhnutnosť“ využitia týchto opatrení. Ďalej v právnej úprave chýbalo jasné pravidlo o počte možných predĺžení doby použitia sledovacích opatrení a úplne absentovala možnosť dotknutých osôb domôcť sa účinnej ochrany proti svojoľným zásahom do ich práv.

⁵ K tomu bližšie pozri napr. *Klass a ďalší v. Nemecko*, rozsudok zo 6. septembra 1978, ods. 37 – 38; alebo *Liberty a ďalší v. Spojené kráľovstvo*, rozsudok z 1. júla 2008, ods. 56.

⁶ Pozri napr. *Kruslin v. Francúzsko*, rozsudok z 24. apríla 1990; *Wisse v. Francúzsko*, rozsudok z 22. decembra 2005; *Kopp v. Švajčiarsko*, rozsudok z 25. marca 1998; *Amann v. Švajčiarsko*, rozsudok zo 16. februára 2000; *Dragojević v. Chorvátsko*, rozsudok z 15. januára 2015; *Bašić v. Chorvátsko*, rozsudok z 25. októbra 2016, atď.

Prístup nehodnotenia právnej úpravy *in abstracto*, ale hodnotenia veci konkrétne vo vzťahu k sťažovateľovi, ktorý namietal okrem iného aj nedostatočnosť záruk proti zneužitiu v právnej úprave však Súd zvolil v prípade *Pastyřík v. Česká republika* (rozhodnutie z 31. mája 2011), v ktorom nakoniec zamietol sťažnosť ako zjavne nepodloženú.

Niektoré právne úpravy testom splnenia kritérií vyplývajúcich z judikatúry Súdu prešli. Ako príklad možno spomenúť prípad *Kennedy v. Spojené kráľovstvo* (rozsudok z 18. mája 2010), v ktorom sa Súd s odstupom času zaoberal zmenenou britskou právnou úpravou spolu s vysvetleniami, ktoré prinieslo zverejnenie praktického kódexu. Pokladal ju za vyhovujúcu a rozhodol, že článok 8 Dohovoru porušený nebol. Britská právna úprava je však často predmetom sťažností pred Súdom. V súčasnosti pred Súdom prebieha konanie o viacerých prípadoch, v ktorých buď mimovládne organizácie alebo novinárske združenia namietajú okrem iného porušenie článku 8 Dohovoru v dôsledku toho, že sa pravdepodobne môžu stať objektom odpočúvania zo strany spravodajských služieb, a to podľa platnej právnej úpravy, ktorá podľa nich nespĺňa Súdom vyžadované záruky. Odvolávajú sa na odhalenia Edwarda Snowdena, bývalého správcu systémov v Národnej bezpečnostnej agentúre Spojených štátov (NSA). Ide o prípady *Big Brother Watch a ďalší v. Spojené kráľovstvo* (č. 58170/13), *Bureau of Investigative Journalism a Alice Ross v. Spojené kráľovstvo* (č. 62322/14) a *10 ľudsko-právnych organizácií a ďalší v. Spojené kráľovstvo* (č. 24960/15). Súd v súčasnosti prejednáva aj prípady proti ďalším štátom, v ktorých sa sťažovatelia sťažujú na nedostatky v právnej úprave týkajúcej sa využívania ITP, ktoré podľa nich predstavujú porušenie článku 8 Dohovoru, ale aj iných článkov, predovšetkým článku 13 (právo na účinný prostriedok úpravy), článku 10 (slobody prejavu), prípadne ďalších. Ide napríklad o prípady *Centrum För Rättvisa v. Švédsko* (č. 35252/08) alebo *Tretter a ďalší v. Rakúsko* (3599/10).

Súd spočiatku vo svojich rozsudkoch explicitne nevyslovil požiadavku, aby o použití tajných opatrení na sledovanie osôb bola informovaná, samozrejme až *a posteriori*, sledovaná osoba. Pridržiaval sa názoru, že povaha a logika tajného sledovania vyžaduje, aby sa nielen sledovanie samotné, ale aj jeho následná kontrola uskutočňovali bez vedomia kontrolovanej osoby. Opakovane skonštatoval, že skutočnosť, že jednotlivec nie je informovaný ani potom ako sledovanie skončilo, nie je nezlučiteľná s článkom 8 Dohovoru, ak systém poskytuje dostatočné záruky proti zneužitiu. Náznaky vývoja iným smerom možno nájsť v prípade *Weber a Saravia v. Nemecko* (rozhodnutie z 29. júna 2006). Predmetom sťažnosti bolo okrem iného rozšírenie právomocí federálnej spravodajskej služby v súvislosti s tzv. strategickým sledovaním, zameraným na získavanie informácií prostredníctvom odpočúvania za účelom zisťovania a odvrátenia vážneho nebezpečenstva hroziaceho štátu, napr. ozbrojených útokov na území štátu, medzinárodných teroristických útokov alebo iných závažných činov, ako aj použitie získaných informácií a ich odovzdávanie ďalším orgánom. Ide o systém opatrení na sledovanie, ktorý je odlišný od tzv. individuálneho sledovania, spočívajúceho v odpočúvaní jednotlivcov podozrivých z trestných činov na účely trestného stíhania. Súd preskúmal kvalitu príslušného nemeckého zákona z hľadiska jeho zlučiteľnosti so zárukami práva na rešpektovanie súkromného života. Ešte sa neodchýlil od ustáleného názoru, že skutočnosť, že odpočúvaná osoba nie je po skončení odpočúvania o jeho uskutočnení informovaná, sama osebe neznamená, že zásah do jej práv nespĺňa podmienku nevyhnutnosti v demokratickej spoločnosti, zároveň však podotkol, že hneď, ako možno odpočúvanú osobu informovať o použití opatrení na jej sledovanie bez toho, aby sa tým ohrozil účel ich použitia, mala by jej byť takáto informácia poskytnutá. Po preskúmaní príslušnej nemeckej legislatívy, ktorá takúto povinnosť pre štátne orgány s určitými obmedzeniami stanovuje, ako aj rozhodovacej činnosti nemeckého federálneho ústavného súdu, ktorý zákonné záruky ešte rozšíril, dospel k záveru, že táto vyhovuje požiadavkám článku 8 Dohovoru a sťažnosť na porušenie článku 8 Dohovoru zamietol ako zjavne nepodloženú.

Následne Súd v roku 2007 vyhlásil rozsudok v prípade *Združenie pre európsku integráciu a ľudské práva a Ekimdzhiev v. Bulharsko* (rozsudok z 28. júna 2007). Sťažovatelia napadli existenciu vnútroštátneho zákona umožňujúceho použitie osobitných opatrení na tajné sledovanie za účelom odhaľovania a zabránenia závažným trestným činom alebo ochrany národnej bezpečnosti, ktorý ich vystavuje hrozbe, že v ňom upravené prostriedky sledovania voči nim môžu byť použité bez toho, aby o tom boli niekedy vyzvednutí. Namietali tiež, že vo vnútroštátnom právnom poriadku neexistuje žiaden účinný prostriedok nápravy, ktorým by mohli napadnúť použitie osobitných prostriedkov sledovania osôb. Súd preskúmal bulharskú právnu úpravu, a to tak napadnutý zákon, ako aj trestné poriadky. Pokiaľ ide o kvalitu inkriminovaného zákona, dospel k záveru, že zatiaľ čo v počiatočnom štádiu sledovania príslušné zákonné ustanovenia poskytujú dostatočné záruky proti svojvoľnému sledovaniu osôb (sledovanie možno realizovať iba na základe príkazu sudcu, v naliehavých prípadoch na základe príkazu ministra vnútra, pričom do 24 hodín musí byť vydaný súdny príkaz, príkaz je časovo obmedzený a vydať ho možno iba na základe náležite odôvodnenej písomnej žiadosti kompetentných zložiek), v neskorších štádiách, najmä v priebehu sledovania alebo po jeho skončení, už tomu tak nie je. Súd predovšetkým kritizoval, že (i) zákon neupravuje možnosť preskúmania realizácie opatrení zameralých na tajné sledovanie žiadnym externým a nezávislým orgánom alebo úradníkom (hoci zákon stanovuje povinnosť oznámiť sudcovi, ktorý vydal príkaz, ukončenie tajného sledovania, nestanovuje povinnosť oboznámiť ho s výsledkami sledovania a ani povinnosť pre príslušného sudcu preskúmať dodržanie zákona pri realizácii týchto opatrení), (ii) v zákone absentujú pravidlá upravujúce zaznamenávanie spravodajskej činnosti a uchovávanie a zničenie záznamov, (iii) celá kontrola systému tajného sledovania je zverená výlučne ministerstvu vnútra, pričom spôsob, akým minister vykonáva túto kontrolu, zákonom stanovený nie je, a (iv) osoby, ktoré sú objektom tajného sledovania, nie sú o použití týchto opatrení nikdy (ani dodatočne) informované. Súd uviedol, že dôsledkom tohto stavu je, že pokiaľ na základe získaných informácií nedôjde k trestnému stíhaniu osoby, alebo nedôjde k úniku informácií, dotknuté osoby sa nikdy nedozvedia, že boli sledované a nemôžu sa preto domáhať odškodnenia za prípadné nezákonné zásahy do ich práva na rešpektovanie súkromného života. Podľa Súdu tak bulharský právny poriadok neobsahuje jednu z dôležitých záruk proti neoprávnenému používaniu osobitných opatrení na tajné sledovanie osôb. Súd tiež podotkol, že podľa dostupných informácií je v Bulharsku v porovnaní s inými krajinami vydávaných príliš veľa príkazov na odpočúvanie, pričom samotné vnútroštátne orgány vo svojich správach poukázali na viacero prípadov porušenia zákona. Na základe všetkých uvedených skutočností Súd dospel k záveru, že bulharský právny poriadok neposkytuje dostatočné záruky proti zneužitiu opatrení na tajné sledovanie osôb a jeho existencia predstavuje taký zásah do práva sťažovateľov, zaručeného článkom 8 Dohovoru, ktorý nie je „v súlade so zákonom“ v zmysle druhého odseku tohto ustanovenia. Preto v tomto prípade došlo k porušeniu článku 8 Dohovoru.

V ďalšom rozsudku v prípade *Kirov proti Bulharsku* (rozsudok z 22. mája 2008) Súd potvrdil vyslovený názor a konštatoval, že tento prípad jednoznačne preukazuje absenciu akejkoľvek *a posteriori* kontroly – či už automatickej alebo na základe žiadosti dotknutej osoby – použitých opatrení na tajné sledovanie osôb, vykonávanej orgánom oddeleným od zložiek, ktoré tieto opatrenia realizovali. Súd poukázal na to, že tento prípad zároveň preukazuje, že sťažovateľ, ktorý sa dozvedel o odpočúvaní, nemal možnosť získať informácie o okolnostiach, za ktorých bolo nariadené, o jeho trvaní alebo o získaných poznatkoch, pretože informácie boli predmetom štátneho tajomstva a boli klasifikované ako „prísne tajné“, resp. boli zničené pred skončením trestného konania proti sťažovateľovi na základe interného predpisu ministra vnútra, ktorý bol tiež

utajovanou skutočnosťou. Sťažovateľ tak podľa názoru Súdu nepožíval minimálne záruky proti svojvoľným zásahom do jeho práv, a preto došlo k porušeniu článku 8 Dohovoru.

Požiadavka existencie *ex post* notifikačného mechanizmu v právnej úprave sa v ďalšom období natrvalo usadila v judikatúre Súdu. V už spomínanom prípade *Roman Zakharov v. Rusko* Súd kritizoval okrem iného účinnosť prostriedkov nápravy v súvislosti s odpočúvaním. Tieto boli dostupné iba osobe, ktorá bola schopná predložiť dôkaz o tom, že bola odpočúvaná, pričom získanie takéhoto dôkazu bolo nemožné v situácii, keď právna úprava neobsahovala žiaden mechanizmus oboznamovania osôb o odpočúvaní a ani žiadnu možnosť prístupu k informáciám o odpočúvaní. V nedávnom prípade *Szabó a Vissy v. Maďarsko* Súd výslovne poukázal na to, že možnosť dotknutých osôb domôcť sa účinnej ochrany proti svojvoľným zásahom do ich práv je nutne podmienená tým, že hneď, ako pominú dôvody sledovania alebo sa dosiahol jeho účel, musia sa osoby o tom, že boli sledované, dozvedieť. V uvedenom prípade právna úprava žiadny takýto mechanizmus neupravovala. Súd za týchto podmienok neakceptoval, že by úlohu kontroly mohol plniť bezpečnostný výbor parlamentu, ktorému je minister vnútra povinný dvakrát ročne predložiť správu o povolených sledovaniach, keďže táto správa nie je verejne prístupná a výbor nie je oprávnený nahliadať do jednotlivých spisov, a teda poskytovať nápravu v individuálnych prípadoch.

Záverom treba povedať, že slovenská právna úprava má v tomto smere tiež určité rezervy. Pri odpočúvaní, zázname telekomunikačnej prevádzky a sledovaní údajov prenášaných prostredníctvom počítačového systému, realizovaných v rámci trestného konania, príslušná právna úprava s určitými obmedzeniami obsahuje *ex post* notifikačný mechanizmus, resp. možnosť získať potrebné informácie nahliadnutím do spisu trestného konania.⁷ Pri odpočúvaní realizovanom mimo rámca trestného konania podľa zákona č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov (zákon o ochrane pred odpočúvaním) právna úprava za žiadnych okolností neukladá príslušným orgánom povinnosť oboznámiť dotknutú osobu *a posteriori* s tým, že bola odpočúvaná.⁸ Napriek existencii účinných prostriedkov nápravy v slovenskom právnom poriadku, ktorými možno dosiahnuť preskúmanie uskutocnených tajných opatrení na sledovanie osôb a v prípade neoprávnenosti tohto zásahu získať odškodnenie, tak v niektorých prípadoch dotknutá osoba zostáva bez reálnej možnosti ich využiť, keďže sa o použití spomínaných opatrení voči nej nedozvie.⁹

⁷ Pozri § 115 ods. 6 a ods. 8 až 11 a 116 ods. 3 až 6 zákona č. 301/2005 Z. z. Trestný poriadok.

⁸ Pozri § 8 a 9 zákona č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov (zákon o ochrane pred odpočúvaním).

⁹ K tomu bližšie pozri aj Bálintová, M.: *Záruky proti zneužitiu odpočúvania*. Justičná revue, 60, 2008, č. 10, s. 1351–1358.

Ústavné hranice využívania informačno-technických prostriedkov v trestnom konaní

Constitutional Limits of Using Information-technology in Criminal Proceeding

Ján Svák¹

Abstrakt: Ústavné hranice využívania informačno-technických prostriedkov v trestnom konaní sú chápané predovšetkým z pohľadu štádia súdneho konania trestného, ktoré sa stále považuje za vyvrcholenie a rozhodujúcu fázu trestného konania. Autor vo svojom vystúpení poukazuje na tendencie rozhodovacej činnosti Európskeho súdu pre ľudské práva do práva na súkromia použitím dôkazu získaného použitím informačno-technických prostriedkov.

Abstract: The constitutional limits of using of information technology in criminal proceeding are taken primarily from the perspective of the stage of trial proceedings of which is still considered to be the culmination of a crucial phase of the criminal proceeding. The author highlights the tendency of the decision-making activities of the European Court of Human Rights on the right to privacy, by using of evidence obtained through the information technology.

Kľúčové slová: Ústava, trestné konanie, právo na súkromie, rozhodujúci dôkaz

Key word: Constitution, Criminal proceeding, Right to privacy, Decisive evidence

Ústava Slovenskej republiky (ďalej „ústava“) v širšom slova zmysle v oblasti ľudských práv inkorporuje do svojho obsahu aj rozhodnutia Ústavného súdu Slovenskej republiky (ďalej „ústavný súd“) a rozhodnutia Európskeho súdu pre ľudské práva (ďalej „ESLP“), ktoré sú základnou pramennou bázou pre určovanie ústavných hraníc využívania informačno-technických prostriedkov (ďalej „ITP“) v trestnom konaní. To je prvá tzv. rozširujúca poznámka vo vzťahu k predmetu konferencie.

Druhá, naopak, zužujúca poznámka sa dotýka vymedzenia pojmu „trestné konanie“. Ústavné hranice budú v ďalšom chápané predovšetkým z pohľadu súdneho štádia trestného konania, ktoré stále považujem za vyvrcholenie a rozhodujúcu fázu trestného konania aj keď z určitého pohľadu na efektívnosť súdneho rozhodovania ním môže byť exekučné konanie. Napriek tomu, že sa budem zaoberať úplne začiatočnou fázou, a to prijatím právnej úpravy v oblasti používania (využívania) ITP z hľadiska jej ústavnoprávnej kvality, tak ústavné hranice posuniem do aplikáčnej fázy a budem sa zaoberať dôkazom získaným ITP očami sudcu, ktorý rozhodne o jeho prípustnosti pri určovaní viny alebo nevinu obžalovaného. Pripomínam, že pred očami tohto súdu je zároveň § 2 ods. 2 zákona č. 385/2000 Z. z. o sudcoch a prísediacich a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, ktorý mu prikazuje, aby rozhodoval „nestranne, spravodlivo, bez zbytočných prietahov a len na základe skutočností zistených v súlade so zákonom“. Tu si kladiem asi tú najzávažnejšiu otázku, ktorá je až zarážajúco paradoxná, a to či zákonne získaným dôkazom sa má na mysli aj dôkaz získaný síce zákonným spôsobom, ale zároveň protiústavným. Inými slovami môže byť v zhode s právom na spravodlivé súdne konanie použitie dôkazu získaného tým, že sa poruší iné ústavné právo? V prípade použitia dôkazov

¹ Prof. JUDr. Ján Svák, DrSc., Fakulta práva, Paneurópska vysoká škola v Bratislave, e-mail: jan.svak@paneurouni.com.

získaných ITP môže ním byť v prvom rade právo na súkromie, ktoré síce *expressis verbis* takto pomenované v ústave nie je, ale vyplýva minimálne z takto označeného čl. 8 Dohovoru o ochrane ľudských práv a základných slobôd (ďalej „Dohovor“), čo opakovane konštatuje aj ústavný súd.²

Rozhodovacia prax EŠP je v prípade využívania dôkazov pred vnútroštátnymi súdmi už od precedenčného rozhodnutia vo veci *Schenk*³ pomerne benevolentná. Vychádza v zásade zo štyroch princípov, a to

- širokej miery voľnej úvahy štátu (ponecháva predovšetkým na vyhodnotení sudcu vnútroštátneho súdu, či predmetný dôkaz využije ako relevantný dôkazný prostriedok z pohľadu vnútroštátneho právneho poriadku),
- absencie povinnosti z čl. 6 Dohovoru (právo na spravodlivý súdny proces) pre EŠP hodnotenia prípustnosti dôkazov ako takých, ale „len“ potreby preskúmania či v konkrétnom trestnom konaní boli dodržané základné pravidlá spravodlivého súdneho procesu,
- prioritného posúdenia toho, či v predmetnom trestnom konaní bolo zabezpečené právo na obhajobu, najmä z hľadiska jeho kontradiktórnosti (v tomto smere je určujúce ako a v akom rozsahu sa mohol obvinený, resp. jeho obhajca vyjadriť k inkriminovanému dôkazu a spochybniť ústavnosť či zákonnosť spôsobu jeho získania),
- širšieho pohľadu na okolnosti prípadu, či už z pohľadu verejného záujmu na zachovaní bezpečnosti štátu a jeho boja proti kriminalite, ale aj z hľadiska zachovania ľudských práv jednotlivca, ktoré sú garantované Dohovorom.

Z týchto princípov vychádzal (a nateraz ich teda nemá dôvod ani meniť) aj v nedávnom prípade *Bašić*,⁴ kde rozhodol, že bol porušený čl. 8 Dohovoru lebo súdne odôvodnenie príkazu na odpočúvanie a záznam telekomunikačnej prevádzky sťažovateľa v rámci jeho tajného sledovania nezodpovedalo zásade zákonnosti a primeranosti v konkrétnom prípade. EŠP nepovažoval za odôvodnenie príkazu len suché konštatovanie vnútroštátneho súdu, že „*zadováženie dôkazných prostriedkov nemohlo byť vykonané iným spôsobom, pretože by tým bolo zmarené objasnenie trestného činu*“. EŠP chýbalo najmä zdôvodnenie toho, prečo vyšetrovanie nemohlo byť vykonané inými, menej rušivými prostriedkami.

Na druhej strane však EŠP nevidel porušenie čl. 6 Dohovoru, ktoré sťažovateľ namietal z dôvodu, že bol uznaný vinným výlučne na dôkazoch získaných nezákonným spôsobom a ako sám aj konštatoval, pri porušení práva na súkromie sťažovateľa chráneného čl. 8 Dohovoru. EŠP vzal do úvahy najmä skutočnosť, že sťažovateľ mal možnosť napadnúť spôsob získania dôkazov v rámci samotného trestného konania a že v danej veci boli vypočutí príslušní policajti, ktorí „ozrejmili“ spôsob získania a zdokumentovania nahrávok z odpočúvania. Za dôležitý prvok pre posúdenie spravodlivosti súdneho procesu EŠP nepovažoval skutočnosť, že predmetné dôkazy získané tajným sledovaním boli východiskovými pre začatie trestného konania (išlo o podozre-

² V rozhodnutí č. I. ÚS 13/2000 ústavný súd konštatuje, že: „Ústava pojem ‚súkromný a rodinný život‘ ani ‚obydlie‘ bližšie nedefinuje. Nakoľko základné práva a slobody podľa ústavy je potrebné vykladať a uplatňovať v zmysle a duchu medzinárodných zmlúv o ľudských právach a základných slobodách (PL. ÚS 5/93, PL. ÚS 15/98), ústavný súd pri vymedzení obsahu uvedených pojmov prihliadal aj na príslušnú judikatúru týkajúcu sa predovšetkým čl. 8 ods. 1 Dohovoru o ochrane ľudských práv a základných slobôd (ďalej len ‚dohovor‘).“

³ Rozhodnutie vo veci *Schenk c. Švajčiarsko* zo dňa 12. júla 1988 týkajúce sa sťažnosti č. 10862/84. Z neskorších rozhodnutí formulujúcich základné princípy využiteľnosti „pochybných“ dôkazov v trestnom konaní možno pripomenúť rozhodnutia EŠP vo veciach *Khan c. Spojené kráľovstvo* z 12. mája 2000 týkajúce sa sťažnosti č. 35397/97, *P.G. a J.H. c. Spojené kráľovstvo* z 25. septembra 2001 týkajúce sa sťažnosti č. 44787/98, *Allan c. Spojené kráľovstvo* z 5. novembra 2002 týkajúce sa sťažnosti č. 48539/99, *Bykov c. Rusko* z 10. marca 2009 týkajúce sa sťažnosti č. 4378/02, *Fomin c. Moldavsko* z 11. októbra 2011 týkajúce sa sťažnosti č. 36755/06.

⁴ Rozhodnutie vo veci *Bašić c. Chorvátsko* zo dňa 25. októbra 2016 týkajúce sa sťažnosti č. 22251/13.

nie z účasti na organizovanom obchodovaní s drogami) a „rozhodujúcimi“ aj pre jeho uznanie viny a odsúdenie. Práve objasnenie významu „rozhodujúci“ dôkaz má z hľadiska skúseností získaných v minulosti na našom území s aplikáciou tzv. vyšinského teórie korunného dôkazu osobitné posolstvo.

Pojem „rozhodujúci dôkaz“ sa pokúsil v zostave Veľkej komory ozrejmiť v prípade *Al-Khawaja a Tahery*⁵ a to tým spôsobom, že za rozhodujúci sa označuje dôkaz tak významný alebo dôležitý, že ho je možné považovať za určujúci pre výsledok konania. Keď v skoršom prípade *Heglas*⁶ ešte ESLP požadoval, okrem dôkazu získaného tajným odpočúvaním v rozpore s čl. 8 Dohovoru, aj ďalšie dôkazy, tak v prípade *Bašić* tými ďalšími dôkazmi boli výpovede svedkov, ktorí tajné sledovanie uskutočnili, čo už je na hranici toho, že za korunný (rozumej ako jediný) dôkaz môže byť považovaný dôkaz získaný ITP, ktorého hodnovernosť potvrdia ako svedkovia v rámci kontradiktórneho konania tí, ktorí sťažovateľa tajne sledovali.

Pri posudzovaní toho, či použitím ITP bolo porušené právo na súkromie je však ESLP už oveľa prísnejší a vyžaduje „zákonnosť“ ich získania. Zákonné podmienky pre využitie ITP sú len pre pripomenutie v zmysle ustálenej judikatúry ESLP, v zásade tri, a to

- existencia vnútroštátneho zákona,
- prístupnosť zákona a
- predvídateľnosť zákona v súlade s medzinárodným právom, čo predstavuje kvalitatívnu stránku zákona.

Problematickou je spravidla tretia podmienka, ktorú v konkrétnom prípade testuje ESLP z pohľadu čl. 8 Dohovoru pri posudzovaní zákonnosti vydania príkazu na tajné sledovanie a jeho realizácie. V zhode s J. Kratochvílom možno medzi tieto zákonné podmienky a požiadavky na tajné sledovanie zaradiť

- vymedzenie okruhu tajne sledovaných osôb,
- reštriktívne určenie okruhu tajne sledovaných osôb,
- časové obmedzenie (s možnou prolongáciou) tajného sledovania, ktoré osobitne je dôležité pri tajnom odpočúvaní,
- proces vyhodnocovania, použitia a sledovania získaných informácií, najmä konkrétnych dát,
- opatrenia, ktoré je potrebné prijať pri predávaní dát iným osobám,
- okolnosti, za ktorých môžu byť, resp. musia byť dáta zničené,
- prostriedky, ktoré majú byť pri tajnom sledovaní použité a tiež postupy pri ich dodržiavaní,
- účinná vonkajšia kontrola,
- informovanie tajne sledovaných osôb, napr. o tom, že boli tajne odpočúvané.⁷

Kvalita ústavnosti zákona je testovaná jednak vo všeobecnosti, a to spravidla pri abstraktnej kontrole ústavnosti vnútroštátnym ústavným súdom a jednak *in concreto* pri preskúmvaní sťažností najmä na porušenie čl. 8 Dohovoru, pričom rozhodnutia ESL sa už tradične prenášajú aj do zmien vnútroštátneho právneho poriadku.

Test ústavnosti zákona z pohľadu ústavnosti súdu možno zdokumentovať na dvoch príspevkoch z posledného obdobia, ktoré pracovne označme ako „mobily“ a „biele kone“.

⁵ Rozhodnutie vo veci *Al-Khawaja a Tahery c. Spojené kráľovstvo* z 15. decembra 2011 týkajúce sa sťažnosti č. 26766/05 a 22228/06.

⁶ Rozhodnutie vo veci *Heglas c. Česká republika* z 1. marca 2007 týkajúce sa sťažnosti č. 5935/02.

⁷ Porovnaj Kmec, J., Kosař, D., Kratochvíl, J., Bobek, M.: *Evropská úmluva o lidských právech. Komentář*. 1. vydání. Praha: C. H. Beck, 2012, s. 922.

V prípade „mobily“ išlo o pomerne mediálne známu zákonnú povinnosť poskytovateľa elektronických komunikácií uchovávať prevádzkové údaje, lokalizačné údaje a údaje komunikujúcich strán odo dňa uskutočnenia komunikácie počas 6 mesiacov, ak ide o pripojenie k internetu, internetovú elektronickú poštu a telefonovanie prostredníctvom internetu, a počas 12 mesiacov, ak ide o ostatné komunikácie.

Skupine poslancov, ktorá podávala ústavný podnet sa nepozdávalo najmä to, že *„každý deň je o každom obyvateľovi Slovenska povinne zaznamenané kto s kým telefonoval, komu posielal textové správy a emaily, kedy tak urobil, kde sa vtedy nachádzal, aký telefón alebo službu použil, ako dlho trvala predmetná komunikácia a mnoho ďalších. Kombináciou týchto informácií dokážeme opísať pohyb každého obyvateľa na Slovensku, ktorý používa mobilný telefón či internet, predpovedať jeho správanie, okruh známych, záľuby, zdravotný stav, sexualitu, či iné osobné údaje a tajomstvá... Na základe údajov, ktoré sa takto uchovávajú, je možné zostaviť dokonalý osobnostný, komunikačný a pohybový profil jednotlivca, odhaľujúci radu podstatných charakteristík jeho identity a chovania, inými slovami odhaľujú podstatnú časť jeho súkromia.“*

Podobne ako v prípadoch, ktoré rozhodoval Ústavný súd Českej republiky,⁸ konštatovali, že *„... v konkrétnom prípade môže byť tak zásah do súkromia závažnejší, pokiaľ pôjde o uchovávanie a využívanie prevádzkových a lokalizačných údajov, ako keby išlo o uchovávanie obsahu komunikácie...“* (bod 14 rozhodnutia ÚS SR č. PL. ÚS 10/2014).

Ústavný súd Slovenskej republiky v zhode s konštantnou judikatúrou ESLP⁹ ako aj Súdneho dvora Európskej únie¹⁰ konštatoval, že ide o významný zásah do práva na súkromie, ktorý plní aj legitímny cieľ (užitočný nástroj pre účely vyšetrovania, odhaľovania a stíhania závažnej trestnej činnosti, avšak *„napadnuté ustanovenia neobstoja v druhom kroku testu proporcionality, lebo nepodmieňujú zisťovanie údajov o uskutočnenej komunikačnej prevádzke zo strany orgánov činných v trestnom konaní požiadavkou nevyhnutnosti a pre ich aplikáciu neustanovujú účinné prostriedky kontroly, ktoré by umožňovali účinnú ochranu základného práva na informačné sebaurčenie dotknutých osôb v priebehu celého obdobia, počas ktorého tieto orgány disponujú predmetnými údajmi. Pre úplnosť posúdenia ústavnosti napadnutých ustanovení je potrebné uviesť, že by neprešli ani cez tretí krok testu proporcionality, ktorého podstatou je posúdenie proporcionality v užšom zmysle.“* (bod 138).

V druhom prípade „biele kone“, ktoré je zaujímavé pre ústavné právo aj z pohľadu určenia hranice medzi abstraktnou a konkrétnou kontrolou ústavnosti sťažovateľ podal na Najvyššom

⁸ Porovnaj k tomu rozhodnutia Ústavného súdu Českej republiky č. PL. ÚS 24/10, PL. ÚS 42/11 a I. ÚS 631/05, ktoré konštatovali, že je nevyhnutné, aby prijaté opatrenia zasahujúce do práva na súkromie obsahovali adekvátne záruky ochrany pred zneužitím, čo sa pre jednotlivcov stáva naliehavejším práve v dnešnej dobe, kedy vďaka enormnému rozvoju a výskytu nových informačných technológií a elektronickej komunikácie (v tzv. kyberpriestore) je predovšetkým vďaka rozvoju internetu a mobilnej komunikácie každú minútu zaznamenávané zhromažďované a fakticky prístupňované enormné množstvo dát, údajov a informácií, ktoré zasahujú aj do súkromnej sféry každého jednotlivca, a to aj napriek tomu, že on sám do nej vedome nikoho pustiť nechce.

⁹ Odvolal sa pri tom najmä na rozsudky vo veci *Amann c. Švajčiarsko* zo 16. februára 2000 týkajúce sa sťažnosti č. 27798/95 a *Rotaru c. Rumunsko* zo 4. mája 2000 týkajúce sa sťažnosti č. 28341/95.

¹⁰ Rozsudok *Digital Rights Ireland Ltd. proti Minister for Communications, Marine and Natural Resources a iní c. Kärtner Landesregierung a iní*, C-293/12 a C-594/12, EU:C:2014:238, bod. 37. V zmysle týchto rozhodnutí existuje spojitosť medzi právom na súkromie podľa čl. 7 Charty základných práv EÚ a právom na ochranu osobných údajov podľa čl. 8 Charty spočíva v koncepte **informačného sebaurčenia**, ktorý implikuje nutnosť existencie kontroly jednotlivca nad informáciami dotýkajúcimi sa jeho osoby. Koncept informačného sebaurčenia spočíva v nároku jednotlivca určiť, kedy, ako a v akom rozsahu budú informácie o ňom sprístupnené ostatným. Súdny dvor EÚ v týchto rozsudkoch tiež konštatoval, že značná intenzita zásahu do práva na súkromie je daná rovnako skutočnosťou, že uchovávané údaje a ich neskoršie použitie bez toho, aby účastník alebo registrovaný užívateľ boli o tom informovaní, môže v povedomí dotknutých osôb vyvolať pocit, že ich súkromný život je predmetom neustáleho sledovania.

súde Slovenskej republiky žalobu voči Finančnému riaditeľstvu Slovenskej republiky a Kriminálnemu úradu finančnej správy podľa § 250v OSP ako prostriedok ochrany pred nezákonným zásahom v súvislosti s tým, že uvedené orgány štátnej správy vedú sťažovateľa v zozname „BIELE KONE“. Ako z tvrdení sťažovateľa vyplýva, uvedený zoznam „bielych koní“ obsahuje zoznam fyzických osôb, ktoré podľa žalovaných orgánov verejnej správy majú predstavovať „biele kone“ s tým, že k jednotlivej fyzickej osobe je spravidla priradená právnická osoba, resp. právnické osoby, v ktorých má byť „biely kôň“ činný, aj s uvedením rodného čísla „bieleho koňa“, daňového identifikačného čísla daňového subjektu a ďalších údajov. Uvedený zoznam „bielych koní“ podľa tvrdenia sťažovateľa Finančné riaditeľstvo a jemu podriadené daňové úrady, ako aj Kriminálny úrad finančnej správy používajú pri svojej činnosti a disponujú s ním najmä daňoví kontrolóri. Sťažovateľ je v daňových konaniach správcom dane ako „biely kôň“ aj vyhodnocovaný. Žaloba sťažovateľa bola najvyšším súdom zamietnutá.

Ústavný súd jednak „poučil“ najvyšší súd, že súdne precedensy ESLP sú prameňom slovenského ústavného práva a mal sa s nimi zaoberať v odôvodnení svojho rozhodnutia¹¹ a jednak ho usmernil, že „podstatné a relevantné pre uplatnenie účinnej a efektívnej ochrany základného práva na súdnu ochranu v spojení so základným právom na ochranu súkromia v rozsahu ochrany osobných údajov boli otázky:

- či je legitímne viesť zoznam „bielych koní“ (teda či je legitímne zhromažďovať a zoraďovať údaje o osobách na účel, pre ktorý sa vedie zoznam „bielych koní“)
- či konajúce orgány štátu majú právomoc viesť predmetný zoznam
- či právna úprava, podľa ktorej sa zoznam „bielych koní“ vedie, má kvalitu predpísanú Dohovorom a Ústavou, teda či orgány štátu
 - (i) aplikovali právnu úpravu, ktorej kvalita zaručovala obmedzenie ústavnej ochrany osobných údajov iba z legitímnych dôvodov,
 - (ii) aplikovali právnu úpravu, ktorá zaručuje obmedzenie ústavnej ochrany osobných údajov iba po určený čas,
 - (iii) aplikovali právnu úpravu, ktorá umožňuje súdny prieskum obmedzenia ústavnej ochrany osobných údajov
- či sa zoznam „bielych koní“ vedie v súlade s platnou právnou úpravou
- či zaradenie konkrétnej osoby (žalobcu) do tohto zoznamu je legitímne.“¹²

Prípád „biele kone“ opätovne potvrdzuje snahu orgánov ochrany ústavnosti o to, aby všeobecné súdy venovali osobitnú pozornosť dodržiavaniu záruk práva na súkromie pri zhromažďovaní a zbere údajov využiteľných pre účely trestného konania (v tomto prípade správneho trestného súdnictva), ale rovnako nedáva jasnú odpoveď, či by použitie dôkazov získaných protiústavným spôsobom mohlo byť využiteľné v následnom konkrétnom trestnom konaní na súde, ak by boli dodržané minimálne záruky spravodlivého súdneho procesu. Je možné pred-

¹¹ Ústavný súd pripomenul, že ESLP Európsky súd pre ľudské práva o použití informačno-technických prostriedkov dohľadu štátnymi orgánmi spôsobom znamenajúcim obmedzenie práva na súkromie uviedol, že prostriedky tajného dohľadu nad občanmi, ktoré sú typické pre policajný štát, sú tolerovateľné podľa Dohovoru len vtedy, ak sú striktné nevyhnutné na ochranu demokratických inštitúcií (*Klass and Others v. Germany*, séria A, č. 28, bod 41). Túto výnimku, podľa ESLP, opodstatňujú dve okolnosti: prvou je technický pokrok zaznamenaný vo vývoji špiónážnych prostriedkov a následne aj v prostriedkoch kontrašpiónážneho dohľadu; druhou okolnosťou je rozmach terorizmu v Európe. V dôsledku týchto okolností sa demokratické zriadenia ocitajú v ohrození. Aby im štát mohol vzdorovať a účinne predchádzať, musí mať možnosť podrobiť tajnému dohľadu podozrivé živly pôsobiace vo sfére jeho jurisdikcie. Vzhľadom na to ESLP uznal, že existencia právnej úpravy, ktorou sa vytvára možnosť uplatnenia tajného dohľadu nad poštovými zásielkami a telekomunikáciami za výnimočných podmienok, je nevyhnutná v demokratickej spoločnosti v záujme národnej bezpečnosti a/alebo na predchádzanie nepokojom a zločinosti (*Klass and Others v. Germany*, séria A, č. 28, bod 41).

¹² Rozhodnutie Ústavného súdu SR č. III. ÚS 400/2016.

pokladať, že aplikácia pravidiel „rozhodujúceho dôkazu“ by v prípade jeho získania zo zdrojov napojených na prípady „mobily“ a „biele kone“ bola ťažko aplikovateľná. Iná situácia by zrejme bola keby tieto zdroje boli podkladom pre použitie ITP a dôkazy získané na ich základe by boli využité v konkrétnom konaní pred súdom, kde by sa všeobecné súdy riadili aktuálnou judikatúrou ESLP k čl. 6 Dohovoru.

Odposlech a záznam telekomunikačního provozu v České republice – záruky přezkoumání zákonnosti příkazu k odposlechu

The Interception and Recording of Telecommunications in the Czech Republic – the Legal Guarantees of the Reviewing of the Interception Order

Jiří Jelínek¹

Abstrakt: Článek pojednává o právní úpravě odposlechu a záznamu telekomunikačního provozu v české trestněprocesní úpravě. Tato úprava je obsažena v ustanovení § 88 tr. řádu. Autor nejprve vymezuje pojem a zákonné podmínky pro provedení odposlechu telekomunikačního prostředku a podmínky pro použití záznamu o provedeném odposlechu jako důkazu v trestním řízení. V další části se uvádí nedostatky české právní úpravy obsažené v trestním řádu. Poslední část je věnována oprávnění odposlouchávané osoby požádat dodatečně, po skončeném odposlechu, Nejvyšší soud o přezkoumání zákonnosti příkazu k provedení odposlechu a zákonnosti vlastního provedeného odposlechu. Autor soudí, že de lege ferenda by bylo žádoucí zavést možnost nezákonně odposlouchávané osoby napadnout mimořádným opravným prostředkem meritorní rozhodnutí, vzešlé z nezákonných odposlechů.

Abstract: The article deals with legislation on interception and recording of telecommunications in Czech criminal procedural law. This legislation is to be found in the § 88 of the Criminal Procedure Code. First the author defines the term of and legal conditions for the interception of telecommunications as well as the use of the record of the interception as an evidence in criminal proceedings. In the next part the author shows the deficiencies of the Czech legislation in the Criminal Procedure Code. The last part deals with the right of the subject of the interception to ask the Supreme Court to review the legality of the interception order and also of the performed interception itself. The author's opinion is that there should be embedded the possibility of the subject of illegal interception to defend himself by an extraordinary appeal against unlawful decision which was based on illegal interceptions.

Klíčová slova: Trestní řízení, odposlech a záznam telekomunikačního provozu, přezkoumání zákonnosti nařízeného odposlechu, mimořádné opravné prostředky.

Key words: criminal procedural law, the interception and recording of telecommunications, the review of the legality of the interception order, the extraordinary appeals.

Úvodem

Odposlech a záznam telekomunikačního provozu (§ 88 tr. řádu) představují jednu ze dvou skupin zajišťovacích úkonů prováděných v souvislosti s telekomunikačním provozem. Druhou skupinou pak je zjišťování údajů o uskutečnění telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat (§ 88a tr. řádu).

Oproti odposlechu a záznamu prováděnému podle § 88 tr. řádu, kdy se sleduje vlastní telekomunikační provoz, o jehož obsahu se pořizuje záznam, ustanovení § 88a tr. řádu se vztahuje na údaje o telekomunikačním provozu již v minulosti uskutečněném (tj. „neodposlouchávaném“).

¹ Prof. JUDr. Jiří Jelínek, CSc., Právnická fakulta, Univerzita Karlova v Praze, jelinek@prf.cuni.cz.

Jde o údaje, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat (např. volající a volané číslo).

Rozdíl mezi oběma skupinami spočívá dále v tom, že zatímco odposlech a záznam telekomunikačního provozu směřují do budoucna, zjišťování údajů o uskutečněném telekomunikačním provozu směřuje k zjištění údajů již uskutečněných.

Tento příspěvek se zabývá první z uvedených skupin, a to především ve světle současné české právní úpravy a soudní judikatury související s otázkou zákonnosti příkazu k odposlechu.

Odposlech telekomunikačního provozu v trestním řízení představuje závažný zásah do ústavně zaručených práv a svobod jednotlivce. Na druhé straně záznam odposlechu telekomunikačního provozu patří k jednomu z nejpoužívanějších důkazů v trestním řízení, přičemž při stíhání některých zvláštních forem trestné činnosti, zejména rozsáhlé organizované kriminality, typicky u drogových deliktů, bývá dokonce důkazem klíčovým a nezastupitelným.

Odposlech je vážným zásahem do práv a svobod jednotlivce proto, že se jedná o zásah do práva na ochranu soukromého a rodinného života ve smyslu čl. 8 odst. 1 Evropské úmluvy o ochraně lidských práv, kdy toto právo zahrnuje také ochranu korespondence. Sama Úmluva ovšem v čl. 8 odst. 2 připouští zásah státního orgánu do uvedeného práva tehdy, kdy je to v souladu se zákonem a nezbytné 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.

Z uvedeného vyplývá, že k zásahu může dojít pouze na základě zákona, přičemž takový zásah musí být zároveň i nezbytným k naplnění některého z uvedených zájmů. Nezbytnost jakožto předpoklad provedení zásahu pak vyjadřuje jeho subsidiaritu a charakter *ultima ratio* mezi prostředky, jež mají státní orgány při plnění svých úkolů k dispozici. Jelikož jsou obě podmínky v článku 8 odst. 2 Úmluvy vyjádřeny kumulativně, je nutné dodržet zásadu subsidiarity vždy, a to bez ohledu na konkrétní zákonnou úpravu členského státu Rady Evropy.

Právo na ochranu soukromí a na ochranu tajemství dopravovaných listin pak nalezneme zakotveno také na úrovni českého ústavního pořádku *stricto sensu*, a to v článku 10 odst. 1, odst. 2 a dále v článku 13 Listiny základních práv a svobod. Článek 7 odst. 1 Listiny pak zdůrazňuje, že nedotknutelnost osoby a jejího soukromí je zaručena, přičemž k omezení může dojít jen v případech stanovených zákonem.

Jedním z případů omezení stanovených zákonem ve smyslu shora uvedeného článku 7 odst. 1 Listiny a článku 8 odst. 2 Úmluvy je právě odposlech telekomunikačního provozu upravený v ustanovení § 88 tr. řádu. Ustanovení § 88 odst. 1 tr. řádu pak konkrétně stanoví, že *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, může být vydán příkaz k odposlechu a záznamu telekomunikačního provozu, pokud lze důvodně předpokládat, že jím budou získány významné skutečnosti pro trestní řízení a nelze-li sledovaného účelu dosáhnout jinak nebo bylo-li by jinak jeho dosažení podstatně ztíženo. Odposlech a záznam telekomunikačního provozu provádí pro potřeby všech orgánů činných v trestním řízení Policie České republiky. Provádění odposlechu a záznamu telekomunikačního provozu mezi obhájcem a obviněným je nepřípustné. Zjistí-li policejní orgán při odposlechu a záznamu telekomunikačního provozu, že obviněný komunikuje se svým obháj-*

cem, je povinen záznam odposlechu bezodkladně zničit a informace, které se v této souvislosti dozvěděl, nijak nepoužít. Protokol o zničení záznamu založí do spisu.

Zákonodárce citovanou formulací *nelze-li sledovaného účelu dosáhnout jinak nebo bylo-li by jinak jeho dosažení podstatně ztíženo* vyjadřuje subsidiaritu takového postupu ve smyslu čl. 8 odst. 2 Úmluvy, a to v souladu se zásadou přiměřenosti a zdrženlivosti vymezenou v § 2 odst. 4 tr. řádu. Jde o omezující podmínku nařízení odposlechu a záznamu telekomunikačního provozu na případy, kdy nelze sledovaného účelu dosáhnout jinak nebo kdy by bylo jeho dosažení ztíženo.

Odposlechem telekomunikačního provozu se rozumí odposlech telefonních hovorů z pevné linky i odposlech obdobných přístrojů – faxu, vysílačky, mobilního telefonu či jiného telekomunikačního zařízení. Nutno podotknout, že zákon neupravuje tzv. prostorový odposlech. Odposlech se týká jak veřejné telekomunikační sítě, tak i podnikových (vnitřních) sítí. Ochrana ústavně zaručených práv a svobod se přitom vztahuje na všechny osoby účastníci se telekomunikačního provozu.

S ohledem na závažnost zásahu do ústavně zaručených práv a svobod byl vytvořen rámec záruk chránících před zneužitím odposlechu telekomunikačního provozu v trestním řízení. Za takovéto záruky lze považovat:

- a) definování trestných činů, při jejichž vyšetřování může být odposlech proveden, stejně jako definování osob, které mohou být odposlouchávány,
- b) stanovení doby trvání odposlechu,
- c) stanovení náležitostí příkazu k odposlechu včetně pravidel pro provádění odposlechu,
- d) stanovení pravidel nakládání se záznamem včetně podmínek, za kterých se uskutečněné záznamy zničí,
- e) možnost kontroly zákonnosti provedeného odposlechu a záznamu.

Co je telekomunikačním provozem, stanoví v České republice zák. č. 151/2000 Sb., o telekomunikacích a o změně dalších zákonů (§ 2 odst. 5 cit. zák.). Je jím přepravování nebo směrování informací telekomunikačními zařízeními a sítěmi. Např. jde o provoz telefonu (mobilního i pevného), telefaxu, dálnopisu, vysílačky, elektronické pošty (e-mail). Srov. též zák. č. 127/2005 Sb., o elektronických komunikacích.

Citovaný zákon také stanoví, co se rozumí telekomunikačním tajemstvím (§ 84 odst. 3 cit. zák.). Jsou jimi obsah zpráv přepravovaných nebo jinak zprostředkovaných telekomunikačními zařízeními a sítěmi s výjimkou zpráv určených veřejnosti, provozní doklady, z jejichž obsahu je zjevný obsah přepravovaných zpráv, data související s poskytováním telekomunikační služby, zejména údaje o účastnících telekomunikačního spojení.

Telekomunikační provoz zahrnuje nejen komunikaci s využitím telefonu, telefaxu, mobilního telefonu, vysílačky a jiného telekomunikačního zařízení, ale i zasílání zpráv elektronickou poštou, přičemž prostřednictvím mobilních telefonů lze při využívání internetového připojení rovněž odesílat a přijímat e-maily, tedy využívat jednu z forem elektronické pošty.

Nařízení předsedy senátu (soudce) ke zjištění údajů o telekomunikačním provozu má formu písemného a odůvodněného příkazu; tedy jde o rozhodnutí *sui generis*, proti němuž není přípustný opravný prostředek.

Požadované údaje o uskutečněném telekomunikačním provozu musí být přesně uvedeny v tomto příkazu. Lze požadovat např. seznam příchozích a odchozích hovorů, použitý druh služby, datum, čas, dobu trvání komunikace, místo připojení, místo, odkud bylo voláno.

V praxi v České republice jednoznačně převažuje odposlech mobilních telefonů, přičemž pacatelé využívají dostupnosti mobilních telefonů a snadné výměny volacích čísel prostřednic-

tím výměny SIM karet. Tato čísla velmi často mění, a proto jsou také často nařízené odposlechy ukončovány a vydávány příkazy na nová volací čísla u stejných pachatelů.

Zpráva o uskutečněném telekomunikačním provozu, kterou vypracuje povinný subjekt, tj. držitel telekomunikační licence, je listinným důkazem, který se v řízení před soudem přečte. Předseda senátu nebo soudce, kteří příkaz vydali v něm musí označit orgán činný v trestním řízení, kterému mají být údaje požadované příkazem sděleny.

1. Některé problémy české právní úpravy odposlechu a záznamu telekomunikačního provozu a použití záznamu o odposlechu

Smyslem ustanovení § 88 českého tr. řádu o odposlechu a záznamu telekomunikačního provozu je možnost seznámit se s obsahem dopravovaných zpráv v elektronické podobě, tedy s obsahem tzv. telekomunikačního provozu. Problémem je, že zákonné sousloví „telekomunikační provoz“ již dnes nepostihuje všechny v úvahu přicházející formy elektronických komunikací uskutečňovaných v sítích elektronických komunikací, kam náleží nejen komunikace prostřednictvím veřejných telefonních sítí, ale i jiné služby elektronických komunikací, zejména ty, které se uskutečňují prostřednictvím internetových sociálních sítí či aplikací (Facebook, Skype etc.). Při nedostatku speciální právní úpravy pro různé formy elektronické komunikace se používá toto obecné ustanovení i pro zjištění obsahu e-mailů došlých a uschovaných v e-mailové schránce, a to i včetně fotografií, buď v určitém okamžiku, nebo v určitém období. Pro tento účel se podle našeho mého názoru nepoužije ustanovení § 158d odst. 3 tr. řádu, které míří na jiné případy.

De lege ferenda by bylo žádoucí, kdyby právní úprava v trestním řádu, která je z hlediska použité terminologie i jinak v oblasti komunikačních a informačních technologií zastaralá, a tím do jisté míry i neoperativní, byla v trestním řádu nahrazena co nejjednodušším a obecným vymezením, tak aby bylo jasné, pod jaký pojem lze jaký druh komunikace podřadit, aby to nečinilo problémy ani orgánům činným v trestním řízení, ale ani obhajobě při uplatňování svých práv.

V ustanovení § 88 českého tr. řádu je upraven pouze odposlech telekomunikačního provozu. Toto ustanovení se tedy netýká tzv. prostorového odposlechu (odposlechu hovoru v bytě, v restauraci, ve volném prostoru). Ke škodě věci trestní řád tzv. prostorový odposlech neupravuje, což správné není a de lege ferenda by to mělo být výslovně upraveno. Praxe si při nedostatku výslovné právní úpravy odposlechu „vypomáhá“ ustanovením § 158d odst. 3 tr. řádu, které jak již bylo řečeno shora, míří na jiné případy. Je tomu tak proto, že odposlech a záznam telekomunikačního provozu je zajišťovacím institutem, který je sice svoji povahou a zejména účelem blízký operativně pátracím prostředkům, ale operativně pátrací prostředek to není. Proto soudím, že všechny typy či druhy odposlechu by měly být upraveny na jednom místě v trestním řádu.

Dalším nedostatkem právní úpravy je, že výslovně neupravuje důsledky neoprávněného zveřejnění obsahu byť legálně pořízeného odposlechu, což některé sdělovací prostředky vede k tomu, že toto běžně a třeba i opakovaně v jedné kauze činí. Zveřejňování obsahu odposlechů opatřených v trestním řízení (v souladu s § 88 tr. řádu) nebo jejich přehrávání ve sdělovacích prostředcích (bez ohledu na to, zda obsah odposlechů je z trestněprávního hlediska relevantní či nikoli) naplňuje podle mého názoru znaky trestného činu porušení tajemství dopravovaných zpráv podle § 182 odst. 2 písm. a) českého tr. zákoníku.

Ustanovení § 88 tr. řádu se neuplatní (ani analogicky) v případě, že si soukromá osoba pořídí zvukový záznam bez souhlasu osoby, jejíž hlas je takto zaznamenán (srov. č. 7/08 Sb. rozh. tr.).

Ačkoliv to trestní řád výslovně neuvádí, odposlech a záznam telekomunikačního provozu mohou použít také orgány celní správy při výkonu své působnosti vyplývající z mezinárodních

smluv při provádění dohledu nad osobami, o kterých existují závažné důvody předpokládat, že porušují nebo porušily právní předpisy druhé smluvní strany – § 63 odst. 1 zák. č. 17/2012 Sb., o Celní správě ČR. Výslovné uvedení této skutečnosti v trestním řádu by bylo žádoucí.

Aktuálním problémem nauky i praxe v České republice jsou právní důsledky nesplnění formálních předpokladů (náležitosti příkazu k odposlechu).

Důsledky nenaplnění formálních požadavků příkazu k odposlechu a záznamu telekomunikačního provozu byly v poslední době hojně diskutovány v souvislosti s usnesením Vrchního soudu v Praze ze dne 17. 10. 2016, kterým byla Krajskému soudu v Praze vrácena věc v médiu ostře sledované kauze bývalého hejtmána Středočeského kraje obžalovaného MUDr. D. Ratha. Vrchní soud zrušil rozsudek prvního stupně s poukazem na nemožnost použití záznamu telekomunikačního provozu, neboť příkaz o nařízení odposlechu a záznamu telekomunikačního provozu byl nedostatečně odůvodněn, ať už pokud jde o skutkové okolnosti případu zdůvodňující takto závažný zásah do práv a svobod, tak i pokud jde o nařízenou nejvyšší přípustnou délku trvání odposlechu. Vrchní soud své rozhodnutí opřel o usnesení Nejvyššího soudu ČR ze dne 14. 1. 2014, sp. zn. 4 Pzo 3/2013, v němž se mj. uvádí, že za náležitost příkazu k odposlechu a záznamu telekomunikačního provozu je nutno považovat i uvedení konkrétních skutkových okolností, které vydání příkazu, včetně doby jeho trvání, odůvodňují, dále zde musí být uveden účel odposlechu a záznamu telekomunikačního provozu a také vysvětleny důvody, proč nelze sledovaného účelu dosáhnout jinak nebo proč by bylo jinak jeho dosažení podstatně ztížené.

S tímto závěrem se ovšem dle mého názoru nelze bez dalšího ztotožnit. Domnívám se, že nedostatek odůvodnění příkazu k odposlechu a záznamu telekomunikačního provozu nezákonnost provedeného odposlechu zakládat nemusí. Povahu pochybení bude vždy nutné zvažovat i z materiálního hlediska, tedy zda i přes chybějící odůvodnění existují v konkrétním případě podmínky pro provedení tohoto úkonu (srov. č. 37/2013 Sb. rozh. tr.). Pokud tedy z dalšího průběhu řízení vyplyne, že materiální podmínky pro vydání příkazu k odposlechu a záznamu telekomunikačního provozu byly naplněny, formální nedostatky vydaného trestního příkazu tím mohou být zhojeny, záleží na míře nedostatku v konkrétní kauze. Naopak, pakliže příkaz dostatečně odůvodněn nebyl a v trestním řízení nebudou zjištěny poznatky, které by mohly nedostatečně odůvodnění příkazu zhojit, nutno dovodit nezákonnost provedeného odposlechu (srov. nález Ústavního soudu ČR sp. zn. II. ÚS 789/06 ze dne 27. 9. 2007).

Vzhledem k závěru o nepoužitelnosti výstupů z odposlechů a záznamů telekomunikačního provozu v trestním řízení se Vrchní soud dále zabýval i charakterem ostatních shromážděných důkazů podle jejich vztahu k nezákonně opatřeným důkazům a v návaznosti na to, zda je možné považovat tyto důkazy za účinné. V tomto bodě dospěl Vrchní soud k negativnímu stanovisku, když odkázal na doktrínu plodů z otráveného stromu (*fruit of the poisonous tree doctrine*), podle které je nutné za neúčinné důkazy považovat i ty důkazy, jež byly získány na základě předchozích nezákonným způsobem obstaraných důkazů. Tato doktrína je ovšem typická pro právní systém *common law* a v podmínkách České republiky se uplatňuje pouze v omezeném rozsahu. Nemá oporu v trestním řádu ani v nauce. Nelze dovodit závěr, že jakékoli pochybení při opatrování důkazu automaticky způsobuje procesní nepoužitelnost důkazu. Možnostmi využití doktríny plodů z otráveného stromu se již v minulosti opakovaně zabýval Ústavní soud ČR. Ten zastává přístup, že ani rigorózní interpretace této doktríny nevede k závěru, že jakékoli pochybení při opatrování důkazu automaticky způsobuje nepoužitelnost důkazu. Vždy je třeba mj. konkrétně posuzovat, jak intenzivní bylo dané pochybení a zda vůbec bylo způsobilé chování dotčené osoby a proces provádění důkazu ovlivnit. Stejně tak nelze na základě této doktríny učinit závěr, že výskyt nezákonného důkazu způsobuje nepoužitelnost všech důkazů, opatřených v da-

ném řízení. Nepoužitelnost se může týkat toliko těch důkazů, jež jsou od nezákonného důkazu kauzálně odvozeny (srov. nález Ústavního soudu ČR sp. zn. I. ÚS 1677/13 ze dne 23. 10. 2014).

V souvislosti s nutností dodržení zákonných požadavků při vydání příkazu k odposlechu a záznamu telekomunikačního provozu je nutné také poukázat na nevhodnou praxi u mnoho českých soudů, kdy úkony přípravného řízení dle rozvrhu práce vykonávají i soudci z netrestních úseků. Nedostatečná erudice pak může snadno vést k tomu, že vydaný příkaz nebude mít všechny náležitosti, které jsou na něj kladeny zákonem a navazující soudní judikaturou.

Problémů vycházející z nepříliš kvalitní české trestněprocesní legislativy týkající se odposlechu a záznamu telekomunikačního provozu je samozřejmě více, například odposlech mezi advokátem a obviněným, použití záznamu telekomunikačního provozu jako důkazu v jiné trestní věci nebo v jiné civilní věci, abych uvedl alespoň nejfrekventovanější. Rozsah tohoto příspěvku je ovšem limitem pro zevrubné zpracování problematiky.

2. Možnost kontroly zákonnosti provedeného odposlechu a záznamu

Vzhledem k principům právního státu je nutné, aby osoba dotčená odposlechem telekomunikačního provozu byla informována o tomto zásahu do základních práv a svobod a měla možnost v případě jeho neoprávněnosti se proti němu bránit právní cestou.

Na tento požadavek reagují ustanovení § 88 odst. 8 a 9 českého tr. řádu, podle nichž státní zástupce nebo policejní orgán, jehož rozhodnutím byla věc pravomocně skončena, a v řízení před soudem předseda senátu soudu prvního stupně po pravomocném skončení věci, informuje o nařízeném odposlechu a záznamu telekomunikačního provozu osobu – uživatele odposlouchávané stanice, pokud je známa. Informace obsahuje označení soudu, který vydal příkaz k odposlechu a záznamu telekomunikačního provozu, délku trvání odposlechu a datum jeho ukončení. Součástí informace je poučení o právu podat ve lhůtě šesti měsíců ode dne doručení této informace Nejvyššímu soudu návrh na přezkoumání zákonnosti příkazu k odposlechu a záznamu telekomunikačního provozu. Předseda senátu soudu prvního stupně podá informaci bezodkladně po pravomocném skončení věci, státní zástupce, jehož rozhodnutím byla věc pravomocně skončena, bezodkladně po uplynutí lhůty pro přezkoumání jeho rozhodnutí nejvyšším státním zástupcem podle § 174a tr. řádu (3 měsíce od právní moci rozhodnutí ve věci) a policejní orgán, jehož rozhodnutím byla věc pravomocně skončena, bezodkladně po uplynutí lhůty pro přezkoumání jeho rozhodnutí státním zástupcem [§ 174 odst. 2 písm. e) tr. řádu, 30 dnů od doručení].

Informaci předseda senátu, státní zástupce nebo policejní orgán nepodá v řízení o zločinu, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně osm let, spáchaném organizovanou skupinou, v řízení o trestném činu spáchaném ve prospěch organizované zločinecké skupiny, v řízení o trestném činu účasti na organizované zločinecké skupině (§ 361 trestního zákoníku), v řízení o trestném činu účasti na teroristické skupině (§ 312a trestního zákoníku) nebo pokud se na spáchání trestného činu podílelo více osob a ve vztahu alespoň k jedné z nich nebylo trestní řízení doposud pravomocně skončeno, nebo pokud je proti osobě, již má být informace sdělena, vedeno trestní řízení, anebo pokud by poskytnutím takové informace mohl být zmařen účel trestního řízení, nebo by mohlo dojít k ohrožení bezpečnosti státu, života, zdraví, práv a svobod osob.

Na první pohled přitom není zřejmé, zda se shora uvedená výjimka z informování v případě řízení o zločinu, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně osm let, vztahuje pouze tehdy, kdy byl takový čin spáchán organizovanou skupinou, nebo zda se jedná o dva samostatné důvody, pro které nemá orgán činný v trestním řízení povinnost

informovat uživatele odposlouchávané stanice. S ohledem na to, že všechny ostatní případy jsou spojeny s případy trestné součinnosti, ale také vzhledem k nutnosti výkladu příznivějšího pro okruh oprávněných osob, je třeba dovodit, že se jedná o kumulativní podmínky (řízení o zločinu s trestní sazbou nejméně 8 let, který byl spáchán organizovanou skupinou), které musí být naplněny, aby orgán činný v trestním řízení neměl povinnost dotčenou osobu informovat.

Podle § 88 odst. 8 tr. řádu je tedy možné, aby uživatel odposlouchávané stanice podal návrh na přezkoumání příkazu k odposlechu a záznamu telekomunikačního provozu Nejvyššímu soudu. Řízení u Nejvyššího soudu je pak upraveno v ustanoveních § 314l až § 314n tr. řádu. Soud o návrhu rozhoduje v neveřejném zasedání a shledá-li, že zákon byl porušen, vysloví usnesením porušení zákona. Proti tomuto usnesení není přípustný žádný opravný prostředek. K porušení zákona může dojít při vydání příkazu k odposlechu a záznamu telekomunikačního provozu, při provedení příkazu k odposlechu a záznamu telekomunikačního provozu nebo při vydání i provedení příkazu k odposlechu a záznamu telekomunikačního provozu.

Za problematické lze označit, na základě kterých skutečností Nejvyšší soud o zákonitosti odposlechu rozhoduje. Aby mohl soud odpovědně posoudit, zda byl v konkrétním případě odposlech zákonný, musel by mít k dispozici především takové informace, které mě k dispozici soudce, který odposlech nařídil, včetně poznatků operativní povahy, které nelze zajistit.

Pro oprávněnou, tj. odposlouchávanou osobu ovšem výrok Nejvyššího soudu sice otevírá možnost případné náhrady za nemajetkovou újmu, nicméně nemá žádný vliv na právní moc rozhodnutí vzešlého z kauzy, ve které k odposlechu a záznamu telekomunikačního provozu došlo. Takovou právní úpravu lze jen stěží označit za správnou.

De lege ferenda se nabízí dvě možnosti.

Předně možnost, aby oprávněná osoba, jejíž práva byla nezákonným odposlechem a záznamem o telekomunikačním provozu porušena, mohla v případě takového výroku Nejvyššího soudu podat kvalifikovaný podnět ministru spravedlnosti. Ten by byl za takové situace povinen podat stížnost pro porušení zákona, na základě které by předchozí pravomocné rozhodnutí ve věci samé mohlo být Nejvyšším soudem zrušeno. Obnova řízení ani dovolání totiž s ohledem na jejich podmínky (omezení pouze na určitá rozhodnutí, lhůty k podání, okruh namítaných vad apod.) nepředstavují pro oprávněnou osobu účinný prostředek, kterým by mohlo být pravomocné rozhodnutí ve věci samé s poukazem na nezákonnost odposlechu zrušeno.

Pokud by shora uvedené řešení nebylo vhodné, například proto, že by zasahovalo do výlučné pravomoci ministra spravedlnosti podat tento tzv. úřednický opravný prostředek, nabízí se ještě jiná možnost, a sice, že v takovém případě, kdy Nejvyšší soud vysloví nezákonnost nařízeného či provedeného odposlechu, by mohl podat stížnost pro porušení zákona předseda Nejvyššího soudu. Tato varianta má svoji logiku v tom, že předseda Nejvyššího soudu by mohl, ale nemusel podat tento mimořádný opravný prostředek, a tedy mohl zvážit, zda účinná ochrana práv odposlouchávané osoby nebo zájem na spravedlivém rozhodnutí v konkrétní trestní věci si podání tohoto mimořádného opravného prostředku vyžadují. Současně by podání mimořádného opravného prostředku předcházelo odborné posouzení a selekce těch případů, při kterých by případné porušení práv odposlouchávané osoby nemělo vliv na správnost a zákonitost navazujícího meritorního rozhodnutí.

Obě varianty ovšem předpokládají, že v novém, rekodifikovaném českém trestním řádu (který se již téměř 30 let připravuje) zůstane zachována stížnost pro porušení zákona jako mimořádný opravný prostředek, resp. že bude zaveden jiný tzv. úřednický opravný prostředek, ať již bude nazván jakkoli.

Zákonné limity zabezpečovania informácií dôležitých pre trestné konanie¹

Legal Limits Provision of Information Relevant to Criminal Proceedings

Ivan Šimovček²

Abstrakt: Zákonné limity zabezpečovania informácií dôležitých pre trestné konanie možno vidieť v rovine ochrany práva na súkromie na jednej strane a v zákonných možnostiach zásahu do tohto práva. Pri obmedzovaní práva na súkromie nemožno porušiť podmienky prijaté na ochranu súkromia podľa medzinárodných dohovorov o ľudských právach a základných slobodách. Právom na súkromie sa zaručuje ochrana hodnôt uznaných za súkromné pred verejnou mocou, fyzickými aj právnickými osobami. Ochrana nemateriálnych hodnôt súkromnej povahy sa zaručuje ústavou. Nezaručuje sa však absolútna ochrana súkromného a rodinného života, ale priznáva sa len ochrana pred neoprávneným zasahovaním do súkromného a rodinného života.

Abstract: Legal limits provision of information relevant to criminal proceedings can be seen in the level of protection of privacy on the one hand and the legal possibilities interference with this right. In limiting the right to privacy cannot violate the conditions adopted for the protection of privacy under international conventions on human rights and fundamental freedoms. The right to privacy is guaranteed protection of the values found in private before public authorities, natural or legal persons. Protection of non-material values of a personal nature is guaranteed by the Constitution. However, it does not guarantee absolute protection of private and family life, but confers only protection against unauthorized interference in private and family life.

Kľúčové slová: Ústava, ochrana súkromia, ľudské práva, trestné konanie, informačne-technické prostriedky.

Key Words: The Constitution, privacy, human rights, criminal proceedings, information-technical means.

Úvod

Zákonné limity zabezpečovania informácií dôležitých pre trestné konanie možno vidieť v rovine ochrany práva na súkromie na jednej strane a v zákonných možnostiach zásahu do tohto práva.

Zákonná ochrana práva na súkromie sa prejavuje v týchto úrovniach vymedzenia:

- medzinárodná resp. európska úroveň ochrany práva na súkromie,
- ústavná rovina ochrany práva na súkromie,
- vnútroštátna rovina ochrany práva na súkromie.

Medzinárodná a európska úroveň ochrany súkromia

Pri obmedzovaní práva na súkromie nemožno porušiť podmienky prijaté na ochranu súkromia podľa medzinárodných dohovorov o ľudských právach a základných slobodách.³

¹ Príspevok bol spracovaný v rámci riešenia vedecko-výskumného projektu VEGA č. 1/0764/17 s názvom Informačno-technické prostriedky a prostriedky operatívno-pátracej činnosti získavania informácií dôležitých pre trestné konanie.

² Prof. JUDr. Ivan Šimovček, CSc., Právnická fakulta, Trnavská univerzita v Trnave, e-mail: ivan.simovcek@truni.sk.

³ Nález Ústavného súdu SR, sp. zn. PL. ÚS 43/95.

Právo na súkromie je chránené Všeobecnou deklaráciou ľudských práv, v ktorej sa v čl. 12 uvádza, že nikto nesmie byť vystavený svojvoľnému zasahovaniu do súkromného života, do rodiny, domova alebo korešpondencie, ani útokom na svoju česť a povesť. Každý má právo na právnu ochranu proti takým zásahom alebo útokom. Právo na súkromie patrí medzi základné ľudské práva garantované medzinárodnými zmluvami.

Účel priznaného práva na súkromie musí zodpovedať účelu tohto práva podľa čl. 17 ods. 1 Medzinárodného paktu o občianskych a politických právach, ako aj podľa čl. 8 ods. 1 Dohovoru o ochrane ľudských práv a základných slobôd (ďalej len „Dohovor“).⁴

V čl. 8 ods. 1 Dohovoru je právo na rešpektovanie súkromného a rodinného života nasledovne:

1. Každý má právo na rešpektovanie svojho súkromného a rodinného života, obydlia a korešpondencie.
2. Štátny orgán nemôže do výkonu tohto práva zasahovať s výnimkou prípadov, keď je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom alebo zločinnosti, ochrany zdravia alebo morálky alebo na ochranu práv a slobôd iných.⁵

Dané ustanovenia Dohovoru ohľadne práva na ochranu súkromia sú rozvedené v početnej judikatúre Európskeho súdu pre ochranu ľudských práv (ďalej len „ESLP“), z ktorej chcem poukázať len na niektoré.

Rozsudok ESLP vo veci Marckx proti Belgicku (rozhodnutie z 13. júna 1970), v ktorom sú konkrétne charakterizované jednotlivé (napríklad prehliadky a vypočúvanie v prostredí domova; nasadzovanie skrytých odpočúvacích prístrojov (špicľovanie); nahrávanie telefonických hovorov, odpojenie elektrickej energie alebo vody).⁶

Rozsudok v prípade Van Oosterwijck proti Belgicku (rozhodnutie zo 16. novembra 1980) uviedol, že právo na ochranu súkromia má zahŕňať aj právo zakladať a rozvíjať vzťahy s inými ľudskými bytosťami, najmä v citovej oblasti, v záujme rozvoja a naplnenia svojej vlastnej osobnosti.

Rozsudok ESLP vo veci Niemietz proti Nemecku (rozhodnutie zo 16. decembra 1992) vykladá právo na ochranu súkromia extenzívnejšie v súvislosti s prehliadkou obydlia, ale aj kancelárie nemeckého advokáta Niemietza. Európsky súd sa v tomto prípade stotožnil s tvrdeniami sťažovateľa, pokiaľ ide o porušenie čl. 8 Dohovoru a čl. 1 jeho dodatkového protokolu č. 1 v tom, že prehliadka zasiahla do jeho práva na rešpektovanie jeho obydlia a korešpondencie a tým poškodila klientelu jeho kancelárie a jeho povesť.

Rozsudok ESLP vo veci Huvig proti Francúzsku (rozhodnutie z 24. apríla 1990). V danom prípade ESLP konštatoval zásah do súkromného života aj vtedy, ak sa odpočúvanie telefónov týkalo obchodných záležitostí.

Rozsudok ESLP vo veci Chappell proti Spojenému kráľovstvu (rozhodnutie z 30. marca 1989). Európsky súd poskytol ochranu sťažovateľovi podľa čl. 8 Dohovoru, hoci prehliadka smerovala výlučne proti obchodným činnostiam, pričom vychádzal z výkladu slova „home“ v porovnaní s francúzskym ekvivalentom „domicile“.

Rozšírenie aplikovateľnosti práva na súkromie v zmysle čl. 8 Dohovoru aj na profesionálne aktivity a obchodnú činnosť potvrdili aj rozsudok ESLP vo veci Klass a ostatní proti Spolkovej

⁴ Nález Ústavného súdu SR, sp. zn. II. ÚS 94/95.

⁵ Dohovor o ochrane ľudských práv a základných slobôd (čl. 8 ods. 1). http://www.echr.coe.int/documents/convention_slk.pdf (stiahnuté dňa 31. 1. 2017).

⁶ Svák, J. Ochrana ľudských práv v troch zväzkoch. II. zväzok. Bratislava: Eurokódex, 2011, s. 385.

republike Nemecko (rozhodnutie zo 6. septembra 1978), v ktorom Európsky súd konštatoval, že aj aktivita profesionálnej povahy môže patriť pod pojem „súkromný život“ a „korešpondencia“.

V Rozsudku ESLP vo veci: *Gillow proti Spojenému kráľovstvu* (rozhodnutie z 24. novembra 1986) Európsky súd definoval obydlie ako miesto, kde osoba býva alebo vykonáva svoju obvyklú profesiu. Za obydlie pritom treba považovať aj obydlie, ktoré jednotlivec vytvoril v rozpore s vnútroštátnym právom, a tiež obydlie, ktoré je obývané len počas určitého obdobia v roku.

Rozsudok ESLP vo veci *Société Colas Est. proti Francúzsku* (rozhodnutie z 16. apríla 2002), v ktorom súd zdôraznil, že požiadavka na ochranu obdobia sa vzťahuje aj na sídla spoločností a treba rešpektovať súkromie v sídlach spoločností či podnikov (právnických osôb) aj ich pobočiek.

Rozsudok ESLP vo veci *Crémieux proti Francúzsku* (rozhodnutie z 25. februára 1993) a Rozsudok ESLP vo veci *Miaillhe proti Francúzsku* (rozhodnutie z 25. februára 1993), v ktorých súd pod právo na ochranu súkromia zaradil aj kancelárske priestory.

V judikatúre ESLP týkajúcej sa práva na ochranu súkromia možno vidieť viaceré tendencie, medzi ktoré patrí najmä právo na súkromie predstavuje pozitívny záväzok štátu a rozširuje sa do sféry interpersonálnych vzťahov, dochádza s k presnejšiemu vymedzeniu hraníc či limitov zásahov štátu do práva na súkromie, preferenciu vnútroštátnej nápravy porušenia práva na súkromie a extenzívny výklad pojmov obsiahnutých v práve na súkromie.⁷

Pozitívny záväzok štátu vo vzťahu k ochrane práva na súkromie spočíva vo vytvorení podmienok zabráňujúcich porušeniu tohto práva. V už spomínanom rozsudku ESLP *Marckx proti Belgicku* (rozhodnutie z 13. júla 1979) súd rozšíril ochranu práva na súkromie na prípady, keď štát nevytvoril podmienky proti porušeniu tohto práva, t. j. štát nemôže zasahovať do výkonu tohto práva, iba ak v súlade so striktnými podmienkami a naopak má pozitívne záväzky na efektívne rešpektovanie rodinného života.

Rozsudkom ESLP vo veci *Ignaccolo-Zenide proti Rumunsku* (rozhodnutie z 25. januára 2000) sa pozitívny záväzok štátu rozšíril aj nečinnosť štátnych orgánov v prípadoch, v ktorých mali niečo konkrétne vykonať v záujme ochrany tohto práva.

Rozsudok ESLP vo veci *Babylonová proti Slovenskej republike* (rozhodnutie z 20. júna 2006) ustanovil povinnosť zabezpečiť účinný výkon práv vyplývajúcich z Dohovoru v rámci pozitívnych záväzkov štátu, ktoré môžu vyžadovať prijatie opatrení na ochranu práv podľa čl. 8 Dohovoru aj vo sfére vzťahov medzi jednotlivcami. Európsky súd sa v tomto prípade vychádzal z Rozsudku ESLP vo veci *X. a Y. proti Holandsku* (rozhodnutie z 26. marca 1985), v ktorom uviedol, že z pozitívneho záväzku štátu vyplýva povinnosť prijať také prostriedky ochrany práva na súkromie, ktoré by boli dostatočné na ochranu vzájomných vzťahov medzi jednotlivcami, pričom ak nestačia občianskoprávne prostriedky, je potrebná trestnoprávna úprava.

Zákonné možnosti zásahu do práva na ochranu súkromia v rámci trestného konania sú tiež zachytené v judikatúre ESLP. Európsky súd v tejto súvislosti sformuloval niekoľko hľadísk, ktoré sa posudzujú pri konkrétnom prípade zásahu do práva na súkromie, a to hľadiská legitimacy, legality a proporcionality.

Legitimita zásahu štátu do práva na súkromie vyplýva z čl. 8 ods. 2 Dohovoru. Podľa tohto ustanovenia môže štát prostredníctvom svojich orgánov zasiahnuť do práva na súkromie iba vtedy, ak je to v záujme štátu (kvôli ochrane národnej bezpečnosti, verejnej bezpečnosti, predchádzaniu nepokojov a zločinnosti), v záujme spoločnosti (kvôli ochrane zdravia alebo morál-

⁷ Svák, J.: *Ochrana ľudských práv v troch zväzkoch. II. zväzok*. Bratislava: Eurokódex, 2011, s. 393.

ky, zabezpečeniu hospodárskeho blahobytu krajiny) a v záujme jednotlivca (na ochranu jeho práv a slobôd).⁸

Európsky súd pri posudzovaní legitimacy skúma, či opatrenie umožňujúce zásah štátu do práva na súkromie zodpovedá legitímnemu cieľu trestného konania, čo je v trestnom konaní zistenie a usvedčenie páchatelov trestnej činnosti a ich potrestanie vydaním spravodlivého rozhodnutia.

Rozsudok ESLP vo veci L. proti Nórsku (rozhodnutie z 8. júna 1990) sa zaoberal otázkou, či je legitímne, ak sa tajné odpočúvanie vykonáva vo vzťahu k bezpečnosti štátu. Legalita zásahu štátu do práva na súkromie znamená, že štát môže do tohto práva zasiahnuť, len na základe zákona, pričom pojem zákona je interpretovaný široko, nakoľko Európsky súd za zákon nepovažoval iba právny predpis prijatý parlamentom, ale aj podzákonné právne predpisy, ktoré vydali orgány, ktoré nedisponovali zákonodarnou mocou,⁹ ale aj právne predpisy, ktoré vytvorili súdy v krajinách patriacich do právneho systému common law.¹⁰

Európsky súd pri posudzovaní podmienky legality nekladie dôraz na formu právneho predpisu, na ktorého základe sa zasiahne do práva na súkromie, ale na jeho náležitosti, ktoré právny predpis musí naplniť. Predovšetkým ide o dostupnosť a predvídateľnosť zákona. Dostupnosť zákona je zabezpečená jeho verejným publikovaním.¹¹ Predvídateľnosť zákona vyžaduje, aby bol sformulovaný dostatočne, presne a jasne, aby tak umožnil potenciálne dotknutej osobe informáciu o tom, za akých podmienok môže dôjsť k zásahu do jej práva na súkromie.¹²

Proporcionálna zásahu do práva na ochranu súkromia musí byť dodržaná aj výberom prostriedkov, ktorými štát disponuje pri plnení legitímneho cieľa. Základným kritériom pri posudzovaní proporcionality zásahu štátu je jeho nevyhnutnosť v demokratickej spoločnosti. Štát má pri výbere prostriedkov, ktorými chce dosiahnuť legitímny cieľ, možnosť uplatniť voľnú úvahu, pričom je limitovaný tým, že zásah do práva na súkromie vykoná len vtedy, keď je to nevyhnutné a v duchu požiadaviek kladených na demokratickú spoločnosť.

Štát sa nemôže legitímne dovoľávať všeobecnej nevyhnutnosti ako dôvodu na obmedzenie práv a slobôd jednotlivca.

Za demokratickú spoločnosť sa v judikatúre ESLP považuje taká spoločnosť, ktorá sa vyznačuje pluralizmom, toleranciou a „voľným duchom“, čo sa však niekedy zamieňa s pojmom liberalizmus.¹³ Posudzovanie proporcionality je vždy individuálne vzhľadom na konkrétne okolnosti prípadu a podmienky jednotlivých štátov. Európsky súd považoval takto určitý zásah štátu za proporcionálny v jednom štáte, ale ako neproporcionálny v druhom štáte.

Na druhej strane v Rozsudku ESLP vo veci K. U. proti Fínsku (rozhodnutie z 2. decembra 2008) súd upozorňuje na to, že pri meniacich sa podmienkach v jednotlivých štátoch treba prihliadať aj na zblížovanie štandardov, ktoré sa majú v členských štátoch Rady Európy dosiahnuť.¹⁴

ESLP súd stanovil pravidlá či postupy, ktoré by sa mali uplatniť pri posudzovaní zákonnosti zásahu do práva na súkromie a pri výklade právnych noriem, ktoré tieto zásahy upravujú. Rozsudok ESLP vo veci Sunday Times proti Spojenému kráľovstvu (rozhodnutie z 26. apríla 1979)

⁸ Svák, J.: Ochrana ľudských práv v troch zväzkoch. II. zväzok. Bratislava: Eurokódex, 2011, s. 393.

⁹ Rozsudok ESLP vo veci Barthold proti Spolkovej republike Nemecko (rozhodnutie z 25. marca 1985).

¹⁰ Rozsudok ESLP vo veci Kruslin proti Francúzsku (rozhodnutie z 24. apríla 1990).

¹¹ Rozsudok ESLP vo veci Autronic AG proti Švajčiarsku (rozhodnutie z 22. mája 1990).

¹² Pozri Rozsudok ESLP vo veci napr. Klass a ostatní proti Spolkovej republike Nemecko (rozhodnutie zo 6. septembra 1978), Rozsudok ESLP vo veci Silver a ostatní proti Spojenému kráľovstvu (rozhodnutie z 25. marca 1983), Rozsudok vo veci Malone proti Spojenému kráľovstvu (rozhodnutie z 2. augusta 1984), Rozsudok ESALP vo veci Olsson proti Švédsku (rozhodnutie z 24. marca 1988).

¹³ Svák, J. Ochrana ľudských práv v troch zväzkoch. II. zväzok. Bratislava: Eurokódex, 2011, s. 414.

¹⁴ Tamtiež, s. 414.

stanovil, že takéto zásahy sa posudzujú doslovným výkladom, ktorý podľa súdu znamená, že základom akéhokoľvek obmedzenia môžu byť iba kritériá, ktoré sú uvedené v samotnom ustanovení o výnimkách. Toto pravidlo je dôležité najmä pri posudzovaní legality zásahu štátu a pri jeho konkrétnej aplikácii. Súd pritom hodnotí zásah do práva na súkromie z hľadiska jeho legality, legitimacy a proporcionality.

Európsky súd ponecháva zmluvným stranám možnosti na ochranu práva a určitý rámec na úvahu o voľbe vhodných prostriedkov zasahovania do tohto práva v záujme dosiahnutia legitímneho cieľa.¹⁵

V Rozsudku ESLP vo veci Smith a Grady proti Spojenému kráľovstvu a Lustig-Prean a Becket proti Spojenému kráľovstvu (rozhodnutie z 27. septembra 1999) Európsky súd uviedol, že v prvom rade vnútroštátnym orgánom patrí právo posúdenia nevyhnutnosť zásahov do práva na súkromie, pričom Európsky súd je príslušný posúdiť, či dôvody zásahov boli relevantné a dostatočné.

V Rozsudku ESLP veci Klass a ostatní proti Spolkovej republike Nemecko (rozhodnutie zo 6. septembra 1978) súd zdôraznil, že zmluvné štáty majú možnosť posúdiť nevyhnutnosť zásahov, ale súbežne s európskou kontrolou. V rozsudku ESLP vo veci L. proti Nórsku (rozhodnutie z 8. júna 1990) Európsky súd posudzoval, či vnútroštátna právna ochrana je dostatočná, aby vylúčila možnosť zneužitia zásahov štátu do práva na súkromie a v Rozsudku ESLP vo veci Hoffmann proti Rakúsku (rozhodnutie z 23. júna 1993) súd riešil otázku, či vnútroštátne orgány správne vykladajú zákazy podľa príslušných vnútroštátnych právnych predpisov v súlade s čl. 8 Dohovoru.

Interpretačným pravidlom ESLP pri výklade práva na súkromie sa stal rozširujúci výklad. Takto do práva na súkromie bolo zaradené právo na súkromný život, právo na rodinný život, nedotknuteľnosť obydlia a ochranu korešpondencie. Napríklad do práva na súkromný život, okrem tradičných práv spojených so zákazom zberu a zhromažďovania osobných údajov rôznymi spôsobmi (napríklad tajným odpočúvaním telefonických rozhovorov), boli zaradené aj práva vychádzajúce síce zo súkromného života konkrétnej osoby, ale s oveľa väčším spoločenským dosahom.¹⁶

Právo na súkromie možno vymedziť aj negatívne. V Rozsudku ESLP vo veci Brügge mann a Scheuten proti Spolkovej republike Nemecko (rozhodnutie z 12. júla 1977) sa uvádza, že právo na rešpektovanie súkromného života sa automaticky redukuje v závislosti od toho, do akej miery jednotlivec sám dáva svoj súkromný život do kontaktu s verejným životom alebo do úzkeho spojenia s inými chránenými záujmami.

Ústavná ochrana práva na súkromie

Právo na súkromie je širšia kategória zložená z niekoľkých samostatných základných práv, ktoré upravujú najmä články 16, 19 a 21 Ústavy Slovenskej republiky – zákon č. 460/1992 Zb. (ďalej len „Ústava“).

Právo na súkromie je vnútorne diferencované a preto je upravené vo všeobecnej rovine i v konkrétnejších ustanoveniach, ktoré upravujú a chránia rôzne vzťahy vyplývajúce z práva na súkromie. Všeobecnú úpravu ochrany súkromia možno nájsť v čl. 16 Ústavy; v ďalších spomenutých ustanoveniach sú potom konkretizované ďalšie práva.

¹⁵ Svák, J. Ochrana ľudských práv v troch zväzkoch. II. zväzok. Bratislava: Eurokódex, 2011, s. 417.

¹⁶ Svák, J. Ochrana ľudských práv v troch zväzkoch. II. zväzok. Bratislava: Eurokódex, 2011, s. 419.

Podľa čl. 16 ods. 1 Ústavy je zaručená nedotknuteľnosť osoby a jej súkromia. Podľa čl. 19 ods. 2 Ústavy má každý právo na ochranu pred neoprávneným zasahovaním do súkromného a rodinného života. V zmysle čl. 19 ods. 3 Ústavy má každý právo na ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe a čl. 21 Ústavy upravuje nedotknuteľnosť obydľia, do ktorého nie je dovolené vstúpiť bez súhlasu toho, kto v ňom býva. Domová prehliadka je prípustná len v súvislosti s trestným konaním, a to na písomný a odôvodnený príkaz sudcu. Iné zásahy do nedotknuteľnosti obydľia možno zákonom dovoliť iba vtedy, keď je to v demokratickej spoločnosti nevyhnutné na ochranu života, zdravia alebo majetku osôb, na ochranu práv a slobôd iných alebo na odvrátenie závažného ohrozenia verejného poriadku.

Vnútoraná diferencovanosť právnej úpravy práva na súkromie bola potvrdená aj viacerými rozhodnutiami Ústavného súdu Slovenskej republiky (ďalej len „Ústavný súd“). V náleze I. ÚS 13/2000 z 10. júla 2001 potvrdil, že ústavou vytvorená ochrana práva na súkromie sa vnútorne diferencuje. Jednotlivými ustanoveniami sa zaručuje ochrana súkromia v rôznych životných situáciách. Do sféry ochrany súkromia patrí aj ochrana obydľia. Podľa okolností konkrétnej veci sa ten istý zásah môže teda dotknúť tak práva na ochranu súkromia, ako aj práva na ochranu obydľia.¹⁷

V náleze I. ÚS 33/95 Ústavný súd uviedol, že „Ústava vo viacerých ustanoveniach dotvára jednotnú úpravu práva na súkromný život, ktorého podstatou je možnosť jednotlivca v určitej sfére spoločenských vzťahov žiť podľa svojich predstáv bez zbytočných obmedzení, príkazov a zákazov ustanovených orgánmi verejnej moci. Ústavou vytvorená ochrana práva na súkromie sa vnútorne diferencuje. Jednotlivými ustanoveniami sa zaručuje ochrana súkromia v rôznych životných situáciách“¹⁸

Pojem súkromný život je pojem široký a nemožno ho vyčerpávajúcim spôsobom definovať, najmä ho nemožno obmedziť na intímnu sféru, v ktorej každý môže viesť svoj osobný život podľa svojej chuti, a úplne z neho vylúčiť vonkajší svet tejto sféry.¹⁹

Účelom Ústavou priznaného práva na súkromie je nielen poskytnúť ochranu práv priznaných podľa § 11 a nasl. Občianskeho zákonníka, ale zároveň aj zabrániť štátnym orgánom i orgánom územnej samosprávy, aby zasahovali do správania jednotlivca nad nevyhnutnú mieru a príliš neprimerane riadili jeho súkromný život. Právom na súkromie sa zaručuje ochrana hodnôt uznaných za súkromné pred verejnou mocou, fyzickými aj právnickými osobami. Ochrana nemateriálnych hodnôt súkromnej povahy sa zaručuje podľa čl. 19 ods. 2 Ústavy. Týmto ustanovením sa nezaručuje absolútna ochrana súkromného a rodinného života, ale priznáva sa len ochrana pred neoprávneným zasahovaním do súkromného a rodinného života. Ústava teda umožňuje také zásahy do súkromného a rodinného života, ktoré sú oprávnené.²⁰

Údaje o osobe sú predmetom ochrany v rámci práva na súkromie aj bez toho, aby sa im v osobitnom ustanovení Ústavy priznala samostatná ochrana. Ústava však nevylučuje akýkoľvek zber údajov o osobe. Ochrana sa priznáva iba pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov.²¹

Oprávnené zhromažďované údaje musí orgán verejnej moci uschovať tak, aby boli chránené pred neoprávneným prístupom iných orgánov verejnej moci, aj pred fyzickými a právnickými

¹⁷ Nález Ústavného súdu SR, sp. zn. I. ÚS 13/2000.

¹⁸ Nález Ústavného súdu SR, sp. zn. I. ÚS 33/95.

¹⁹ Nález Ústavného súdu SR, sp. zn. PL. ÚS 5/93, Nález Ústavného súdu SR, sp. zn. PL. ÚS 15/98.

²⁰ Nález Ústavného súdu SR, sp. zn. II. ÚS 1/97.

²¹ Nález Ústavného súdu SR, sp. zn. II. ÚS 94/95.

mi osobami. Ak orgán verejnej moci zhromažďuje údaje o osobe, ktoré nie je oprávnený zistiť, uschovať alebo inak získať do svojej dispozičnej sféry, ide o porušenie Ústavy.

Stav technológií sťažujúci prístup k údajom ani iné opatrenia prijaté na ochranu údajov uložených v informačnom systéme nemožno zamieňať s ústavnou ochranou pred neoprávneným zhromažďovaním údajov o osobe.²²

Obmedzenie práva na ochranu súkromia je nevyhnutné prípade, že cieľ obmedzenia inak dosiahnuť nemožno. Obmedzenie práva na ochranu súkromia je nevyhnutné aj v demokratickej spoločnosti. Zásah do práva na súkromie musí zodpovedať naliehavej spoločenskej potrebe a musí byť primeraný sledovanému legitímnemu cieľu.

V náleze I. ÚS 274/05, sa uvádza, že zásahy do práva na súkromie treba vykladať v logickej nadväznosti. Predovšetkým sa skúma, či daný skutkový stav možno považovať za právom chránené súkromie. V ďalšom sa skúma, či bol zásah legitímny a napokon, či bol proporcionálny. Ak sa dospeje k negatívnej odpovedi pri niektorej z týchto otázok, ďalej sa už v skúmaní problematiky nepokračuje.

Ochranu práva na súkromie možno vidieť aj v Rámcovom rozhodnutí Rady 2008/977/SVV z 27. 11. 2008 o ochrane osobných údajov spracúvaných v rámci policajnej spolupráce v trestných veciach.

Vnútroštátna úprava ochrany práva na súkromie

Vnútroštátna úprava ochrany práva na súkromie vychádza z práva každej fyzickej osoby na ochranu svojej osobnosti, najmä života a zdravia, občianskej cti a ľudskej dôstojnosti, ako aj súkromia, svojho mena a prejavov osobnej povahy.²³

Za osobné údaje možno považovať údaje týkajúce sa fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu.²⁴

Zákonné podmienky narušenia práva na ochranu súkromia možno nájsť vo viacerých právnych predpisoch, upravujúcich spôsoby zabezpečovania informácií o súkromí osôb.

Pre účely zabezpečovania informácií dôležitých pre trestné konanie sú rozhodujúce ustanovenia piatej hlavy Trestného poriadku (ďalej len „TP“) s názvom Zabezpečovanie informácií.²⁵ Trestný poriadok podrobne rozoberá spôsoby zabezpečovania informácií takými prostriedkami, akými sú sledovanie osôb a vecí (§ 113 TP), vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov (§ 114 TP), odpočúvanie a záznam telekomunikačnej prevádzky (§ 115 TP), oznámenie údajov o telekomunikačnej prevádzke (§ 116 TP), agent (§ 117 TP) a porovnávanie údajov v informačných systémoch (§ 118 TP).

Odpočúvanie a záznam telekomunikačnej prevádzky je osobitne upravené aj v zákone o ochrane pred odpočúvaním.²⁶ Tento zákon ustanovuje podmienky použitia informačno-technických prostriedkov bez predchádzajúceho súhlasu toho, komu zasahuje do súkromia orgán štátu, ktorý informačno-technický prostriedok používa. Zákon sa nevzťahuje na použitie informačno-technických prostriedkov v trestnom konaní.

²² Drgonec, J.: Ústava Slovenskej republiky. Komentár. 2. vydanie. Šamorín: Heuréka, 2007, s. 228.

²³ § 11 Zák. č. 40/1964 Zb. Občiansky zákonník.

²⁴ § 4 ods. 1 zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

²⁵ § 113–118 zákona č. 301/2005 Z. z. Trestného poriadku.

²⁶ Zák. č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním).

Informačno-technickými prostriedkami na účely tohto zákona sú najmä elektrotechnické, rádiotechnické, fototechnické, optické, mechanické, chemické a iné technické prostriedky a zariadenia alebo ich súbory používané utajovaným spôsobom pri vyhľadávaní, otváraní, skúmaní a vyhodnocovaní poštových zásielok a iných dopravovaných zásielok, odpočúvaní a zaznamenávaní v rámci telekomunikačných činností a vyhotovovaní a využívaní obrazových, zvukových alebo iných záznamov.

Informačno-technické prostriedky môžu používať len týmto zákonom určené orgány štátu v rozsahu podľa osobitných predpisov²⁷ iba vtedy, ak je to v demokratickej spoločnosti nevyhnutné na zabezpečenie bezpečnosti štátu, obranu štátu, predchádzanie a objasňovanie trestnej činnosti alebo na ochranu práv a slobôd iných. Použitím informačno-technického prostriedku sa môže právo na ochranu súkromia obmedziť len v nevyhnutnom rozsahu a nie dlhšie, ako je to nevyhnutné na dosiahnutie zákonom uznaného cieľa, na ktorý slúži.

Na záver príspevku by som sa chcel pozastaviť pri Slovenskej informačnej službe (ďalej len „SIS“) a jej legálnym limitom narušovania práva na ochranu súkromia vzhľadom na trestné konanie. Informačná služba poskytuje informácie o trestnej činnosti útvarom Policajného zboru a prokuratúry, a to najmä o páchaní organizovanej trestnej činnosti.²⁸ SIS má právo na sprístupnenie a poskytnutie informácií a osobných údajov z informačných systémov orgánov verejnej moci; tieto údaje sa poskytujú a sprístupňujú bez súhlasu dotknutej osoby a o ich poskytnutí a sprístupnení sa tieto osoby neinformujú.²⁹

SIS je ďalej oprávnená vytvárať a prevádzkovať informačné systémy a spracúvať v nich osobné údaje fyzických osôb a viesť informačné systémy a evidencie takýchto údajov. Údaje o správaní osoby mladšej ako 14 rokov nesmú byť ukladané do evidencií.³⁰

SIS je oprávnená pri plnení niektorých svojich úloh³¹ a na účely spolupráce³² spracúvať osobitné kategórie osobných údajov v rozsahu podľa osobitného predpisu.³³

V pripravovanom novom zákone, ktorý okrem iného navrhuje premenovať SIS na „Úrad civilného spravodajstva“ sa rozširuje okruh prostriedkov právnej ochrany fyzických osôb a právnických osôb vo veciach neoprávneného zásahu do ich základných práv a slobôd, resp. možného porušenia všeobecne záväzných právnych predpisov činnosťou spravodajských služieb. Na tento účel sa navrhuje ustanoviť osobitný inštitút sťažností a upravuje sa osobitný režim ich vybavovania, ktorý je odlišný od všeobecnej právnej úpravy.

Na rozdiel od platnej právnej sa navrhuje ustanoviť podrobnejší režim používania osobitných prostriedkov cestou ich taxatívneho vymenovania v zákone. Súčasne sa ustanovuje, že spravodajské služby musia pri používaní osobitných prostriedkov a využívaní osobitných oprávnení rešpektovať základné princípy a zásady v rámci zohľadnenia ústavného princípu legality dovoľujúci štátnym orgánom konať iba na základe ústavy, v jej medziach a v rozsahu a spôsobom, ktorý ustanoví zákon. Navrhovaná úprava súčasne zohľadňuje existujúci právny stav na úseku používania informačno-technických prostriedkov reprezentovaný osobitnou zákonnou úpravou.³⁴

²⁷ Zák. č. 198/1994 Z. z. o Vojenskom spravodajstve, Zák. č. 67/1992 Zb. o Vojenskom obrannom spravodajstve. Zák. č. 46/1993 Z. z. o Slovenskej informačnej službe.

²⁸ § 2 ods. 6 Zák. č. 46/1993 Z. z. o Slovenskej informačnej službe.

²⁹ § 15 ods. 2 Zák. č. 46/1993 Z. z. o Slovenskej informačnej službe.

³⁰ § 17 ods. 1, 2 Zák. č. 46/1993 Z. z. o Slovenskej informačnej službe.

³¹ § 2, ods. 1, 2, 4 Zák. č. 46/1993 Z. z. o Slovenskej informačnej službe.

³² § 1 ods. 3 a § 16 Zák. č. 46/1993 Z. z. o Slovenskej informačnej službe.

³³ § 8 Zák. č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

³⁴ Dôvodová správa k návrhu zákona o Úrade civilného spravodajstva.

Literatúra:

DESET, M. *Prostriedky zabezpečovania informácií dôležitých pre trestné konanie a právo na súkromie*. Bratislava. Typy Universitatis Tyrnaviensis a Veda 2016.

DRGONEC, J. *Ústava Slovenskej republiky. Komentár*. 2. vydanie. Šamorín: Heuréka, 2007, s. 175.

SVÁK, J. *Ochrana ľudských práv v troch zväzkoch*. II. zväzok. Bratislava: Eurokódex, 2011.

Šimovček, I. a kol. *Trestné právo procesné*. 2. vydanie. Plzeň, Aleš Čeněk, 2016.

Vývoj právnej úpravy oznámenie údajov o telekomunikačnej prevádzke v trestnom konaní

The Legislation Development of Notification the Telecommunications Operation in Criminal Proceedings

Jozef Čentíš¹

Abstrakt: V príspevku autor venuje pozornosť vývoju právnej úpravy oznámenia údajov o telekomunikačnej prevádzke v slovenskom trestnom konaní. Pozornosť zameriava na úpravu tohto inštitútu od jeho ustanovenia v slovenskom Trestnom poriadku až po súčasnú právnu úpravu. Vyjadruje sa k zmenám v úprave tohto inštitútu, ktoré vyplynuli z poznatkov aplikačnej praxe, ako aj rozhodovacej činnosti Ústavného súdu Slovenskej republiky. V príspevku vyjadruje niektoré námety pro futuro.

Abstract: The present paper addresses the development of rules enshrined in national legislation pertinent to communication of data on telecommunications operation in criminal proceedings in Slovakia. Primarily, the author focuses on the alterations/modifications in the arrangements of this institute since its institution into the Criminal Code up until the current legal rules. Further, he expresses his opinion regarding the changes which resulted from the new knowledge and information accumulated from practical application as well as from the decision-making activity of the Constitutional Court of the Slovak Republic. In the paper he also offers some 'pro futuro' suggestions.

Kľúčové slová: spravodlivosť, súkromie, zásah, orgán činný v trestnom konaní, súd, Trestný poriadok, telekomunikačná činnosť, telekomunikačná prevádzka, telekomunikačné tajomstvo, trestné konanie, trestný čin.

Key words: justice, privacy, interference or intervention, law enforcement authority, court, Criminal Code, telecommunications activity, telecommunications operation, telecommunications secrecy, criminal proceedings, criminal offence.

Úvod

Základným predpokladom riadneho výkonu spravodlivosti v demokratickom právnom štáte, je dodržovanie nielen ústavných, ale aj zákonných medzí pre zabezpečovanie a vykonávanie dôkazov. Preto postup ktoréhokoľvek orgánu činného v trestnom konaní alebo súdu, vybočujúceho z rámca procesných predpisov v tomto ohľade, je v rozpore s ústavnosťou štátu a vo svojich dôsledkoch znehodnocuje aj samotný účel trestného konania.² Uvedeným okolnostiam je potrebné venovať pozornosť aj v súvislosti s inštitútom oznámenia údajov o telekomunikačnej prevádzke v trestnom konaní. K obmedzeniu osobnej integrity a súkromia fyzickej osoby (t. j. k prelomeniu ochrany) pri tomto inštitúte môže dôjsť zo strany verejnej moci len celkom výnimočne a ak je to nevyhnutné, a účelu sledovaného verejným záujmom nemožno dosiahnuť inak. Pri nedodržaní tejto podmienky ide o zásah protiústavný. Stíhanie trestných činov je ústavne aprobovateľným verejným záujmom, len ak sa verejná moc pohybuje vo vnútri rámca predvídaného zákonom. Ak umožňuje trestné právo realizáciu verejného záujmu na stíhaní trestnej činnosti pomocou robustných a osobnú integritu fyzickej osoby obmedzujúcich nástrojov, potom ich

¹ Prof. JUDr. Jozef Čentíš, PhD. Právnická fakulta Univerzita Komenského v Bratislave, Generálna prokuratúra Slovenskej republiky.

² Primerane pozri IV. ÚS ČR 1556/07.

použitie musí rešpektovať ústavnoprávne limity.³ Ak je v priebehu trestného konania porušený niektorý z ústavných limitov zásahov do súkromia, potom nie sú rešpektované najmä články 13 ods. 4, 16 ods. 1, 19 ods. 2 a 3 a 22 Ústavy Slovenskej republiky (ďalej len „Ústava“), pretože tento vytvára priestor a zároveň ustanovuje hranice obmedzenia súkromia. Navyše zásah do súkromia je v zásade obmedzený predovšetkým nevyhnutnosťou takéhoto postupu. V opačnom prípade totiž hrozí nebezpečenstvo, že sa výkon verejnej moci v trestnom konaní stane nástrojom ľubovôle jej dočasných držiteľov proti jednotlivcovi.⁴

I. Pôvodná právna úprava

V podmienkach právneho poriadku Slovenskej republiky sa zákonom č. 457/2003 Z. z., ktorým sa mení a dopĺňa zákon č. 141/1961 Zb. o trestnom konaní súdnom (Trestný poriadok) v znení neskorších predpisov a o zmene a doplnení niektorých zákonov ustanovili podmienky postupu pri poskytovaní a zaobstarávaní údajov o uskutočnenej telekomunikačnej činnosti, ktoré boli predmetom telekomunikačného tajomstva, alebo na ktoré sa vzťahovala ochrana osobných údajov alebo sprostredkovacích údajov a to úpravou § 88 ods. 9 a 10 Trestného poriadku (ďalej len „starý Trestný poriadok“).

Podľa 88 ods. 9 starého Trestného poriadku *„Ak je na objasnenie skutočnosti dôležitej pre trestné konanie o úmyselnom trestnom čine potrebné zistiť údaje o uskutočnenej telekomunikačnej činnosti, ktoré sú predmetom telekomunikačného tajomstva alebo na ktoré sa vzťahuje ochrana osobných údajov alebo sprostredkovacích údajov, nariadi pred začatím trestného stíhania alebo v prípravnom konaní sudca na návrh prokurátora, v konaní pred súdom aj bez takého návrhu sudca alebo predsedu senátu, aby ich právnická osoba alebo fyzická osoba, ktorá vykonáva telekomunikačnú činnosť, oznámila v konaní pred súdom sudcovi alebo predsedovi senátu a v prípravnom konaní prokurátorovi, vyšetrovateľovi alebo policajnému orgánu.“*

Podľa dôvodovej správy k návrhu zákona č. 457/2003 Z. z. (...) jednalo sa najmä o „záznamy, ktoré obsahovali identifikačné účastnícke číslo mobilného telefónu, dátum a čas začiatku hovoru, dobu trvania hovoru, číslo volanej stanice, označenie základnej stanice, ktorá zachytávala hovor v okamžiku spojenia a označenie základnej stanice, ktorá sprostredkovala hovor v okamžiku jeho ukončenia. Podľa 88 ods. 9 starého Trestného poriadku *„Príkaz na zistenie a oznámenie údajov o uskutočnenej telekomunikačnej činnosti sa musí vydať písomne a musí sa odôvodniť.“*

Uvedený postup bolo možné použiť v celom trestnom konaní pre akýkoľvek úmyselný trestný čin. Subjektom oprávneným rozhodovať o aplikácii tohto inštitútu (vydať príkaz na zistenie a oznámenie údajov o uskutočnenej telekomunikačnej činnosti) bol predseda senátu a v prípravnom konaní sudca na návrh prokurátora.

II. Právna úprava oznamovania údajov o telekomunikačnej prevádzke v novom Trestnom poriadku

Dňa 1. januára 2006 nadobudol účinnosť zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov (ďalej len „nový Trestný poriadok“), ktorý došlo v ustanovení § 116 k úprave oznamovania údajov o telekomunikačnej prevádzke v slovenskom trestnom konaní pod názvom „odpočúvanie a záznam telekomunikačnej prevádzky“, pričom tento názov zahŕňal aj

³ Primerane pozri I. ÚS ČR 631/05.

⁴ Kallab, J.: Zločin a trest, Úvahy o základoch trestného práva, Praha, J. R. Vilímek, 1916, s. 8. In: II. ÚS ČR 2806/08.

úpravu § 115 nového Trestného poriadku. Uvedené ustanovenia Trestného poriadku bolo možné nasledovne rozlíšiť takto:

- v ustanovení § 115 nového Trestného poriadku bol (je) ustanovený postup odpočúvania a zaznamenávania telekomunikačnej prevádzky, ktorá prebieha v aktuálnom čase alebo v budúcnosti a postup zisťovania a využívania obsahových údajov alebo prevádzkových údajov prenášaných v reálnom čase prostredníctvom počítačového systému;
- v ustanovení § 116 Trestného poriadku bol (je) ustanovený postup zisťovania a oznámenia údajov o telekomunikačnej prevádzke, ktorá sa uskutočnila v minulosti a postup zisťovania a využívania obsahových údajov alebo prevádzkových údajov prenášaných prostredníctvom počítačového systému.

Na tomto mieste možno označiť zaradenie týchto inštitútov, ktoré ustanovovali odlišnú možnosť zásahu do základných práv a slobôd, najmä do práva na súkromie, za nedôslednosť zákonodarcu. V odbornej literatúre sa zvyčajne zdôrazňovala potreba odlíšenia týchto inštitútov aj z hľadiska ich označenia. Konkrétne ponechanie označenia „*odpočúvanie a záznam telekomunikačnej prevádzky*“ len vo vzťahu k § 115 Trestného poriadku; zároveň ustanovenie § 116 Trestného poriadku označiť ako „*oznámenie údajov o telekomunikačnej prevádzke*.“⁵

II.1 Predpoklady aplikácie odpočúvania a záznamu telekomunikačnej prevádzky (§ 116 nového Trestného poriadku)

Predpokladom aplikácie odpočúvania a záznamu telekomunikačnej prevádzky (§ 116 nového Trestného poriadku) bolo splnenie týchto kumulatívnych podmienok:

- a) existencia trestného konania,
- b) existencia úmyselného trestného činu ako predmetu trestného konania
- c) objasnení skutočností dôležitých pre trestné konanie,
- d) uskutočnená telekomunikačná prevádzka.⁶

Ad a) Existencia trestného konania. Prvou podmienkou ustanovenou v § 116 ods. 1 nového Trestného poriadku bola existencia ustanovenej existencia trestného konania, ktorým sa rozumie podľa § 10 ods. 15 nového Trestného poriadku konanie podľa tohto zákona. Trestný poriadok umožňoval zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke v celom trestnom konaní.

Ad b) Existencia úmyselného trestného činu ako predmetu trestného konania. Druhou podmienkou použitia tohto inštitútu bola existencia úmyselného trestného činu ako predmetu trestného konania. Na aplikáciu tohto inštitútu postačovala existencia akéhokoľvek úmyselného trestného činu ako predmetu trestného konania. Podľa odbornej literatúry táto skutočnosť bola v rozpore s článkom 8 ods. 2 Dohovoru o ochrane ľudských práv a slobôd (ďalej len „Dohovor“), konkrétne s jeho požiadavkou, aby štátny orgán zasiahol do súkromného a rodinného života, obdobia a korešpondencie len v prípadoch, keď je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom a zločinnosti, ochrany zdravia alebo morál-

⁵ K uvedenému nedostatku podrobnejšie pozri ČENTĚŠ, J.: *Odpočúvanie – procesnoprávne a hmotnoprávne aspekty*. Bratislava: C. H. Beck, 2013, s. 90 a nasl. Pozri aj ZÁHORA, J.: *Uchovanie počítačových údajov a ochrana súkromia*. Justičná revue, 63, 2011, č. 6–7, s. 904–913.

⁶ Pozri aj MINÁRIK, Š. a kol.: *Trestný poriadok – stručný komentár*, Iura Edition, Bratislava, druhé, prepracované a doplnené vydanie, 2010, s. 376.

ky alebo ochrany práv a slobôd iných. Naplnenie týchto podmienok v prípade prečinov je ťažko predstaviteľné, až vylúčené.⁷

Túto podmienku bolo potrebné porovnať s článkom 1 ods. 1 Smernice Európskeho parlamentu a Rady 2006/24/ES z 15. marca 2006 o uchovávaní údajov vytvorených alebo spracovaných v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb alebo verejných komunikačných sietí a o zmene a doplnení smernice 2002/58/ES⁸ (ďalej len „Smernica 2006/24/ES“). Z článku 1 ods. 1 Smernice 2006/24/ES vyplýva jej účel, ktorým je harmonizácia predpisov členských štátov, ktoré sa týkajú povinnosti poskytovateľov verejne dostupných služieb elektronických komunikácií alebo verejných komunikačných sietí, pokiaľ ide o uchovávanie prevádzkových údajov alebo lokalizačných údajov, ktoré sú nevyhnutné k identifikácii účastníka či registrovaného užívateľa s cieľom „zaistiť dostupnosť týchto údajov na účely vyšetrovania, odhaľovania a stíhania závažných trestných činov.“ Smernica 2006/24/ES nedefinuje pojem „závažný trestný čin“, preto jeho vymedzenie je ponechané na riešenie vo vnútroštátnych predpisoch. Podľa hodnotiacej správy Komisie Rade a Európskemu parlamentu o Smernici 2006/24/ES, väčšina členských štátov vymedzila pojem „závažný trestný čin“ odkazom na minimálnu dobu odňatia slobody, možnosť uložiť trest odňatia slobody alebo na zoznam trestných činov definovaných v právnych predpisoch. V podmienkach Slovenskej republiky nie je definovaný pojem „závažný trestný čin“. V § 10 a 11 Trestného zákona sú pri trestnom čine použité pojmy „prečin“, „zločin“ a „obzvlášť závažný zločin“, nie však „závažný trestný čin“.

Z uvedených dôvodov podmienka úmyselného trestného činu (vyjadrená v § 116 ods. 1 nového Trestného poriadku) sa javila ako príliš liberálna z hľadiska charakteru možného zásahu do práva na súkromie, a to aj s prihliadnutím na článok 1 ods. 1 Smernice 2006/24/ES.

Ad c) Objasnenie skutočností dôležitých pre trestné konanie. Zo znenia § 116 ods. 1 nového Trestného poriadku vyplývalo, že vydanie príkazu na zistenie a oznámenie údajov o uskutocnenej telekomunikačnej prevádzke bolo v podstate podmienené sledovaným účelom, ktorým bolo „objasnení skutočností dôležitých pre trestné konanie“. Takáto možnosť zásahu do práva na súkromie bola formulovaná veľmi široko a neurčito a umožňovala vyžiadanie a použitie predmetných údajov zo strany štátnych orgánov v podstate vždy, ak bolo možné nájsť súvislosť s prebiehajúcim trestným konaním. Závažnosť tohto inštitútu možno zvýrazniť aj tým, že zistenie údajov o tom, s kým určitá osoba komunikuje, ako často komunikuje, z akého miesta komunikuje, akými prostriedkami môže prispieť k zisteniu podstatných údajov o súkromí tejto osoby.

Ad d) Uskutočnená telekomunikačná prevádzka. Možno uviesť, že tento inštitút sa vzťahoval na zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke, ktoré boli predmetom telekomunikačného tajomstva alebo sa ne vzťahuje ochrana osobných údajov. Uvedené ustanovenie umožňovalo zisťovanie údajov, ktoré boli prenášané prostredníctvom počítačového systému.

II.2 Nedostatky úpravy § 116 nového Trestného poriadku

Okrem vyššie uvedených nedostatkov úpravy § 116 nového Trestného poriadku možno poukázať aj na absenciu jasných a detailných pravidiel obsahujúcich minimálne požiadavky na zabezpečenie uchovávaných údajov, ktoré by zaručovali, že nedôjde k ich poskytnutiu a k použitiu k iným, než zákonom ustanoveným účelom. Išlo najmä o zamedzenie prístupu tretích osôb

⁷ Pozri MINÁRIK, Š.: Zo súdnej praxe, 2012 č. 4, s. 153.

⁸ Ú.v. EÚ L 105 z 13. apríla 2006.

a ustanovenie procedúry ich zničenia,⁹ obdobne tak, ako to ustanovoval § 115 ods. 8 nového Trestného poriadku.

V súvislosti s týmto nedostatkom možno poukázať na rozhodovaciu činnosť Európskeho súdu pre ľudské práva, ktorý pri konkretizácii uvedených požiadaviek na právnu úpravu umožňujúcu zásah do súkromia zo strany orgánu verejnej moci v podobe použitia záznamov telefonických hovorov, tajného dohľadu, zberu informácií a dát zo súkromnej (osobnostnej) sféry konštatoval, že je „vopred nutné vymedziť jasné a detailné pravidlá upravujúce rozsah a použitie takéhoto zásahu, ustanoviť minimálne požiadavky na dĺžku, spôsob uloženia získaných informácií a údajov, ich použitie, prístup tretích osôb k nim, a zakotviť postupy vedúce k ochrane celistvosti a dôvernosti údajov a tiež k ich zničeniu, a to spôsobom, aby jednotlivci disponovali dostatočnými zárukami proti riziku ich zneužitia a svojvoľe. Nevyhnutnosť disponovať takýmito zárukami je o to väčšia, keď sa jedná o ochranu osobných údajov podrobených automatickému spracovaniu, najmä pokiaľ sú tieto údaje využívané k policajným cieľom a v situácii, keď sa dostupné technológie stávajú stále komplikovanejšími. Vnútroštátne právo musí najmä zaručiť, že zhromaždené údaje sú skutočne relevantné a nie sú prehnané vzhľadom k účelu, na ktorý boli zaistené a ďalej, že sú uchovávané vo forme umožňujúcej identifikáciu osôb počas doby nepresahujúcej nevyhnutnú mieru k dosiahnutiu účelu, pre ktorú boli zaistené.“¹⁰

Ďalším nedostatkom podľa odbornej literatúry bola tiež absencia náležitosti príkazu na zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke. Účelom tejto úpravy bolo, aby súd pri svojom rozhodovaní disponoval všetkými dostupnými informáciami, napr. o užívateľovi alebo majiteľovi užívateľskej adresy, či zariadenia. Zároveň bolo vhodné tiež ustanoviť možnosť, aby súhlas k poskytnutiu dát mohol dať aj užívateľ telekomunikačného zariadenia, ku ktorému sa majú údaje o uskutočnenej telekomunikačnej prevádzke vzťahovať. V takomto prípade by nebolo potrebné vydať príkaz na zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke.

K určitosti právnej úpravy § 116 nového Trestného poriadku bolo potrebné ustanoviť tiež podmienku tzv. subsidiarity zisťovania údajov o uskutočnenej telekomunikačnej prevádzke, formuláciou „*nemožno sledovaný účel dosiahnuť inak alebo inak by bolo jeho dosiahnutie podstatne sťažené.*“ Doplnenie § 116 ods. 1 nového Trestného poriadku o túto formuláciu znamenalo prehlásenie zásady primeranosti a zdržanlivosti (§ 2 ods. 2 Trestného poriadku), ako aj subsidiarity použitia tohto inštitútu.¹¹

Podstatnou udalosťou pre ďalšiu úpravu § 116 nového Trestného poriadku nesporne bolo to, že skupina 31 poslancov Národnej rady Slovenskej republiky (ďalej len „národná rada“) dňa 10. októbra 2012 podala Ústavnému súdu Slovenskej republiky (ďalej len „ústavný súd“) návrh na začatie konania o súlade právnych predpisov v súvislosti s uchovávaním prevádzkových a lokalizačných údajov o elektronickej komunikácii (ďalej len „návrh“). Návrh bol podaný za účelom začatia konania o súlade § 58 ods. 5, 6 a 7, § 63 ods. 6 zákona o elektronických komunikáciách, § 116 Trestného poriadku a § 76a ods. 3 zákona Národnej rady Slovenskej republiky č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov (ďalej len „zákon o Policajnom zbore“) s ustanoveniami čl. 1 ods. 1, čl. 13 ods. 4, čl. 16 ods. 1, čl. 19 ods. 2, 3. Čl. 22, čl. 26 Ústavy, čl. 7 ods. 1, čl. 10 ods. 2, 3, čl. 13, čl. 17 Listiny Základných práv a slobôd (ďalej len „Listina“), čl. 8,

⁹ Primerane pozri Pl. ÚS ČR 24/10.

¹⁰ Preambula a článok 5 Dohovoru o ochrane dát a zásada č. 7 Odporúčania Rady ministrov č. R (87) zo 17. septembra 1987 týkajúce sa úpravy využitia osobných údajov v policajnom sektore, Weber a Savaria v. Nemecko z 29. júna 2006 a Liberty a ostatní v. Spojené kráľovstvo z 1. júla 2008, In: Pl. ÚS ČR 24/10.

¹¹ Podrobnejšie pozri ČENTĚŠ, J.: Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. Bratislava: C. H. Beck, 2013, s. 146 a 232.

čl. 10 Dohovoru a čl. 7, čl. 8, čl. 11, čl. 52 ods. 1 Charty základných práv Európskej únie (ďalej len „Charta“).

Ústavný súd o podanom návrhu rozhodol nálezom sp. zn. PL.ÚS 10/2014 z 29. apríla 2015 (publikovaný v Zbierke zákonov pod č. 139/2015 Z. z.) tak, že ustanovenia § 58 ods. 5 až ods. 7 a § 63 ods. 6 zákona o elektronických komunikáciách v znení neskorších predpisov, § 116 Trestného poriadku a § 76a ods. 3 zákona o Policajnom zbore nie sú v súlade s čl. 13 ods. 4, čl. 16 ods. 1, čl. 19 ods. 2 a 3 a čl. 22 Ústavy, čl. 7 ods. 1, čl. 10 ods. 2 a 3 a čl. 13 Listiny, čl. 8 Dohovoru a čl. 7, čl. 8 a čl. 52 ods. 1 Charty. Podľa čl. 125 ods. 3 Ústavy dňom vyhlásenia tohto nálezu v Zbierke zákonov Slovenskej republiky stratili účinnosť ustanovenia § 116 Trestný poriadok, § 76a ods. 3 zákona o Policajnom zbore v a ustanovenia § 58 ods. 5 až 7 a § 63 ods. 6 zákona o elektronických komunikáciách. V zmysle tohto nálezu ak národná rada neuvedie tieto ustanovenia do súladu s čl. 13 ods. 4, čl. 16 ods. 1, čl. 19 ods. 2 a 3 a čl. 22 Ústavy, čl. 7 ods. 1, čl. 10 ods. 2 a 3 a čl. 13 Listiny a s čl. 8 Dohovoru, strácajú po šiestich mesiacoch od vyhlásenia tohto nálezu v Zbierke zákonov Slovenskej republiky platnosť.

III. Súčasná právna úprava oznamovania údajov o telekomunikačnej prevádzke v novom Trestnom poriadku

V nadväznosti na uvedený nález národná rada schválila nové znenie § 116 nového Trestného poriadku a to v článku III zákona č. 397/2015 Z. z., ktorým sa na účely Trestného zákona ustanovuje zoznam látok s anabolickým alebo iným hormonálnym účinkom a ktorým sa menia a dopĺňajú niektoré zákony (ďalej len „zákon č. 397/2015 Z. z.“), ktorý nadobudol účinnosť 1. januára 2016.

Zákonom č. 397/2015 Z. z. sa zmenil názov ustanovenia § 116 Trestného poriadku, ktorý znie „Oznámenie údajov o telekomunikačnej prevádzke“, čím došlo aj k rozlíšeniu tohto ustanovenia od ustanovenia § 115 Trestného poriadku (odpočúvanie a záznam telekomunikačnej prevádzky).

Uvedeným zákonom zároveň došlo aj k zmene zákonných podmienok k oznámeniu údajov o telekomunikačnej prevádzke. Predpokladom aplikácie inštitútu oznámenia údajov o telekomunikačnej prevádzke (§ 116 nového Trestného poriadku) je splnenie týchto zákonných podmienok:

- a) existencia trestného konania,
- b) existencia taxatívne určeného úmyselného trestného činu alebo existencia trestného činu, pri ktorom bol spôsobený následok na zdraví poškodeného ako predmetu trestného konania,
- c) nevyhnutná potreba údajov, ktoré sa využijú pri objasnení skutočností dôležitých pre trestné konanie,
- d) subsidiarita použitia tohto inštitútu.
- e) uskutočnená telekomunikačná prevádzka.

Z hľadiska zákonných podmienok ustanovených v § 116 nového Trestného poriadku možno zvýrazniť najmä dve podstatné zmeny, ktorými sú úprava trestných činov a subsidiarita použitia tohto inštitútu.

Vo vzťahu k okruhu trestných činov možno uviesť, že zákonodarca túto zákonnú podmienku rieši tromi spôsobmi, ktorými sú:

- existencia taxatívne určeného úmyselného trestného činu ustanoveného v Trestnom zákone (úmyselný trestný čin, za ktorý zákon ustanovuje trest odňatia slobody, ktorého horná

hranica je najmenej tri roky, trestný čin ochrany súkromia v obydlí, podvodu, nebezpečného vyhrážania, nebezpečného prenasledovania, šírenia poplášnej správy, podnecovania, schvaľovania trestného činu),

- existencia trestného činu, ktorým bola spôsobená ťažká ujma na zdraví alebo smrť alebo
- existencia iného úmyselného trestného činu, pri ktorom na konanie zaväzuje medzinárodná zmluva.

Ďalej zákonodarca v § 116 ods. 1 nového Trestného poriadku ustanovil tzv. subsidiaritu použitia tohto inštitútu, ktorá je vyjadrená v formulácii „*nemožno sledovaný účel dosiahnuť inak alebo inak by bolo jeho dosiahnutie podstatne sťažené*.“ Doplnenie § 116 ods. 1 nového Trestného poriadku o túto formuláciu možno vnímať ako prehlbenie zásady primeranosti a zdržanlivosti (§ 2 ods. 2 Trestného poriadku). Takouto právnou úpravou je tento inštitút legitimovaný ako ultima ratio posledné opatrenie kriminálnej politiky, keď účelom je ochrana spoločnosti pred páchatelmi trestných činov. Rozsah povolenia vychádza v každej konkrétnej trestnej veci z individuálnych podmienok. Je to jednak rozvrh časový, teda dĺžka doby na ktorú je vykonávanie úkonu povolené. Čo sa týka časového rozsahu povolenia vždy musia byť zohľadnená primeranosť tejto doby, ide teda o dobu nevyhnutne nutnú, po ktorú má byť zasahované do práv iného, to aj zodpovedá zásade zdržanlivosti a primeranosti.

Podstatnou okolnosťou ustanovenou v zákone č. 397/2015 Z. z. bolo aj to, že ustanovenie § 116 ods. 2 nového Trestného poriadku ustanovuje náležitosti vydaného príkazu na zistenie a oznámenie údajov o telekomunikačnej prevádzke, ktorý vydáva predseda senátu a pred začatím trestného stíhania alebo v prípravnom konaní sudca pre prípravné konanie na návrh prokurátora. Samotný príkaz musí byť písomný a odôvodnený aj skutkovými okolnosťami. Príkaz na zistenie a oznámenie údajov o telekomunikačnej prevádzke sa musí vydať písomne a odôvodniť; súčasťou príkazu je aj spôsob, rozsah a lehota oznámenia údajov. Ak sa príkaz týka konkrétneho používateľa, musí byť v ňom uvedená jeho totožnosť, ak je známa.

Významnou obsahovou náležitosťou príkazu na zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke je jeho odôvodnenie. Tento príkaz má obsahovať také odôvodnenie, aby bol z neho zrejmy sledovaný legitímny cieľ, ktorý by umožnil posúdiť či bol zásah nevyhnutný v demokratickej spoločnosti podľa článku 8 ods. 2 Dohovoru.¹² Navyše Trestný poriadok ustanovuje požiadavku odôvodnenia príkazu na zistenie a oznámenia údajov o telekomunikačnej prevádzke aj skutkovými okolnosťami. Splnenie tejto podmienky vyžaduje, aby súd konkrétne odôvodnil skutočnosti, na základe ktorých boli naplnené zákonné podmienky na vydanie tohto príkazu. Tieto podmienky nie sú naplnené v prípade iba formálneho (všeobecného) odôvodnenia príkazu, ktoré spočíva iba v citácii príslušných právnych predpisov a absencii skutkových okolností, z ktorých vychádza. Z týchto dôvodov nemožno akceptovať postup, ktorý zotrváva len na formálnych náležitostiach a celkom rezignuje na splnenie materiálnych podmienok potrebných na vydanie tohto príkazu.

Trestný poriadok tiež ustanovuje dobu použitia tohto inštitútu tak, že ak nejde o zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke, zisťovanie a oznamovanie týchto údajov môže trvať najviac šesť mesiacov; tento čas môže v prípravnom konaní na písomný a odôvodnený návrh prokurátora sudca pre prípravné konanie predĺžiť vždy o ďalšie dva mesiace, a to aj opakovane. Príkaz na zistenie a oznámenie údajov o telekomunikačnej prevádzke sa doručuje podniku poskytujúcemu verejné siete alebo služby.

V ustanovení § 116 ods. 3 nového Trestného poriadku zákonodarca ustanovil povinnosť zničenia údaju získaného použitím tohto inštitútu. Tento postup sa uplatní v prípade, ak sa pri tom-

¹² Niemetz v. Nemecko zo 16. decembra 1992.

to inštitúte vôbec nezistili skutočnosti dôležité pre trestné konanie. Táto skutočnosť nastane vtedy, keď zistený údaj nemá žiadnu súvislosť s predmetom trestného konania. V takomto prípade príslušný orgán, ktorého rozhodnutím trestná vec právoplatne skončila (orgán činný v trestnom konaní alebo súd) je povinný získaný údaj zničiť. K zničeniu záznamu má pritom prichádzať *ex officio*.¹³

V prípade zničenía záznamu Trestný poriadok tiež ustanovuje povinnosť:

- založenia zápisnice o zničení záznamu do spisu,
- upovedomenia určitých osôb o zničení záznamu.

Trestný poriadok ustanovuje povinnosť vyhotoviť zápisnicu o zničení záznamu. Táto zápisnica sa zakladá do spisu.

Z Trestného poriadku vyplýva, že povinnosť upovedomenia o zničení záznamu sa týka osoby (ak je známa), ktorej sa použitie tohto inštitútu týka (§ 116 ods. 3 nového Trestného poriadku). Možno uviesť, že táto povinnosť sa neuplatní vo vzťahu k osobe, ktorá má právo nazeráť do spisov napr. obvinený alebo poškodený (§ 69 nového Trestného poriadku), ktorý sa o zničení majú možnosť dozvedieť zo zápisnice o zničení, ktorá sa založí do spisu.

Ak dotknutá osoba nemá možnosť nazeráť do spisu, je orgán, ktorého rozhodnutím bola vec právoplatne skončená a posteriori povinný informovať túto osobu o zničení záznamu. Informácia obsahuje označenie súdu, ktorý vydal príkaz na zistenie a oznámenie údajov o telekomunikačnej prevádzke, a údaj o lehote, počas ktorej sa tento príkaz vykonával. Súčasťou informácie je poučenie o práve podať v lehote dvoch mesiacov od jej doručenia návrh na preskúmanie zákonnosti príkazu na zistenie a oznámenie údajov o telekomunikačnej prevádzke Najvyššiemu súdu Slovenskej republiky.¹⁴ Informáciu podá orgán, ktorého rozhodnutím sa vec právoplatne skončila, a v konaní pred súdom predseda senátu súdu prvého stupňa do troch rokov od právoplatného skončenia trestného stíhania v danej veci.

Možno tiež doplniť, že Trestný poriadok ustanovuje určité výnimky z povinnosti upovedomenia dotknutej osoby o zničení záznamu (§ 116 ods. 5). Vzhľadom na pomerne široký okruh osôb, ktoré majú možnosť nazeráť do spisu (§ 69 nového Trestného poriadku), zrejme nebude použitie týchto výnimiek obvyklé. Pri plnení tejto povinnosti je potrebné analogicky prihliadnuť aj na rozhodovaciu činnosť Európskeho súdu pre ľudské práva, ktorú zaujal vo vzťahu k odpočúvaniu. Podľa tejto rozhodovacej činnosti odpočúvaná osoba by mala byť informovaná o použití opatrení na jej sledovanie ihneď, ako je to možné bez toho, aby sa zmaril účel ich použitia.¹⁵ Obzvlášť to platí o odpočúvaných osobách, ktoré sa o tom nemôžu dozvedieť v rámci trestného konania, resp. nemajú právo nazeráť do spisu. Takýmto osobám sa síce pri upovedomení o zničení záznamu neposkytujú informácie, ktoré sa zistili pri odpočúvaní, pretože takáto požiadavka nevyplýva z rozhodovacej činnosti Európskeho súdu pre ľudské práva; postačujúce je, ak sa dotknutá osoba vyrozumie o samotnom fakte odpočúvania, aby sa mohla domáhať preskúmania jeho zákonnosti.¹⁶ Na druhej strane možno zvýrazniť, že podľa rozhodovacej činnosti Európskeho súdu pre ľudské práva aktivita alebo nebezpečenstvo, ku ktorému sledovacie opatrenia smerujú, môže pretrvávajúť roky, či dokonca desaťročia po tom, čo bolo od týchto opatrení upustené. Následné upozornenie každej osoby dotknutej opatrením, by mohlo kompromitovať dlhodobý cieľ, ktorým bolo pôvodne nariadenie sledovania odôvodnené. Navyše takéto upozornenie

¹³ Primerane pozri II. ÚS ČR 789/06.

¹⁴ K ďalšiemu postupu pozri § 362f a 362g Trestného poriadku.

¹⁵ Weber a Saravia v. Nemecko z 29. júna 2006.

¹⁶ DESET, M.: Niektoré aspekty legality odpočúvania. In: Právny obzor, 93, 2010, č. 3, s. 253.

by hrozilo prispieť k odhaleniu pracovných metód spravodajských služieb, pole ich pôsobnosti a prípadne aj totožnosti ich príslušníkov.¹⁷

Ak sa využitím postupu podľa § 116 ods. 1 nového Trestného poriadku zistili skutočnosti významné pre trestné konanie (zakladajúce dôvodné podozrenie z trestného činu uvedeného v § 116 ods. 1 nového Trestného poriadku), údaj sa stáva dôkazom, ktorý môže usvedčovať podozrivého alebo obvineného zo spáchania trestného činu. Na druhej strane môžu byť postupom podľa § 116 ods. 1 nového Trestného poriadku zistené skutočnosti, ktoré vyvíňujú podozrivého alebo obvineného z podozrenia zo spáchania trestného činu. V takomto prípade záznam z odpočúvania byť môže byť použitý ako poklad na vydanie meritórneho rozhodnutia napr. zastavenie trestného stíhania (§ 215 nového Trestného poriadku).

Pre úplnosť možno uviesť, že postup podľa § 116 ods. 1 až 5 nového Trestného poriadku sa rovnako vzťahujú na údaje prenášané prostredníctvom počítačového systému.

Na podklade týchto skutočností možno charakterizovať oznámenie údajov o telekomunikačnej prevádzke v trestnom konaní ako zákonom povolený zásah orgánov verejnej moci do súkromia fyzickej osoby, ktorý im za účelom objasnenia skutočností dôležitých pre trestné konanie umožňuje získať údaje o telekomunikačnej prevádzke (ktoré sú inak predmetom telekomunikačného tajomstva alebo sa na ne vzťahuje ochrana osobných údajov), ktorá sa uskutočnila v minulosti alebo získať obsahové údaje alebo prevádzkové údaje prenášané prostredníctvom počítačového systému, za účelom zabezpečenia dôkazu v trestnom konaní. V tomto prípade ide o poskytnutie požadovaných údajov ex post, teda údajov o telekomunikačnej prevádzke, ktorá sa uskutočnila pred doručením príkazu na zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke.

IV. Záver

Súčasná právna úprava inštitútu oznámenia údajov o telekomunikačnej prevádzke v prevažnej miere reflektovala na zmienený nález ústavného súdu. Vzhľadom na túto právnu úpravu je potrebné prísne posudzovať splnenie zákonných podmienok ustanovených k využitiu tohto inštitútu, ktorým sa zasahuje najmä do práva na súkromie. Z tohto dôvodu je žiaduce, aby tak aplikčná prax orgánov činných v trestnom konaní a súdov využívala tento prostriedok ako ultima ratio pri zásahoch do súkromia jednotlivca.

Zoznam literatúry

- ČENTĚŠ, J.: Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. Bratislava: C. H. Beck, 2013, 272 s., ISBN 978-80-89603-09-1.
- DESET, M.: Niektoré aspekty legality odpočúvania. Právny obzor, 93, 2010, č. 3, s. 245–255.
- MINÁRIK, Š. a kol.: Trestný poriadok – stručný komentár, druhé, prepracované a doplnené vydanie. Iura Edition, 2010, 1392 s., ISBN 978-80-8078-369-3.
- MINÁRIK, Š.: Zo súdnej praxe, 2012 č. 4, s. 176–179.
- ZÁHORA, J.: Uchovanie počítačových údajov a ochrana súkromia. Justičná revue, 63, 2011, č. 6–7, s. 904–913.

¹⁷ Klass a ostatní v. Nemecko zo 6. septembra 1978.

Príslušnosť súdu na rozhodovanie o použití informačno-technických prostriedkov

Jurisdiction of Courts to Decide Using of Informational-technical Means

Sergej Romža¹

Abstrakt: Použitím informačno-technických prostriedkov, tak v rámci trestného konania, ako aj mimo jeho rámca, dochádza k invazívnemu zásahu do práva na súkromie jednotlivca, ktoré patrí k ústavne garantovaným základným právam. Z uvedeného dôvodu uplatnené prostriedky ochrany tohto základného práva, musia korelovať charakteru a významu chráneného záujmu a zároveň musia poskytovať efektívnu ochranu tohto práva. Zároveň konajúce súdy, ktoré rozhodujú o použití informačno-technických prostriedkov, teda vykonávajú súdnu kontrolu zákonnosti ich použitia, musia spĺňať požiadavky zákonného súdu, pod ktorý je potrebné subsumovať aj ich príslušnosť, a to tak vecnú, ako aj miestnu. Kritériá zakladajúce príslušnosť súdov rozhodujúcich o použití informačno-technických prostriedkov, musia spĺňať kritériá predvídateľnosti a právnej istoty.

Abstract: Using informational-technical means and in the framework of criminal proceedings, as well as outside its framework, there is invasive interference with the right to privacy of individuals belonging to the constitutionally guaranteed fundamental rights. For this reason, applied means of protection of this fundamental right must correlate the nature and importance of the protected interest and also must provide effective protection of this right. At the same time acting courts deciding using of informational-technical means, so exercise judicial review of the legality of their use must comply with the statutory court, under which must be subsumed and their affiliation, both substantive and local. The criteria for establishing the jurisdiction of the courts deciding using of informational-technical means, must meet the criteria of predictability and legal certainty.

Kľúčové slová: Informačno-technické prostriedky; príslušnosť súdu; právomoc súdu; princíp právneho štátu; princíp predvídateľnosti; zákonný sudca; právo na súkromie; policajný zbor; právo na spravodlivé súdne konanie; zákon o ochrane pred odpočúvaním.

Keywords: Informational-technical means; Jurisdiction; jurisdiction; the rule of law; the principle of predictability; statutory judge; the right to privacy; police force; the right to a fair trial; Law on protection against eavesdropping.

I. Všeobecné východiská vzťahujúce sa k právomoci a príslušnosti súdov

Súdy ako štátne orgány s teóriou práva, sú vybavené právomocou a príslušnosťou.²

Právomocou súdu sa rozumie súhrn oprávnení, ktoré zákon priznáva súdom ako štátnym orgánom, na rozdiel od oprávnení, ktoré priznáva iným štátnym orgánom, čím sa súdy ako štátne orgány, odlišujú od iných štátnych orgánov.

Ide o vymedzenie súdnej moci navonok, a to vo vzťahu k iným štátnym orgánom, napríklad orgánom prokuratúry alebo Policajného zboru.³

¹ Doc. JUDr. Sergej ROMŽA, PhD. Právnická fakulta, Univerzita Pavla Jozefa Šafárika Košice, e-mail: sergej.romza@upjs.sk.

² ŠIMOVCÉK, I. a kol.: Trestní právo procesné. Plzeň: Aleš Čeněk, 2011, s. 76.

³ IVOR, J., POLÁK, P., ZÁHORA, J.: Trestné právo procesné I. Bratislava. Wolters Kluwer, 2017, s. 142.

Príslušnosťou súdu sa rozumie vymedzenie okruhu spoločenských vzťahov, na ktoré sa vzťahuje a na ktorých sa vykonáva príslušná právomoc.⁴

Vecná príslušnosť, určuje druh súdu, ktorý je príslušný na vybavenie trestnej veci určitého druhu. Osobitým druhom vecnej príslušnosti je funkčná príslušnosť, ktorá určuje ktorý stupeň súdu je príslušný konať v určitom štádiu trestného konania.⁵

Miestnou príslušnosťou, sa rozumie vymedzenie pôsobnosti medzi viacerými súdmi toho istého stupňa.⁶

Žiada sa osobitne akcentovať, že príslušnosť súdov je reálnym naplnením ústavnej zásady, že nikoho nemožno odňať jeho zákonnému sudcovi, a to v súlade s ust. čl. 48 ods. 1 Ústavy Slovenskej republiky (ďalej len ako „Ústava“).

V zmysle ust. čl. 48 ods. 1 Ústavy „nikoho nemožno odňať jeho zákonného sudcovi. Príslušnosť súdu ustanoví zákon.“

Ústavný súd Slovenskej republiky (ďalej len ako „Ústavný súd“) k uvedenému poznamenáva „účelom práva priznaného podľa tohto ustanovenia je zabezpečiť občanovi, aby ochranu jeho právam poskytol sudca ako predstaviteľ tej zložky súdnej moci, ktorá má právomoc o veci konať, a aby ochranu práva, v rámci súdnej moci, poskytol sudca zo súdu, ktorý je **vecne a miestne príslušný**“.⁷

Legálnu definíciu zákonného sudcu nachádzame v ust. § 3 ods. 3 zákon č. 757/2004 Z. z. o súdoch a o zmene a doplnení niektorých zákonov, v znení neskorších predpisov: „*zákonný sudca je sudca, ktorý vykonáva funkciu sudcu na príslušnom súde a bol určený v súlade so zákonom a s rozvrhom práce, na konanie a rozhodovanie o prejednávanej veci. Ak súd rozhoduje v senáte, zákonnými sudcami sú všetci sudcovia určení podľa rozvrhu práce na konanie a rozhodovanie v senáte*“.

II. Vymedzenie podstaty a účelu využitia informačno-technických prostriedkov

Vymedzenie podstaty, účelu, ale rovnako tak podmienok, za splnenia ktorých môžu oprávnené subjekty využívať informačno-technické prostriedky (ďalej len ako „ITP“), nachádzame tak v ust. § 10 ods. 21 Trestného poriadku, a to v rámci trestného konania, ako aj v ust. § 2 ods. 1 zákona č. 166/2003 Z. z. „o ochrane pred odpočúvaním“.

Ust. § 10 ods. 21 Trestného poriadku, obsahuje legálnu definíciu ITP, ktorými sa rozumejú „*elektrotechnické, rádiotechnické, fototechnické, optické, mechanické, chemické a iné technické prostriedky a zariadenia alebo ich súbory používané utajovaným spôsobom, pri odpočúvaní a zázname prevádzky v elektronických komunikačných sieťach, obrazových, zvukových alebo obrazovozvukových záznamoch alebo pri vyhľadávaní, otváraní a skúmaní zásielok, ak sa ich použitím zasahuje do základných práv a slobôd*“.

Rovnako legálnu definíciu ITP obsahuje aj ust. § 2 ods. 1 zákona č. 166 /2003 Z. z., keď za ITP sa považujú najmä „*elektrotechnické, rádiotechnické, fototechnické, optické a mechanické, chemické a iné technické prostriedky a zariadenia alebo ich súbory používané utajovaným spôsobom pri vyhľadávaní, otváraní, skúmaní vyhodnocovaní poštových zásielok a iných dopravovaných zásie-*

⁴ C.d. v poznámke č. 2, s. 76.

⁵ Tamtiež, s. 77.

⁶ C.d. v poznámke č. 3, s. 143.

⁷ Porov.: II. ÚS 87/01, nález z 12. júla 2012.

lok, odpočúvaní a zaznamenávaní v rámci telekomunikačných činností, vyhotovovaní a využívaní obrazových, zvukových alebo iných záznamov“.

V tejto súvislosti sa žiada poznamenať a pripomenúť zároveň, že nemožno stotožňovať, a teda zamieňať si informačno-technický prostriedok a procesný inštitút (dôkazný prostriedok), prostredníctvom ktorého sa informačný – technický prostriedok realizuje – využíva.

Vzhľadom na vágnosť prezentovaných legálnych definícií informačno-technických prostriedkov, ktorá vyplýva z demonštratívneho legislatívno – technického vymedzenia okruhu prostriedkov a zariadení, ktoré možno subsumovať pod pojem ITP, pozitívne možno zhodnotiť snahu Ústavného súdu SR, v koncentrovanej forme prezentovať podmienky, za splnenia ktorých možno určitý technický prostriedok alebo zariadenie, považovať za informačno-technický prostriedok.

V tejto súvislosti Ústavný súd SR judikoval, že technický prostriedok je možné subsumovať pod legálnu definíciu informačno-technických prostriedkov uvedenú v zákone č. 166/2003 Z. z., ak sú kumulatívne splnené nasledovné podmienky:

- a) Požadovaná technická charakteristika (rádiotechnické, elektrotechnické, fototechnické, optické, mechanické, chemické a iné technické prostriedky a zariadenia alebo ich súbory);
- b) Spôsob použitia („používané utajovaným spôsobom, bez predchádzajúceho súhlasu osoby, voči ktorej sa používajú“);
- c) Účel použitia („pri vyhotovovaní a využívaní obrazových, zvukových alebo iných záznamov“);
- d) Zásah do súkromia osoby, voči ktorej sa informačno-technický prostriedok používa;
- e) Taxatívne určený okruh štátnych orgánov oprávnených používať technický prostriedok (Policajný zbor, Slovenská informačná služba, Vojenské spravodajstvo, Zbor väzenskej a justičnej stráže, Colná správa).
- f) Použitie technického zariadenia, v rozsahu podľa osobitného predpisu.

III. Medzinárodné a ústavné limity súdnej intervencie do používania informačno-technických prostriedkov

V súvislosti s používaním ITP nevyhnutne dochádza k zásahom do základných práv a slobôd, garantovaných tak Ústavou SR, ako aj medzinárodnými dokumentmi, ktorými je Slovenská republika viazaná.

Použitím ITP sa primárne zasahuje do súkromia konkrétnej fyzickej osoby.

V medzinárodných dokumentoch, je právu na súkromie, poskytovaná ochrana, v koncentrovanej forme v ust. čl. 8 ods. 1, 2 Dohovoru o ochrane ľudských práv a základných slobôd (ďalej len ako „Dohovor“).

Podľa čl. 8 ods. 1 Dohovoru „každý má právo na rešpektovanie svojho súkromného rodinného života, obdobia a korešpondencie“.

Právo na súkromie spočíva v práve jednotlivca samostatne sa rozhodnúť podľa vlastného uváženia, či a v kom rozsahu majú byť skutočnosti z jeho súkromného života sprístupnené iným alebo zverejnené.⁸

⁸ ČENTĚŠ, J.: Odpočúvanie – procesnoprávne a hmotnoprávne aspekty, Bratislava: C. H. Beck, 2013, s. 1.

Súkromie je chápané ako priestor, kde sa jednotliviec slobodne vyvíja a realizuje svoju osobnosť podľa vlastných predstáv bez zbytočných obmedzení, príkazov a zákazov ustanovených orgánom verejnej moci.⁹

Účelom práva na súkromie je ochrana jednotlivca pre svojvoľným a neprimeraným zásahom verejnej moci do jeho súkromia.¹⁰

Podľa čl. 8 ods. 2 Dohovoru, nemôžu štátne orgány, do výkonu práva na súkromie zasahovať, s výnimkou prípadov, keď je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom alebo zločinnosti, ochrany zdravia alebo morálky alebo na ochranu práv a slobôd iných.

Podľa čl. 8 ods. 2 Dohovoru, zásah do súkromia, musí byť realizovaný v súlade so zákonom, pričom pojem zákon nemožno vnímať len z formálneho hľadiska, ale komplexne ako súbor právnych noriem doplnených súdnou interpretáciou.¹¹

Zásah do súkromia možno považovať za zásah realizovaný v súlade so zákonom, ak zákon má určitú kvalitu, ktorá sa vyhodnocuje prostredníctvom naplnenia nasledovných referenčných kritérií:

1. Musí byť **prístupný** dotknutej osobe, teda, aby občan mal možnosť vedieť, za akých okolností a podmienok, môže štátny orgán zasiahnuť do jeho práv;
2. Musí byť **dostatočne určitý**, aby umožňoval občanom regulovať ich správanie, podľa podmienok stanovených zákonom. Jednoducho zákon musí občanom umožniť predvídať dôsledky, ktoré môže ich konanie spôsobiť. Požiadavka **predvídateľnosti** teda znamená, že zákon musí byť dostatočne jasný vo svojich pojmoch, aby občanom primerane naznačil, za akých okolností a podmienok sú štátne orgány oprávnené siahnuť po utajení a potenciálne nebezpečnej intervencii s právami na rešpektovanie súkromného a rodinného života, obydľia a korešpondencie.
3. Musí byť **v súlade s princípmi právneho štátu**.¹²

Právo na súkromie je garantované aj na vnútroštátnej právnej úrovni, konkrétne predovšetkým v čl. 16 ods. 1 Ústavy SR, keď ustanovuje, že „*nedotknuteľnosť osoby a jej súkromia je zaručená. Obmedzená môže byť len v prípadoch ustanovených zákonom*“.

IV. Príslušnosť súdu na rozhodovanie o použití ITP

1. Príslušnosť súdu na rozhodovanie o použití ITP, v rámci trestného konania, konkrétne pred začatím trestného stíhania a v prípravnom konaní, je koncipovaná ako osobitná príslušnosť, keď Trestný poriadok v ust. § 24 ods. 4, deklaruje, že pred začatím trestného stíhania a v prípravnom konaní, je príslušný Okresný súd v sídle toho Krajského súdu, v obvode ktorého je súd, ktorý by bol príslušný na konanie o obžalobe. Samozrejme s výnimkou vecí, ktoré patria do pôsobnosti Špecializovaného trestného súdu.

Z uvedeného teda vyplýva, že vecne príslušným súdom na rozhodovanie o použití ITP (pred začatím trestného stíhania a v prípravnom konaní), je Okresný súd v sídle Krajského súdu

⁹ BLAŠKOVÁ, A.: Ochrana obydľia ako súčasť práva na súkromie; Justičná revue, 2011, č. 3, s. 467. Rovnako porov.: Súdny dvor EU ROQUETTE FRÉSES SA z 22. októbra 2002; Najvyšší súd SR, v rozhodnutí pod sp. zn.: 8Sžo 36/2008, definoval súkromie, ako súkromie bezprostredne nadväzujúce na osobu občana – odev, predmety, ktoré má pri sebe, ako aj celú intímnu oblasť človeka, jeho záujmy (aj profesionálne), vzťahy, styky, atď.

¹⁰ C.d. v poznámke č. 8, s. 2.

¹¹ Porov.: MALONE v. SPOJENÉ KRÁLOVSTVO; HUVIG v. FRANCÚZSKO, KLASS v. NEMECKO.

¹² KRUSLIN v. FRANCÚZSKO; HUVIG v. FRANCÚZSKO; KVASNICA v. SLOVENSKO.

a miestne príslušným súdom je Okresný súd v sídle Krajského súdu, v obvode ktorého sa nachádza Okresný súd, ktorý by bol príslušný na konanie o obžalobe, pričom miestne príslušným súdom na konanie o podanej obžalobe, je primárne, súd v obvode ktorého bol trestný čin spáchaný.

Zákonodarca odôvodňuje potrebu a nevyhnutnosť osobitným spôsobom, upraviť príslušnosť súdu rozhodujúceho o použití ITP, v rámci trestného konania, a teda jej koncentráciu na Okresné súdy v sídle Krajských súdov, citlivosťou procesných inštitútov, s realizáciou ktorých je spojené používanie ITP. Zákonodarca pod citlivosťou zrejme mal na mysli zabezpečenie potrebnej miery (stupňa) utajenia vydávaných rozhodnutí, pred ich realizáciou.

Žiada sa v tejto súvislosti poznamenať, že tejto argumentácii možno vcelku porozumieť, jednoducho z aplikačného hľadiska má svoje ratio.

Na strane druhej vyvstáva legitímna otázka, aké garancie poskytuje Okresný súd v sídle Krajského súdu vo vzťahu k zabezpečeniu utajenia vydávaných príkazov, resp. vo všeobecnosti vo vzťahu k rozhodovaniu o použití ITP, ktoré neposkytujú ostatné Okresné súdy, mimo sídla Krajského súdu.

Ide hádam o:

- Osobitné kritériá výberu sudcov rozhodujúcich o použití ITP;
- Vyššiu odbornú erudovanosť;
- Osobitné organizačno-technické opatrenia;

Osobne sa nedomnievam, aby bolo možné pozitívne, uspokojivo a presvedčivo odpovedať na nastolené otázky, a tým odôvodniť aj legitimitu založenia osobitnej príslušnosti Okresných súdov v sídle krajských súdov na rozhodovanie o použití ITP.

2. Ako som už v úvode avizoval, odlišným spôsobom je koncipovaná príslušnosť súdu rozhodujúceho o použití ITP, mimo trestného konania, v režime zákona č. 166/2003 Z. z., o ochrane pred odpočúvaním.

Zákonodarca v § 4a predmetného zákona, ustanovuje príslušnosť súdu na rozhodovaní o použití ITP.

- a) V zmysle ust. § 4a ods. 1 cit. zákona „na rozhodovanie o použití ITP, podľa tohto zákona, je vecne príslušný Krajský súd, s výnimkou, ak ide o vec patriacu do pôsobnosti Špecializovaného trestného súdu.“¹³

Z uvedeného teda vyplýva, že na rozhodovanie o použití ITP, v režime zákona o ochrane pred odpočúvaním, je vecne príslušný Krajský súd oproti režimu Trestného poriadku, kde je založená vecná príslušnosť Okresného súdu v sídle Krajského súdu.

Zákonodarca, túto zmenu v koncepcii vecnej príslušnosti súdov pri rozhodovaní o použití ITP, nijako bližšie neobjasňuje.

V tejto súvislosti možno vysloviť dôvodnú pochybnosť o potrebe a vhodnosti delegovania vecnej príslušnosti na Krajský súd, oproti stavu v režime Trestného poriadku. Nazdávam sa, že pokiaľ je Okresný súd v sídle Krajského súdu dostatočne kompetentný na rozhodovanie o použití ITP, v režime Trestného poriadku, potom by túto kompetenciu zvládol aj v režime zákona o ochrane pred odpočúvaním, teda mimo trestného konania.

¹³ O informačno-technických prostriedkoch rozhodujú sudcovia vecne príslušného súdu určení predsedom tohto súdu. Predseda súdu určí potrebný počet sudcov tak, aby bola zabezpečená neodkladnosť vybavovania tejto súdnej agendy. Mená a priezviská určených sudcov oznámia predsedovia vecne príslušných súdov prezidentovi Policajného zboru, generálnemu riaditeľovi Zboru väzenskej a justičnej stráže, generálnemu riaditeľovi Finančného riaditeľstva Slovenskej republiky a riaditeľovi Slovenskej informačnej služby. Predseda krajského súdu príslušného na udeľovanie súhlasov pre potreby Vojenského spravodajstva aj riaditeľovi Vojenského spravodajstva.

Prípadná argumentácia spočívajúca v tom, že mimo rámca trestného konania, ešte nie je dostatočne precizovaná konštrukcia skutku, či jeho právna kvalifikácia, celkom neobstojí, nakoľko v režime zákona o ochrane pred odpočúvaním, mali by sa nasadzovať (používať) ITP v neskorších štádiách operatívneho rozpracovania veci, kedy je už tak predbežná štruktúra skutku, ako aj jeho právna kvalifikácia, dostatočne adresná.

Navyše ani v rámci trestného konania, v štádiu pred začatím trestného stíhania, kedy na rozhodovanie o použití ITP je vecne príslušným súdom okresný súd v sídle Krajského súdu, nemusí sa vyznačovať konštrukcia skutku, vrátane jeho právnej kvalifikácie, väčšou mierou istoty – adresnosti.

- b) Zákon o ochrane pred odpočúvaním zároveň v ust. § 4a ods. 2 precizuje aj miestnu príslušnosť súdu rozhodujúceho o použití ITP, keď ustanovuje, že „na rozhodovanie o súhlase na použitie ITP, je miestne príslušný Krajský súd, v obvode ktorého má sídlo žiadateľ o vydanie súhlasu na ich použitie alebo jeho organizačný útvar, alebo Krajský súd, v obvode ktorého sa nachádza objekt Zboru väzenskej a justičnej stráže, ak sa majú použiť ITP v tomto objekte“.

Z cit. ustanovenia je zrejmé, že zákonodarca koncipuje miestnu príslušnosť súdu alternatívne, pričom právnou skutočnosťou, ktorá zakladá miestnu príslušnosť súdu je sídlo žiadateľa alebo jeho organizačného útvaru.

V tejto súvislosti som toho názoru, že interpretačné, ako aj aplikačné problémy, zakladá už samotné alternatívne vymedzenie miestnej príslušnosti konajúceho súdu, ktoré sa navyše odvíja (je naviazané) od sídla žiadateľa, alebo jeho organizačného útvaru, bez akýchkoľvek ďalších obmedzujúcich, či spresňujúcich podmienok, ktoré by efektívne zamedzili, či obmedzili možnosti v účelovom postupe žiadateľa, pri zakladaní miestnej príslušnosti súdu.

Jednoducho som toho názoru, že súčasná koncepcia zakladania miestnej príslušnosti súdu rozhodujúceho o súhlase s použitím ITP umožňuje žiadateľovi založiť miestnu príslušnosť ktoréhokoľvek Krajského súdu, v obvode ktorého má žiadateľ organizačný útvar (čo v prípade Policajného zboru prichádza do úvahy každý krajský súd v Slovenskej republike), a to aj v tom prípade, keď v obvode Krajského súdu, ktorému bola podaná žiadosť o udelenie súhlasu s použitím ITP, nie je realizovaná vec, ktorej sa súhlas týka, resp. nie je činný ani organizačný útvar, ktorý túto vec realizuje a nebol v obvode konajúceho Krajského súdu ani spáchaný skutok, ktorého sa týka operatívna činnosť.

Absentuje teda kauzalita medzi konajúcim súdom a miestom spáchania skutku a sídlom, v ktorom je činný organizačný útvar, realizujúci vec.

Som toho názoru, že založenie miestnej príslušnosti súdu rozhodujúceho o udelení súhlasu s použitím ITP, nemôže byť vecou autonómnej úvahy žiadateľa a viery, že žiadateľ možnosť, ktorú mu zákonodarca poskytol vo forme alternatív skutočnosti zakladajúcich túto príslušnosť, účelovo nevyužije, či nezneužije.

Navyše dôvodné pochybnosti a obavy vzbudzuje už samotná skutočnosť, že miestna príslušnosť konajúceho súdu sa alternatívne odvíja zakladá od sídla organizačného útvaru (organizačnej zložky) žiadateľa, pričom v prípade PZ, právomoc zakladať a meniť organizačnú štruktúru jednotlivých útvarov PZ, je zverená, v zmysle ust. § 4 ods. 2,3, ZPZ, ministromi vnútra, na základe interných normatívnych aktov (nariadení Ministra vnútra).

Jednoducho Minister vnútra, na základe cit. kompetenčného ust. môže vo svojej pôsobnosti zriaďovať a rušiť jednotlivé útvary PZ, vrátane ich organizačných zložiek (súčasť), ktoré v súvislosti s rozhodovaním o použití ITP v režime z. č. 166/2003 Z. z., vystupujú v pozícii žiadateľov, a tým aj kreovať právne skutočnosti, ktoré zakladajú miestnu príslušnosť súdu rozhodujúceho o vydávaní súhlasu na použitie ITP.

Popísaným spôsobom sa vytvára potenciálna aj reálna možnosť modifikovať – skutočnosti rozhodujúce pre založenie miestnej príslušnosti konajúceho súdu, na základe zákona, nie však spôsobom ustanoveným zákonom, v dôsledku čoho dochádza k popretiu zásady zákonného sudcu, deklarovanej v ust. čl. 48 ods. 1 Ústavy, ako aj čl. 6 ods. 1 Dohovoru.

Som toho názoru, že spôsob akým sú jednotlivé zákonné podmienky, zakladajúce miestnu príslušnosť Krajského súdu, na rozhodnutie o vydaní súhlasu na použitie ITP, normatívne vyjadrené v ust. § 4a ods. 2 zákona č. 166/2003 Z. z., nespĺňajú požiadavky vyplývajúce z ust. čl. 6 ods. 1 a čl. 8 ods. 1, 2 Dohovoru, ako aj požiadavky vyplývajúce z ust. čl. I Ústavy SR, konkrétne nerešpektuje elementárny princíp právneho štátu a jeho atribútov, princípu predvídateľnosti právnej úpravy a princípu právnej istoty.

Jednoducho som toho názoru, že avizovaná vágnosť normatívnej úpravy, zakladajúcej miestnu príslušnosť konajúceho súdu, vytvára stav, ktorý umožňuje rôznorodý a účelový výklad predmetného ust. § 4a ods. 2 Zákona č. 166/2003 Z. z., čím sa zakladá stav právnej neistoty.

Som toho názoru, že právna norma umožňujúca zásah do súkromia jednotlivca, musí byť formulovaná dostatočne zrozumiteľne a určito ustanoviť podmienky, za splnenia ktorých je štátny orgán oprávnený použiť invazívne opatrenia zasahujúce do základných práv jednotlivca.

De lege ferenda je preto namieste precizovať normatívnu úpravu podmienok, za splnenia ktorých sa zakladá miestna príslušnosť Krajského súdu rozhodujúceho o vydávaní súhlasu na použitie ITP takým spôsobom, aby miestna príslušnosť konajúceho súdu, nebola ponechaná na výber – autonómnu úvahu žiadateľa, ale aby táto bola naviazaná na miesto spáchania skutku, resp. na sídlo žiadateľa, resp. organizačného útvaru realizujúceho operatívnu činnosť.

Zoznam literatúry:

BLÁŠKOVÁ, A.: Ochrana obydlia ako súčasť práva na súkromie; *Justičná revue*, 2011, č. 3.

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

IVOR, J., POLÁK, P., ZÁHORA, J.: *Trestné právo procesné*; Bratislava. Wolters Kluwer, 2017.

ŠIMOVČEK, I. a kol.: *Trestní právo procesné*. Plzeň: Aleš Čeněk, 2011.

Súdny dvor EU ROQUETTE FRÉSES SA z 22. októbra 2002; Najvyšší súd SR, v rozhodnutí pod sp. zn.: 8Sžo 36/2008, definoval súkromie, ako súkromie bezprostredne nadväzujúce na osobu občana – odev, predmety, ktoré má pri sebe, ako aj celú intímnu oblasť človeka, jeho záujmy (aj profesionálne), vzťahy, styky, atď.

MALONE v. SPOJENÉ KRÁLOVSTVO; HUVIG v. FRANCÚZSKO, KLASS v. NEMECKO.

KRUSLIN v. FRANCÚZSKO; HUVIG v. FRANCÚZSKO; KVASNICA v. SLOVENSKO.

II. ÚS 87/01, nález z 12. júla 2012.

Prostriedky operatívnej techniky – kategória kreovanej teórie kriminálno-policaijného poznania

Means of the Operative Technology – Category of the Developed Theory of Criminal and Police Cognition

Miroslav Lisoň¹

Michal Marko²

Abstrakt: Autori vo svojom príspevku informujú odbornú verejnosť o dosiahnutých výsledkoch vedeckej práce, ktorú realizujú pri kreovaní teórie kriminálno-policaijného poznania v systéme policaijných vied. Špecificky riešia otázky, ktoré sa týkajú používania prostriedkov v tomto špecifickom policaijnom poznaní.

Abstract: The authors of this paper provide information for expert public about results of their scientific work which is realized during development of the Theory of Criminal-Police Cognition in the system of the police science. Specific questions about using means in this specific cognition are solved in this paper.

Kľúčové slová: policaijné vedy, kriminálno-policaijné poznanie, policaijné konanie, policaijná realita, realita kriminálno-policaijného poznania, prostriedky kriminálno-policaijného poznania.

Keywords: police science, criminal and police cognition, police act, police reality, reality of criminal and police cognition, means of criminal and police cognition.

Úvod

Na to, aby príslušníci polície plnili svoje poslanie (*úlohy, funkcie*), musia byť stále zdokonaľované zodpovedajúce legislatívne, organizačno-riadiace, taktické a technické predpoklady pre ich konanie. Zjednodušene povedané, skutočnosť, že konanie polície je charakterizované mimoriadnym bohatstvom obsahu, mnohostrannosťou javov, udalostí a vzťahov, vyžaduje aj zodpovedajúcu rôznorodosť metód, postupov a prostriedkov pri účelovej realizácii jeho procesov. Preto je potrebné z metodologického a metodického hľadiska v štruktúre policaijného konania generovať určité kategórie v podobe organizačno-taktických foriem, ktoré sa od seba líšia tak právnym základom, zameraním, ako aj metódami a prostriedkami.³

Prax potvrdzuje, že bez spracovanej teórie týchto požiadaviek je obťažné plniť v súlade s identifikovanými potrebami. Teória svoju spoločenskú funkciu plní predovšetkým tým, že vypracováva objektívne poznanie, ktoré je využiteľné pri zvyšovaní úrovne účinnosti a efektivity konania (*plnenia stanovených úloh*) a zároveň ho pomáha zavádzať do praxe. Teoretické poznanie, z hľadiska plnenia úloh v systéme policaijného konania, významným spôsobom prispieva k napĺňaniu princípov slobody, demokracie a práva v súlade s jednotlivými funkciami právneho štátu.

Teória zaujíma významné miesto v samotnom systéme policaijného poznávania.

¹ Prof. Ing. Miroslav Lisoň, PhD., Akadémia Policaijného zboru v Bratislave, katedra kriminálnej polície, Sklabinská 1, 835 17 Bratislava.

² JUDr. Michal Marko, PhD., Akadémia Policaijného zboru v Bratislave, katedra kriminálnej polície, Sklabinská 1, 835 17 Bratislava.

³ HOLOMEK, J. – T. ŠIMANOVSKÁ Úvod do metodológie praktických vied: Policaijné vedy ako vedy praktické. Bratislava: Akadémia PZ v Bratislave, 2002, s. 42. 163 s.

1 Teória kriminálno-policačného poznania v systéme policačných vied

Zdrojom vývoja poznania v policačnej praxi a vývoja policačnej teórie je permanentne riešenie filozofického rozporu medzi policačnou teóriou a praxou, pričom policačná prax je určujúcou stránkou tejto rozpornej jednoty. Potrebu a oblasti vedeckého poznávania činnosti polície tak v konečnom dôsledku determinuje policačná prax.

Úlohou vedeckého poznávania súčasnej policačnej praxe je slúžiť jej samotnej. Pokiaľ má vedecké poznanie plniť túto úlohu, musí rezolútne eliminovať všetky prvky dogmatizmu alebo praktikizmu stále sa ešte prejavujúcich u niektorých policačných „odborníkov“. Praktikizmus i dogmatizmus deformujú dynamický vzťah medzi poznaním a praxou, teóriou a skúsenosťami a sú objektívne škodlivé nielen pre policačnú teóriu, ale predovšetkým pre policačnú prax samotnú.⁴

1.1 Teórie v systéme policačných vied

V súvislosti s rozvojom policačných vied je možné uviesť, že často diskutovanou otázkou je vymedzenie ich špecifického predmetu. Z výsledkov tejto diskusie je zrejmé, že vymedzenie tohto základného atribútu policačných vied je v súčasnosti zložitým teoretickým a praktickým problémom. Aplikovaný výskum potvrdzuje, že je to najmä preto, lebo odborníci sa nemôžu zhodnúť na identite teoretických a praktických potrieb policačného konania. V týchto intenciách za pozitívne je možné označiť, že kontinuálne a konštruktívne prebieha odborná vedecká diskusia o týchto potrebách. Na základe jej výstupov je možné vysloviť záver, že už v súčasnej dobe **policačné vedy** v svojom obsahu subsumujú vznikajúci **systém vedeckých poznatkov o policačnej realite**.

Policačné vedy predstavujú systém poznania o policačnom konaní, ktorý sa explanáciou a projektovaním policačnej reality účelovo rozvíja (*konštituuje*) v súlade so spoločenskými potrebami.

Policačná realita je objektívne vyskytujúca sa skutočnosť v ľudskej spoločnosti, v ktorej sú realizované procesy policačného konania a vytvárajú sa a fungujú jeho konštrukty (*v praktickom vyjadrení – logistika*).

Procesy policačného konania tvoria najmä situácie, v ktorých sú účelovo štruktúrovane realizované metódy a prostriedky ich zabezpečenia (*činnosti*).

Konštrukty (logistiku) policačného konania tvorí najmä zovšeobecnené vedecké poznanie vo forme právnych noriem, stratégií, taktík, metodík, systémov organizácie práce a riadenia, profesionálnej prípravy ich realizátorov ...

Aj napriek tomu, že to nie je „*expressis verbis*“ vyjadrené, z týchto úvah vyplýva, že úlohou policačných vied nie je len podpora policačnej praxe, ale aj hlboké poznanie a vysvetlenie policačnej reality.

Výsledky aplikovaného výskumu potvrdzujú, že kompozícia policačných vied vykazuje konkrétne rezervy. To však nepopiera ich prínos, ktorý korešponduje s čiastkovou saturáciou praktických a teoretických potrieb. Očakávaným pozitívom je, že policačné vedy (*v súčasnej etape ich konštituovania*) plnia dôležité praktické a teoretické funkcie. Je to evidentné z registrovanej zvýšenej úrovne účinnosti a efektivity procesov policačného konania. Základnú štruktúru systému policačných vied, ako vedy, vytvárajú **dve zložky – teória a výskum**. Teoretická zložka policačných vied predstavuje systém poznatkov, ktoré prezentujú popis a explanáciu (*vedecké vysvetlo-*

⁴ ŠKROVÁNEK, J. K niektorým problémom vzťahu policačnej teórie a praxe. In. Policačná teória a prax, č. 1/2004, s. 81, 82.

vanej) procesov a javov policajnej reality.⁵ Výskumná zložka poskytuje dáta a zdôvodnenie pre tento opis a explanáciu. Vo svojej podstate je to vysokokvalifikovaná organizovaná odborná činnosť zameraná na získanie nových poznatkov (*základný výskum*), respektíve na objavovanie postupov, ktorými možno využiť teoretické poznatky v policajnej praxi (*aplikovaný výskum*).

Vedecké poznanie je efektívne, ak systémovo integruje obidve jeho roviny, t. j. rovinu empirickú a teoretickú. Aj keď miera ich zastúpenia je v rôznych oblastiach poznania (*dokonce aj v rôznych vedných disciplínach*) rozdielna, nemôže niektorá z nich úplne absentovať.

Presadzovanou zásadou pri konštituovaní policajných vied je, aby zložky ich teórie a výskumu boli vzájomne prepojené. Táto interpretácia potvrdzuje, že pri napĺňaní tohto očakávania sú registrované situácie, v ktorých uvedená synergia nefunguje. To negatívne determinuje akceptáciu systému policajných vied (*poznania*), a to tak v praktickej, ako aj v teoretickej rovine. Osobitne sa to odráža pri účelovom systémovom členení policajných vied na základe funkčných oblastí policajnej reality, predovšetkým – **spoločenskej (regulačnej, ochranej, donucovacej, výchovnej, vzdelávacej a pod.), poznávacej a organizačno-riadiacej**. Je tomu tak preto, lebo tieto funkcie je možné systémovo využiť pri eventuálnom vytváraní teórií vedných odborov v systéme policajných vied.

Iný pohľad na rozhodujúcu oblasť vedeckého poznávania policajnej reality možno prezentovať podľa základných hľadísk určujúcich postavenie, miesto a úlohy polície v spoločnosti. Podľa toho prístupu by obsah mal vychádzať z hľadiska spoločenského (*politického, občianskeho*), organizačného a z hľadiska bezpečnostného.⁶

Autori zastávajú názor, že tieto úvahy vykazujú konkrétnu relevanciu, a to najmä vo vzťahu k účelovej diverzifikácii policajnej reality, ktorej prejavy je potrebné rešpektovať pri vytváraní teórií v systéme policajných vied. Tento permanentný proces rozvoja policajných vied je potrebné zosúladiť s identifikovanými praktickými a teoretickými potrebami.

1.2 Stav kreovania teórie kriminálno-policačné poznanie

Vedeckou ambíciou pracovníkov katedry kriminálnej polície Akadémie PZ v Bratislave je vypracovať základnú teoretickú systémovú štruktúru, ktorú je možné akceptovať pri kreovaní vedného odboru „kriminálno-policačné poznanie“ v policajných vedách. Cieľom tohto procesu, v systematickom postupe pri presadzovaní tejto ambície, je operacionalizovať pojem „teória kriminálno-policačného poznania“ a to popisom jej špecifických črt (rysov), teda vlastností, ktorými sa táto teória vyznačuje. Pri postupnom napĺňaní týchto cieľov je použité poznanie získavané aplikovaným výskumom. Objektom tohto výskumu sú javy súvisiace s kriminálno-policačným poznaním (v systéme účelovo realizované spravodajská činnosť, operatívno-pátracia činnosť a vyšetrovanie), ktoré je účelovo realizované v systéme policajného konania. Vzhľadom na nekonečnú rozmanitosť tohto objektu, pri jeho skúmaní a vysvetľovaní sú vydeľované len niektoré jeho časti, vlastnosti a stránky, ktoré sú od ostatných nutne abstrahované. Tento zredukovaný súhrn komponentov, stránok, vlastností a vzťahov tejto poznávacej činnosti vymedzuje predmet

⁵ HOLCR, K. – V. PORADA a kol. Policačné vedy Úvod do teórie a metodológie. Plzeň, 2011, s. 222, Policačné vedy bez vlastnej teórie by samozrejme stratili status vedného odboru. „...Policačné vedy sa líšia od vied fundamentálnych predovšetkým typom otázok a adekvátnych odpovedí, ktorých systémová integrácia tvorí systém teórie. Za meritórne otázky vied fundamentálnych sú považované otázky, čo je a prečo to je? A vied praktických, čo má byť a ako to čo najefektívnejšie dosiahnuť? ... Artefakty vied fundamentálnych sú hodnotené, pravdivé alebo nepravdivé, vied praktických ako, správne alebo nesprávne. Policačné vedy ako vedy praktické si tak budujú svoj systém teórie, avšak iným spôsobom ako vedy fundamentálne. Jeho ďalšie rozvíjanie patrí k trvalým úlohám vedeckého spoločenstva policajných vied.“

⁶ PORADA, V. – K. HOLCR a kol. Policejní vědy Plzeň, 2011, s. 72 a násl.

tohto výskumu, ktorý je pracovne označený termínom „realita kriminálno-polícijného poznania“ (ďalej len realita policajného poznania). Realita policajného poznania je teda určitá „optika“, prostredníctvom ktorej sú vedecky skúmané a vysvetľované účelovo realizované činnosti v systéme kriminálno-polícijného poznania.

Voľba objektu teoretického skúmania, predovšetkým jeho predmetu je účelová a cieľavedomá. Je determinovaná množstvom obmedzujúcich činiteľov, predovšetkým úrovňou poznania všeobecne a objektom poznania zvlášť, nárokov súvisiacich s personálnou, časovou, regulačnou, materiálnou a inou realizáciou výskumu.⁷

Systematicky spracované poznanie z aplikovaných výskumov má charakter teórie. Tú tvorí systém poznatkov, ktoré prezentujú popis a explanáciu (vedecké vysvetľovanie) javov registrovaných pri účelovej realizácii kriminálno-polícijného poznania. Obsahovú štruktúru teórie tvorí súbor tvrdení charakterizujúcich črty reality policajného poznania, teda vlastností, ktorými sa prvky tohto predmetu výskumu vyznačujú a môžu sa rozvíjať. Jej autori, v danej etape kreovania, ich považujú za pravdivé.

Proces kreovania teórie kriminálno-polícijného poznania je všeobecne začatý analýzami stavu, určením cieľov a realizáciou postupov, ktorými je možné verifikáciou stanovených hypotéz dosiahnuť.

„Čo je typické pre súčasný stav kreovania teórie kriminálno-polícijného poznania?“ „Ako je možné pristupovať pri hodnotení stavu kreovania teórie kriminálno-polícijného poznania?“

Vo všeobecnosti je možné uviesť, že pri nachádzaní odpovedí na takto sformulované otázky je predovšetkým možné odhaliť potrebu a stanoviť ciele, ktoré je možné určitým konaním dosiahnuť. Pritom je možné akceptovať, že kreovanie predstavuje dynamickú kategóriu, ktorou je charakterizovaný proces.

Pri hodnotení stavu kreovania teórie kriminálno-polícijného poznania sa ukazuje ako vhodné v prvom rade akceptovať axiomatické pravidlá dialektiky, ktoré umožňujú poznávať koridory vývinu a vývoja jej systému. Dialektika pomáha odhaľovať vzájomné súvislosti, ktoré sa prejavujú v konkrétnych interakčných väzbách kreovaného systému teórie. Dialektickým prístupom je možné vymedziť dôvody súvisiace s predpokladom existencie väzieb medzi prvkami v systéme teórie, resp. zistiť ich objektívnu absenciu a pod. Akceptácia dialektiky vykazuje relevanciu v celom procese explanácie javov (*objektov*) teórie kriminálno-polícijného poznania.⁸ V daných súvislostiach (*pri hľadaní odpovedí na nami formulované otázky*) je možné vysloviť čiastkový záver: **proces kreovania teórie kriminálno-polícijného poznania je determinovaný samotným vývinom a bojom protirečení v prírodných a spoločenských javoch, ktoré sa prejavujú v javoch a samotných procesoch, ktorými je ich možné účelovo, účinne a efektívne poznávať.**

Z iného uhla pohľadu identitu parametrov stavu kreovania teórie kriminálno-polícijného poznania (*ďalej len stav*) je možné charakterizovať aplikovaním identifikácie systému. Identifikácia systému je špecifický proces poznávania objektov (*identifikovaných a identifikujúcich*). Umožňuje identifikujúcim subjektom definovať na identifikovanom objekte systémový model vlastnosťami, ktoré charakterizujú jeho existenciu a správanie (*identitu*). To potvrdzuje, že základným predpokladom naplnenia týchto zámerov a cieľov je dosiahnutie takej úrovne a hĺbky poznania o objekte, aby ho bolo možné systémovo modelovať. Strategická podoba parametrov

⁷ ERNEKER, J. – V. PORADA, a kol. Poznávání potřeb a transfer vědeckých poznatků do policejní praxe. Praha: PA ČR Praha, 2006, s. 78.

⁸ LIŠOŇ, M. Evalvacia funkcionality a organizácie a riadenia operatívno-poznávacej činnosti. In. Policajná teória a prax, ročník XVIII. č. 3/2010, s. 5–22.

modelu je vyjadrením zvrchovanej vôle identifikujúceho subjektu dosiahnuť vytýčené zámery a ciele. Ich určovanie je koncentrovaným vyjadrením tejto vôle.⁹

Z publikovaného vedeckého poznania vyplýva, že v procese kreovania teórie kriminálno-polícijného poznania (*predovšetkým logickými operáciami*) je do jej systému systematicky, cieľavedome, konštruktívne implementované poznanie z policajných vied (*zovšeobecnenie, analógia, dedukcia atď.*). Opačne, táto teória predovšetkým induktívne poskytuje spracované poznanie pre ďalší proces ich konštituovania. Dosahované poznanie už v tomto štádiu kreovania je využívané pri strategickom rozvoji kriminálno-polícijného poznania. Z toho vyplýva, že teória kriminálno-polícijného poznania je dynamická vedecká kategória, ktorá sa v konkrétnom procese účelovo a cieľavedome vyvíja. Kreovanie teórie korešponduje s dosahovanou úrovňou praktického poznania o skúmaných javoch objektívneho sveta. Z toho vyplýva, že vytýčené ciele v procese kreovania teórie kriminálno-polícijného poznania sú adresné. Jej autori rešpektujú požiadavky konkrétnych subjektov a predovšetkým si uvedomujú, že pre nich túto teóriu vytvárajú (*prax, teória, policajné vedy*). V súlade s napĺňaním konkrétného účelu a sledujúc určené ciele svojím informačným potenciálom (*arzenálom*), zvyšujú úroveň potrebného poznania a takto pozitívne ovplyvňujú možnosti a schopnosti subjektov, ktoré sa podieľajú na účelovom plnení špecifických policajných úloh. Identitu týchto skutočností určujú výsledky analýzy postupov a informačných výstupov z kriminálno-polícijného poznania. Táto analýza je účelovo a cieľavedome zameraná na hodnotenie plnenia konkrétnych praktických úloh. Účelovo realizovanými činnosťami v systéme kriminálno-polícijného poznania sú dominantne identifikované kriminálne aktivity, ktorých obsah a formy sa permanentne vyvíjajú. Pozitívom je, že pri ich poznávaní čoraz častejšie nachádzajú svoje uplatnenie aj informačné výstupy z teórie a pod.¹⁰

Základný kontext v procese kreovania teórie kriminálno-polícijného poznania, ktorý určuje jej zmysel a poslanie, je jej špecifický predmet. Tým je **realita kriminálno-polícijného poznania (ďalej len realita policajného poznania)** – objektívna skutočnosť, ktorú táto teória skúma a používa pri vysvetľovaní určených objektov. V daných súvislostiach je možné konštatovať, že teória tento predmet systematicky rozvíja.

Pri kreovaní teórie sú vnímané nové spoločenské aspekty. Kreovanie teórie kriminálno-polícijného poznania korešponduje so zmenami spoločenských procesov. Vytváranie jej inštrumentária (*pojmový systém, kategórie, teoretické modely, formy myslenia, ...*) je spájané s explanáciou aj nových prístupov, ktoré sú v súlade s vývojom a rozvojom procesov kriminálno-polícijného poznania, pre ktoré sú typické otvorenosť a možnosti spoločenskej kontroly pri ich účelovej realizácii.

Z úloh, ktoré sú priamo, resp. sprostredkovane determinované bezpečnostnou situáciou vyplýva, že samotný rozsah a mnohotvárnosť teórie kriminálno-polícijného poznania je v súčasnej dobe širokospektrálny. Do jej systémového obsahu vstupujú stále aktualizované témy a problémy. Pri jeho budovaní, aj zavádzaním „*umelých*“ prvkov, sú rešpektované vopred zdôvodnené ciele, sféry pôsobenia, štruktúra a taktika postupu.

Proces kreovania teórie kriminálno-polícijného poznania tvorí systém. jeho projektovanie vykazuje relatívnu stálosť a uzavretosť. do svojho obsahu neprijíma ľubovoľné vstupy, ale iba tie, ktoré sú predvídané a s ktorými sa vopred počíta. Interdisciplinárnosť koncepcií obohacuje pohľad na túto teóriu. Prejavuje sa to najmä vo vzťahu k širším základom *teórií krimi-*

⁹ OBOŇA, J. Systém a systémová analýza v prax. Bratislava: Alfa 1990, s. 210. 272 s. ISBN 80-05-00104-5.

¹⁰ LISOŇ, M. – P. POLÁK. Možnosti využitia identifikácie pri poznávaní legalizácie príjmov z trestnej činnosti, In.: Odhalování a identifikace výnosů z neznámých zdrojů a podezřelých obchodu, Sborník vstupních studií, Praha: Police history, 2008, s. 100–143 a iné.

nalistiky, kriminológie, práva, konštituovaných policajných a ďalších vied, ktoré sú frekventovane využívané najmä v systéme poznávania kriminálnych aktivít. **V procese kreovania teória kriminálno-policajného poznania, do jej základu sú implementované teórie a výskumné metódy z iných vedných disciplín.** Túto skutočnosť je možné identifikovať a popísať z informačných tokov, napríklad analýzou citácií, ktoré sú využívané vo vedeckých publikáciách charakterizujúcich procesy kriminálno-policajného poznania a opačne. **Pre kreovanú teóriu kriminálno-policajného poznania abstraktnosť a všeobecnosť výpovedí z iných vedných disciplín nie je východiskom, ale už výsledkom skúmania konkrétnych systémov (*dispozíciou poznania*).** To výrazne prispieva k zvyšovaniu efektivity jej kreovania.

Práve tieto skutočnosti vykazujú konkrétnu relevanciu pri ďalšej systematickej činnosti v cieľavedomom budovaní teórie kriminálno-policajného poznania.

Pri hodnotení stavu kreovania teórie kriminálno-policajného poznania je možné konštatovať, že už v súčasnej dobe táto systémovo realizovaná činnosť vykazuje konkrétnu organizovanosť, ktorá je vlastná každému jeho subsystému a jeho prvkom.

Kreovanie teórie kriminálno-policajného poznania v súčasnom štádiu vývoja tvorí štruktúrovaný systém s adresným riadením. Ako systém je a musí byť začlenený do vyššieho systému, ktorým sú konštituované policajné vedy. Konkrétnymi vzťahmi, ktoré sú vytvorené spoločnými a špecifickými vlastnosťami v systéme reality policajného poznania, je možné charakterizovať jej relatívnu samostatnosť.

Uvedené skutočností je možné objektivizovať demonštratívnym charakterizovaním prístupov a postupov, ktoré autori akceptujú pri plnení úloh spájaných s kreovaním teórie kriminálno-policajného poznania.

2 Prostriedky v systéme kriminálno-policajného poznania

Účelovú realizáciu kriminálno-policajného poznania ovplyvňuje celý rad faktorov. Medzi týmito faktormi majú osobitné miesto možnosti a schopnosti vnímať a fixovať relevantné informácie (*oprávnený záujem*). Aj napriek určitej zložitosti je možné konštatovať, že v celom rade prípadov determinujúce faktory vnímania príslušníci polície môžu pozitívne ovplyvňovať, predovšetkým využitím rôznych prostriedkov.

Zákon ani iná právna norma nedáva vyčerpávajúci výpočet všetkých prostriedkov a taktických postupov, ktoré sa používajú alebo môžu použiť pri napĺňaní účelu kriminálno-policajného poznania. Každý pokus o taxatívny výpočet prostriedkov v jednotlivých právnych normách vo svojich dôsledkoch nie je ničím iným než pokusom zastaviť proces rozvoja, zdokonaľovania a rozširovania vedeckého základu praktickej realizácie tejto špecifickej poznávacej činnosti. Napokon vopred ani nemožno zistiť všetky konkrétne situácie, v ktorých sa aplikujú technické a taktické prostriedky a postupy.

Prostriedky používané v kriminálno-policajnom poznaní predstavujú subjekty, nástroje, pomôcky, ich súbory, ktorými je možné dosahovať vyššiu účinnosť a efektívnosť práce pri plnení stanovených úloh.

2.1 Klasifikácia prostriedkov v kriminálno-policajnom poznaní

Príslušníci polície pri plnení úloh kriminálno-policajného poznania sú oprávnení využívať prostriedky v súlade s ich kompetenciami, ktoré sú reglementované v právnom poriadku Slovenskej republiky a medzinárodných dohovoroch, ku ktorým Slovenská republika pristúpila. V teórii kriminálno-policajného poznania (*rešpektujúc potreby ich explanácie a projektovania*) sú tieto

prostriedky klasifikované do troch skupín. Do prvej skupiny patria tie, ktoré majú **všeobecnú využiteľnosť**. Jedná sa o prostriedky, ktoré sú využívané aj pri realizácii iných druhov poznávacích činností, mimo polície. Týmto prostriedkami je možné výrazne ovplyvňovať napríklad úroveň policačného pozorovania (*sledovania*), zisťovania niektorých kvantitatívnych vlastností poznávaného objektu (*prostriedky využívané pri pozorovaní osoby operatívneho záujmu na väčšiu vzdialenosť, v noci, resp. pri skúmaní mikrovlastností objektov, spotreby, vzdialenosti*) a pod.

Do druhej skupiny sú zaradené **špeciálne prostriedky**, ktoré sú používané pri realizácii procesov policačného konania. Východiskom pri ich explanácii sú spoločné úlohy, ktoré občan deleguje na políciu. V súlade s plnením stanovených úloh ide predovšetkým o tieto prostriedky:

- špeciálne technické (rôzne prostriedky výpočtovej techniky, spojovacie a dopravné prostriedky, materiálno-technické vybavenie polície a pod.),
- strelné zbrane a donucovacie prostriedky (slzotvorné prostriedky, obušok, putá a iné),
- informačné systémy a policačné evidencie (údaje o známych páchateloch a ich trestných činoch, o neobjasnených trestných činoch atď.),
- kriminalisticko-technické (rôzne technické prostriedky, zariadenia a ich súbory, materiály, postupy, spôsoby a pravidlá ich použitia) a iné.

Tretiu skupinu prostriedkov tvoria tie, ktoré vznikli a vznikajú v súlade konkrétnymi realizačnými požiadavkami a potrebami. Vo vzťahu k realizácii kriminálno-policačného poznania tieto prostriedky majú špecifický charakter. Príslušníci polície pri ich používaní sú povinní rešpektovať celý rad limitujúcich faktorov, ktoré vyplývajú z:

- ✓ ich právnej charakteristiky, osobitne zákonnými podmienkami ich použitia (*kontroly*),
- ✓ cieľov, ktoré je možné ich použitím dosiahnuť (*výkonnosť*),
- ✓ personálnej a ekonomickej náročnosti a pod.

Z týchto dôvodov v kreovanej teórii táto skupinu prostriedkov je označovaná syntetizujúcim termínom – **prostriedky kriminálno-policačného poznania** (*prostriedky KPP*). Tento pragmatický prístup súvisí s možnou aplikáciou špecifických postupov pri explanácii týchto prostriedkov.

2.2 Prostriedky kriminálno-policačného poznania

Z výsledkov nami aplikovaného výskumu vyplýva, že prostriedky KPP sú zavádzané do policačnej praxe v súlade s jej potrebami.¹¹ Z tohto dôvodu ich parametre (*vymedzené právnu kompetenciou*) majú korešpondovať s taktickými a technickými možnosťami súčasnej etapy vývoja spoločnosti (*vývoja vedy a techniky*) a predovšetkým vývoja praxe a teórie kriminálno-policačného poznania. V prípade, ak to neplatí, je to znakom, že príslušníci polície prostriedky KPP nedostatočne používajú, alebo parametre týchto prostriedkov nekorešpondujú s potrebami praxe, čo sa vždy nepriaznivo prejaví pri plnení konkrétnej poznávacej úlohy.

V systéme kreovania teórie kriminálno-policačného poznania **explanácia týchto prostriedkov a následné projektovanie ich nasadenia sú spájané s akceptáciou ich javových vlastností a podstaty**. Z empirického poznania vyplýva, že špecifické vlastnosti, ktoré sú registrované pri používaní prostriedkov KPP majú rôzne formy prejavu. Zhoda („*spoločný menovateľ*“) je evidentná v podstate týchto prostriedkov. **Obdobne pre potreby skúmania a vysvetľovania prostriedkov KPP je významné aj to, že ich používanie je účelové v súlade s vymedzeným cieľom (čiastkovým, resp. výstupným)**. Túto okolnosť najpriliehavejším spôsobom vyjadruje **pojem takтика a technika používania prostriedku KPP** (*príprava, použitie, zabezpečenie výsledkov, efekty*

¹¹ LISOŇ, M. a kol. Možnosti rozvoja OČP. Záverečná správa z výskumu. Bratislava: Akadémia PZ v Bratislave. Bratislava: Akadémia PZ v Bratislave, knižnica 2012, VÝSK. 183, 131 s. a iné.

a pod.). V konkrétnej syntéze, tieto demonštratívne formulované konštatácie sú využívané pri klasifikácii prostriedkov KPP, ktorá je účelovo využívaná a to tak v praxi, ako aj teórii kriminálno-polícijného poznania.

Rešpektujúc súčasnú úroveň poznania pre potreby praxe a teórie kriminálno-polícijného poznania prostriedky KPP sú klasifikované do skupín:

- **operatívno-technických prostriedkov (*prostriedky techniky*)**,
- **operatívno-informačných prostriedkov (*prostriedky taktiky*)**,
- **operatívno-logistických prostriedkov (*prostriedky podpory*)**.

V súčasnosti v podmienkach Slovenskej republiky je možné za **operatívno-technické prostriedky KPP** považovať **informačno-technické prostriedky (*ďalej len ITP*)** a **prostriedky nástrahovej a zabezpečovacej techniky (*ďalej len PNT*)**.¹² Základnou podmienkou úspechu pri ich používaní je, aby predpokladaný poznávaný jav (*konanie*) alebo stav, ktorý vyvolal ich používanie trval. V opačnom prípade týmito prostriedkami je možné získať informácie o následkoch poznávaného javu, čo spôsobuje, že sa ďalšie špecifické policajné poznávanie sťažuje.

Príslušníci polície v kriminálno-polícijnom poznaní prostriedky operatívnej techniky využívajú na účel získania a fixovania informácií o prebiehajúcom konaní alebo stavoch, ktoré toto konanie vyvolalo (*spôsobil*). Účinnosť a efektívnosť ich používania je závislá od výkonnostných parametrov techniky (*technologické zdroje informácií*).

V systéme realizácie kriminálno-polícijného poznania pri **používaní operatívno-informačných prostriedkov dochádza k rozloženiu síl a zodpovednosti v rámci koordinácie medzi realizujúcim príslušníkom a prostriedkom (*kooperujúci subjekt*)**, pri získavaní cieľovej informácie (*informácií*), resp. pri plnení konkrétnej úlohy. Uvedené rozloženie síl zodpovedá i rozloženiu bezpečnostných rizík, finančných a iných nákladov medzi nimi.

Napríklad rešpektujúc súčasný právny stav v Slovenskej republike, do tejto skupiny je možné zaradiť prostriedky, ktoré sú využívané na účely:

- Trestného poriadku – *zámena obsahu zásielok § 110; kontrolovaná dodávka § 111; predstieraný prevod § 112; sledovanie osôb a vecí § 113; agent § 117,*
- zákona o PZ – *sledovanie osôb a vecí, kontrolovaná dodávka, kriminálne spravodajstvo, používanie krycích dokladov, využívanie osôb konajúcich v prospech PZ, predstieraný prevod vecí a pod.*

Operatívno-informačné sú účelovo vytvorené alebo zriadené kategórie subjektov, ktoré v koordinácii s kompetentnými orgánmi štátnej správy (*s realizátormi*) môžu zvýšiť účinnosť a efektívnosť pri plnení konkrétnych úloh.

Otázkou je: „**Sú tieto teoretické postuláty v policajnej praxi akceptované?**“. Pri hľadaní odpovedí na takto jednoducho sformulovanú otázku sme identifikovali aj prípady (*situácie, udalosti*), v ktorých príslušníci polície pri používaní prostriedkov KPP ich v požadovanom rozsahu neakceptujú. Následkom toho ich činnosť na úseku špecifického poznávania je formálna.

Konkrétne sa to týkalo realizovaných procesov KPP, v ktorých boli využívané tak operatívno-technické prostriedky, ako aj operatívno-informačné prostriedky.

Napríklad analyzovali sme kauzu, v ktorej príslušníci polície pri plnení úloh zvažovali použitie agenta (*príslušník polície*). Účelom jeho nasadenia bolo vyhotoviť obrazový a zvukový záznam – použiť ITP. To znamená, agent mal participovať na vykonávaní informačno-tech-

¹² Zákon č. 301/2005 Z. z. (*Trestný poriadok*) v znení neskorších predpisov, zákon č. 171/1993 Z. z. (*o PZ*) v znení neskorších predpisov, zákon č. 166/2003 Z. z. (*o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním)*) v znení neskorších predpisov, a iné.

nického úkonu.¹³ V týchto situáciách hľadali odpoveď na otázku „v účelovo realizovaných procesoch kriminálno-policačného poznania polície použijú agenta alebo ITP?“. Z ich pohľadu vznikli takticko-technické, ako aj právne problémy (zdôrazňujeme, že je to prezentovaný názor týchto príslušníkov).

Z hľadiska postulátov, ktoré sú systémovo spracovávané v kreovanej teórii kriminálno-policačného poznania je možné k ich prístupu vysloviť celý rad pripomienok:

1. v danom prípade kompetentné orgány štátnej správy využívali pri plnení stanoveného cieľa ITP – (§ 114 TP) a agenta (§ 117 TP), na ich použitie vydáva príkaz príslušný sudca, na použitie každého tohto prostriedku je v praxi zaužívané vydanie samostatného príkazu,
2. agent – prostriedok OPČ je priamo oprávnený použiť ITP pri výkone svojej činnosti (§ 117, ods. 13 TP), aj napriek uvedenému existuje potreba adresnej kontroly používania týchto prostriedkov a teda aj samostatne formulovaný príkaz príslušného sudcu,
3. aj napriek tomu, že táto diverzita spôsobuje redundanciu – a zvýšenú byrokratickú záťaž, ktorá v konečnom dôsledku negatívne ovplyvňuje motiváciu príslušníkov pri používaní týchto kompetencií, z hľadiska práva je opodstatnená.

Tieto závery vyslovujeme aj napriek tomu, že z výkladovej analýzy príslušných ustanovení vyplýva, že dominanciu pri napĺňaní účelu a dosahovaní stanovených cieľov v systéme poznávania vykazuje charakter prostriedkov operatívno-informačných. Pri riešení tejto situácie príslušníci polície (a iné zainteresované kompetentné orgány) by mali akceptovať taktický, technický a predovšetkým procesný charakter používaných prostriedkov,

Z pragmatického hľadiska použitie „agenta“ je predovšetkým zdôvodnené jeho povinnou akceptáciou, osobitne zo strany objektu, proti ktorému pôsobí. To znamená jedná sa o príslušníka polície (resp. ustanovenú osobu – § 10, ods. 20), ktorý sa podieľa na plnení funkcií štátu. Útoky na tento orgán štátu sú neakceptovateľné (sú prísne sankcionované). Kriminálne prostredie musí byť s týmto uzročené.

Operatívno-logistické prostriedky (prostriedky podpory)

Z iného uhla pohľadu, aj v tomto prípade rešpektujúc prístupy, ktoré sú akceptované pri explanačii prostriedkov KPP v systémovom kreovaní teórie kriminálno-policačného poznania, si dovoľujeme poznamenať, že niektoré právne inštrumenty nevykazujú charakter operatívno-informačných, resp. operatívno-technických prostriedkov. Konkrétne sa to podľa postulátov teórie kriminálno-policačného poznania, týka prostriedkov OPČ – krycie doklady a objekty a miesta používané pod legendou (zákon o PZ § 39 ods. 1).

Pri obhajobe tohto stanoviska uvádzame, že právne kompetencie, ktoré sú zakomponované v možnosti využívania prostriedkov KPP sú dominantným kritériom pri charakterizovaní špecifických činností (subsystémy), ktoré sú účelovo realizované v systéme realizácie kriminálno-policačného poznania. Táto realita má nachádzať odrazy aj pri analogickom výklade ustanovení o účelovej realizácii špecifických policačných činností v systéme kriminálno-policačného poznania. De lege lata, právne vymedzenie tohto subsystému kriminálno-policačného poznania je „netradične“ deklarované v ustanovení § 38a zákona č. 171/1993 o PZ, a v § 30 ods. zákona č. 652/2004 Z. z. o orgánoch štátnej správy v colníctve a o zmene a doplnení niektorých zákonov.

¹³ V kriminálno-policačnom poznaní informačno-technický úkon (ďalej len *technický úkon*) je súbor špeciálnych odborných, technických, administratívnych a osobitných policačných činností, ktoré kompetentné orgány štátnej správy vykonávajú pri používaní prostriedkov operatívnej techniky.

Rešpektujú prístupy v kreovanej teórii kriminálno-policiajného poznania, charakteristiku OPČ vymedzujú závery analogického výkladu prostriedkov OPČ, ktoré sú kompetentné orgány štátnej správy oprávnené používať pri plnení zákonom stanovených úloh. Totižto prostriedky OPČ vymedzujú obligatórne poznávací charakter špecifických metód OPČ, ktoré rešpektujú legislatívne pravidlá nie sú vymedzené vo všeobecne záväznej právnej norme. Sú vytvárané v súlade so zásadou prípustnosti v podzákonných normatívnych aktoch.

To znamená, z analogického výkladu ustanovení prostriedkov, ktoré sú zaradené do skupiny operatívno-logistických prostriedkov takéto závery nie je možné jednoznačne vysloviť. Preto do prakticko-teoretického inštrumentária je vhodné de lege ferenda implementovať novú kategóriu (*entitu*) operatívne operácie.

Operatívne operácie tvoria viacúčelové časovo zladené úkony a opatrenia, ktoré sú cieľavedome zamerané, aby v krátkom časovom období boli zistené a zafixované významné skutočnosti operatívneho záujmu alebo boli vytvorené vhodné situácie (*podmienky*) na ďalší postup v účelovo realizovanom procese OPČ alebo v procesoch policajného konania. Príslušníci polície využívajú operatívne operácie pred realizáciou procesov OPČ, v priebehu ich prípravy, realizácie a po realizácii. Ich využitím:

- ✓ určujú ďalší smer pri plnení operatívnych úloh,
- ✓ adresne prijímajú rozhodnutia o aplikácii preventívnych alebo represívnych opatrení a následne ich účinne a efektívne realizujú,
- ✓ vytvárajú vhodné podmienky na účinnú a efektívnu realizáciu procesov OPČ,
- ✓ zabezpečujú informačnú alebo inú ochranu a kontrolu pri realizácii procesov OPČ,
- ✓ zabezpečujú vhodné podmienky (*situácie*) na účinné a efektívne nasadenie (*používanie*) prostriedkov OPČ,
- ✓ vytvárajú vhodné podmienky na aplikáciu metód OPČ (*operatívna operácia je prvkom v systéme ich aplikácie*),
- ✓ vykonávajú čiastkové úlohy súvisiace s prenasledovaním, pátraním, operatívnou ochranou určených osôb a objektov,
- ✓ vytvárajú predpoklady na účinné a efektívne vykonanie niektorých trestno-procesných úkonov a pod.

Z uvedeného vyplýva, že pri vysvetľovaní operatívnych operácií je potrebné skúmať ich štruktúrnú pozíciu a funkciu vo vzťahu k účelovej systémovej realizácii procesov OPČ, a to v dialektickej jednotke. Na základe týchto kritérií je možné **pozície** operatívnych operácií charakterizovať vo vzťahu ku konkrétne účelovo realizovanému procesu OPČ (*v jeho jednotlivých štádiách*). Z tohto eventuálneho charakteru realizačných pozícií operatívnych operácií vyplýva, že ich **funkcie** vo vzťahu k týmto procesom sú špecifické. Osobitne je možné uviesť funkcie, ktoré nesúvisia priamo s poznávaním, a to ani napriek tomu, že kompetentní príslušníci polície ich využitím plnia úlohy súvisiace s účelovou realizáciou procesov OPČ (§ 38a zákona o PZ). To znamená, že využitie operatívnych operácií sa spája tak s účelovým poznaním, ako aj s akčným a taktickým presadzovaním a rešpektovaním práva v procesoch OPČ.

Pri účelovo realizovaných procesoch OPČ najčastejšie dochádza k intencionálnemu zisťovaniu relevancie a transformovaniu vnímanej informácie do vhodného záznamového prostredia, a to v konkrétnej informačnej podobe (*informačný výstup*). Z pragmatického hľadiska, príslušníci polície funkčnú realizačnú štruktúru týchto procesov podporujú adekvátnym využívaním operatívnych operácií so zameraním na:

- ✓ vytváranie vhodných podmienok na zdôvodnenie realizácie procesov OPČ,
- ✓ vytváranie vhodných podmienok pri naplňaní účelu procesov OPČ (logistika),
- ✓ strategické, taktické a metodické zabezpečenie funkčnosti OPČ,

- ✓ zmocnenie sa relevantného poznania vo forme faktov,
- ✓ kvalitatívnu transformáciu faktov do požadovaného informačného poznania,
- ✓ redukciu informácií a elimináciu irelevantných a redundantných informácií, t. j. zníženie množstva informácií z radu príčin, ktoré je možné rozdeliť do dvoch skupín:
 - objektívne príčiny, ktoré spočívajú napríklad v tom, že informačný signál po transformácii nemá dostatočnú kapacitu, aby obsahol interpretované poznanie, ktoré niesol signál pred transformáciou, alebo nie je vôbec prispôsobený na prenos,
 - subjektívne príčiny sú spájané s vlastnosťami realizujúcich príslušníkov polície, ktorí využívajú operatívne operácie (*erudícia pri vnímaní, interpretovaní, fixácii a pod.*) na:
 - dopĺňovanie pôvodného poznania,
 - zabezpečenie potrebnej ochrany v štádiu pred realizáciou procesov OPČ, realizácie a po nej,
 - zamedzenie vzniku ďalších nežiaducich následkov a pod.

Aj napriek tomu, že to nie je *expressis verbis* uvedené, príslušníci polície využitím operatívnych operácií okrem poznania plnia aj iné úlohy. Medzi nimi majú osobitné postavenie operácie spájané s používaním (*nasadením*) prostriedkov OPČ. Realizáciou operatívnych operácií sú umelo vytvárané podmienky vhodné jednak na ich používanie. Podobnú relevanciu operatívnych operácií je možné analogicky využiť aj na aplikovanie metód OPČ (*predovšetkým systémových*).

Bez ohľadu na úplnosť realizáciou operatívnych operácií príslušníci polície v procesoch OPČ plnia funkcie (*poslanie, význam*): poznávacie, preventívne, donucovacie, kontrolné, hodnotiace, ochranné, dezinformačné, realizačné a iné. Vzhľadom na tieto skutočnosti sa operatívne operácie v praxi využívajú buď v utajenom režime, alebo otvorene – bez utajenia.

2.3 Možnosti používania prostriedkov kriminálno-policačného poznania

Niet sporu v tom, že používanie prostriedkov KPP významne ovplyvňuje účinnosť a efektivitu práce s informáciami. V systémovej realizácii kriminálno-policačného poznania ich používaním príslušníci polície vytvárajú potrebné predpoklady na vyhotovenie opisu poznávaného objektu. Bez ohľadu na úplnosť v policačnej praxi sú ich používaním skúmané a zisťované:

- a) súdržnosť systému (*objekt*), ktorá zabezpečuje aj jeho kompaktnosť. Napríklad sú riešené otázky: „či sa objekt správa ako kompaktný systém“; „ako je možné charakterizovať väzby medzi jeho prvkami (sila, čas vzniku, trvania, rozchodu a opätovného vytvorenia)“; „či neprejavuje skúmaný systém tendenciu k rozpadu“; „či nie je v štádiu vytvárania“; „aká je jeho kompaktnosť“ a pod.
- b) Cieľové správanie systému (*objektu*), ktoré je definované vlastným usporiadaním prvkov, ich vlastnosťami a vplyvmi okolia. V tomto prípade týmito faktormi je determinované správanie sa systému. To predstavuje optimálnu skutočnosť, čo v praxi môže viesť k rozporu s jeho očakávaným správaním. Napríklad použitím prostriedkov KPP je vhodné poznávať vlastné správanie systému rešpektujúc možné alternatívy, ktoré sú konfrontované s očakávaným správaním. Pri nezhode je potrebná korekcia v súlade s už spomenutými alternatívami, čo znamená použiť už pripravený iný prostriedok.
- c) Dynamická stabilita a adaptácia systému (*objektu*), jeho schopnosť reagovať na okolnosti, ktoré vznikli v konkrétnej situácii. To pri používaní predpokladá predovšetkým úspešne absorbovať neočakávané a nepredpokladané vplyvy okolia, ktoré môžu mať v poznávanom systéme aj charakter extrémnych hodnôt. Osobitne sa to odráža pri poznávaní reálnych informácií. („Aké faktory pôsobili v čase a mieste realizácie kriminálnej aktivity?“;

„Ktoré okolnosti pôsobili za existujúcej situácie?“, „Ktoré vlastnosti charakterizujú extrémnosť pôsobenia na systém?“, „V akom časovom intervale pôsobili?“, „Ktoré vlastnosti a ako ovplyvnili?“, „Aké odrazy mohli spôsobiť?“ atď.

- d) Zmeny, ktoré súvisia s vývojom systému (*kapacitné vlastnosti, zmena procesu môže viesť k posilneniu cieľov, k zmene cieľov alebo k deštrukcii systému vývoja procesu, resp. jeho štádia, zmena ekonomickej dispozície kriminálnych skupín a pod.*).
- e) Organizáciu práce a riadenie systému (*princípy – spolčenie, zoskupenie, schopnosť vybrať a presadiť také procesy v systéme, ktoré vedú k splneniu cieľov v potrebnom čase*).
- f) Ochrana systému (*vnútorná, vonkajšia; spoľahlivosť prvkov a väzieb, ktoré zabezpečujú aplikáciu prebiehajúcich kriminálnych aktivít vedúcich k naplneniu vnútorných a najmä vonkajších cieľov a pod.*).
- g) Účinnosť a efektívnosť systému, (*prečo dosahuje systém ciele, ako a čo využíva a pod.*).¹⁴

Z tohto neukončeného zoznamu je možné vymedziť právne, personálne, ekonomické požiadavky, ktoré súvisia s účelovým použitím prostriedkov KPP. Predovšetkým ich akceptáciou je možné zdôvodniť personálnu diverzifikáciu zodpovednosti v policajných organizáciách, ktorá je v mnohých prípadoch základným predpokladom pri dosahovaní stanovených informačných cieľov. Z praktického poznania vyplýva, že delegovaná zodpovednosť pri využívaní prostriedkov KPP na konkrétne subjekty má širokospektrálny význam. Ten sa odráža najmä v účinnosti, efektívnosti, kvalite a v neposlednom rade v novej kontrole nielen ich používania, ale celého systému realizácie tohto účelového špecifického policajného poznania.

Záver

Autori tohto príspevku sú presvedčení, že v konkrétnej syntéze aj tieto formulované postuláty, ktorých explanácia je systémovo spracovávaná v teórii kriminálno-policajného poznania, sú využiteľné v praxi. Je tomu tak preto, lebo pri jej kreovaní je akceptovaná identita praktickej potreby. V týchto intenciách pozitívom je, že v súčasnej dobe spracované teoretické stanoviská o kriminálno-policajnom poznaní sú využiteľné pri realizácii legislatívnych, inštitucionálnych ako aj pri strategických, taktických a metodických opatreniach na úseku identifikácie trestných činov. Aj napriek tomu, že policajná prax je konzervatívna (*nerada prijíma niečo nové*) nimi ponúkané poznanie je impulzom k diskusii. To potvrdzuje, že bez komunikácie s praxou nie je možné kreovať teórie v praktických vedách (*policajné vedy*).

Konstruktívnu kritiku prezentovanú k spracovávanému poznaniu v systéme teórie kriminálno-policajného poznania autori vítajú, ak je argumentačne zdôvodnená akceptujú ju s vedecskou pokorou.

Zoznam literatúry

- ERNEKER, J. – V. PORADA, a kol. 2006. *Poznávaní potrieb a transfer vèdeckých poznatkù do policejní praxe*. Praha: PA ÈR Praha, 2006. 232 s. ISBN 80-7251-217-X
- GEIST, B. 1992. *Sociologický slovník*. Praha: Victoria Publishing, 1992. 647 s. ISBN 80-85605-28-7
- HOLCR, K. – V. PORADA a kol. 2011. *Policajné vedy – Úvod do teórie a metodológie*. Plzeň, 2011. 242 s. ISBN 978-80-7380-329-2
- HOLOMEK, J., ŠIMANOVSKÁ, T. 2002. *Úvod do metodológie praktických vied: Policajné vedy ako vedy praktické*. Bratislava: Akadémia PZ v Bratislave, 2002, s. 42. 163 s. ISBN 80-8054-249-X

¹⁴ OBOŇA, J. 1990. *Systém a systémová analýza v praxi*. Bratislava: Alfa, 1990, s. 145.

- LISOŇ, M. a kol. 2012. *Možnosti rozvoja operatívnej činnosti polície: Správa z aplikovaného výskumu*, 1. vyd. Bratislava: Akadémia PZ v Bratislave, 2012, 131 s. Výsk. 183.
- LISOŇ, M. 2012. *Operatívno-pátracia činnosť: všeobecná časť*. 1. vyd. Bratislava: Akadémia PZ v Bratislave, 2012, 225 s. ISBN 978-80-8054-541-3.
- LISOŇ, M. 2010. *Evalvácia funkcionality a organizácie a riadenia operatívno-poznávacej činnosti*. In: Policačná teória a prax, ročník XVIII. č. 3/2010, s. 5–22.
- LISOŇ, M. – P. POLÁK. 2008. *Možnosti využitia identifikácie pri poznávaní legalizácie príjmov z trestnej činnosti*. In.: Odhalování a identifikace výnosů z neznámých zdrojů a podezřelých obchodu, Sborník vstupních studií, Praha: Police history, 2008, s. 100–143.
- OBOŇA, J. 1990. *Systém a systémová analýza v praxi*. Bratislava: Alfa, 1990, 272 s., ISBN 80-05-00104-5.
- ŠKROVÁNEK, J. 2004. *K niektorým problémom vzťahu policačnej teórie a praxe*. In. Policačná teória a prax, č. 1/2004, s. 79–83.
- Zákon č. 171/1993 Z. z. o Policačnom zbore v znení neskorších predpisov.
- Zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov.
- Zákon č. 166/2003 Z. z. Zákon o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) v znení neskorších predpisov.

Monitorovanie obydla kamerovým systémom a jeho využitie pre účely trestného konania¹

Monitoring of Dwellings by Video Surveillance System and its Use for the Purpose of Criminal Proceeding

Jaroslav Ivor²

Abstrakt: Príspevok reaguje na vývoj právnej úpravy po rekodifikácii slovenského trestného práva v roku 2005. Táto priniesla možnosť získať dôkaz aj z dôkazného prostriedku podľa osobitného zákona. Takým je zákon o ochrane osobných údajov, ktorý umožňuje monitorovanie kamerovým systémom. Jadrom je monitorovanie obydla kamerovým systémom a jeho využitie ako dôkazu v svetle judikatúry súdov a tiež návrhy de lege ferenda podľa zahraničných úprav.

Abstract: The article focuses on the relevant developments of the Slovak legal system brought about by the recodification of the Slovak criminal law in 2005. The new Criminal Codes enable to acquire evidence by using various means of proof defined by special pieces of legislation. One of such laws is the Act on the Protection of Personal Data. In compliance with the rules set forth by this Act, video (CCTV) monitoring can be carried out. The gist of the article focuses on the recordings obtained via monitoring of a dwelling and the potential use of such recordings in criminal law (in the context of the applicable court decisions). Finally, the article also presents some ideas on the potential regulation of the matter based on the legal system of other countries.

Kľúčové slová: dôkaz, monitorovanie obydla, osobné údaje, kamerový systém.

Key words: evidence, monitoring of dwellings, personal data, video surveillance system.

Odhalovanie, vyšetrovanie a vôbec efektívne trestné stíhanie najrôznejších prípadov súčasnej kriminality predpokladá okrem iného prekonať závažnú prekážku, ktorou sa často stáva tzv. stav dôkaznej núdze. Znamená to, že v súčasnom trestnom konaní nemožno vystačiť iba s využitím „klasických“ dôkazných prostriedkov, ale čím ďalej tým viac sa začínajú využívať nové, netradičné a originálne dôkazné prostriedky, ktoré sú založené predovšetkým na rýchlo sa vyvíjajúcich progresívnych krokoch techniky a informatiky. Samozrejme použitie a využitie tejto techniky predstavuje závažný zásah do ľudských práv a slobôd a preto je nevyhnutná ich precízna zákonná úprava.

Len pre osvieženie pamäti chcem stručne pripomenúť, že do roku 1990 však v československom právnom poriadku nebolo žiadnym zákonom upravené právo štátnych orgánov použitím operatívnej techniky zasahovať do garantovaných práv a slobôd občanov, aj keď je zrejmé, že spravodajské a bezpečnostné zložky štátu inštitúty odpočúvania telekomunikačnej prevádzky a vyhotovovania obrazových, či zvukových záznamov hojne využívali na základe utajovaných interných rezortných (podzákonných) noriem. Takto získané informácie slúžili na operatívne účely a nemohli byť použité ako dôkazy v trestnom konaní. Trestný poriadok z tohto obdobia (zákon č. 87/1950 Zb., zák. č. 64/1956 Zb. resp. zák. č. 141/1961 Zb.) iba príkladmo vypočítaval dôkazné prostriedky použiteľné v trestnom konaní, pričom až jeho novela z roku 2000 resp. 2002 doplnila k vypočítaným dôkazným prostriedkom aj podmienku ich získania zákonným

¹ Táto práca bola podporovaná Agentúrou na podporu výskumu a vývoja na základe Zmluvy č. APVV-15-0272.

² Prof. JUDr. Jaroslav Ivor, DrSc., Fakulta práva, Paneurópska vysoká škola, Tomášikova 20, 821 02 Bratislava, jaroslav.ivor@paneurouni.com.

spôsobom. Až od tohto štádia možno konštatovať, že sa do nášho právneho poriadku explicitne zaviedla doktrína „ovocia z otráveného stromu“ známa z anglo-amerického právneho systému.

V roku 1990 bol zákonom č. 178/1990 Zb., ktorým sa novelizoval Trestný poriadok č. 141/1990 Zb. prvýkrát do našej právnej úpravy zavedený inštitút odpočúvania a záznamu telekomunikačnej činnosti v ust. § 88 pod názvom „odpočúvanie telefónnych hovorov“, využiteľný po začatí trestného stíhania pre obzvlášť závažné úmyselné trestné činy. Po prijatí novely Trestného poriadku zákonom č. 366/2000 Z. z. mohol odpočúvanie a záznam telekomunikačnej prevádzky s výrazne rozšíreným okruhom skutkových podstát nariadiť len súd a to aj v prípravnom konaní, čiže prokurátor stratil svoje dovtedajšie zákonné zmocnenie na vydanie príkazu na odpočúvanie. Ďalšia novela Trestného poriadku (zák. č. 422/2002 Z. z. zák. č. 458/2003 Z. z.) výrazne sprísnili poskytovanie údajov o telekomunikačnej činnosti, ktoré tvorili predmet telekomunikačného tajomstva alebo na ktoré sa vzťahovala ochrana osobných údajov, pretože boli podmienené súhlasom súdu.

Novela Trestného poriadku zákonom č. 422/2002 Z. z. zároveň uviedla do nášho právneho systému úplne nový, mimoriadne závažný prostriedok zabezpečujúci informácie pre účely trestného konania za využitia informačno-technických prostriedkov – vyhotovovanie obrazových, zvukových alebo iných záznamov podľa § 88 e.

Podľa ustanovenia § 10 ods. 20 platného Trestného poriadku sa informačno-technickými prostriedkami na účely trestného konania rozumejú elektrotechnické, rádiatechnické, foto-technické, optické, mechanické, chemické a iné technické prostriedky a zariadenia alebo ich súbory použité utajovaným spôsobom pri odpočúvaní a zázname prevádzky v elektronických komunikačných sieťach, obrazových, zvukových alebo obrazovo-zvukových záznamov alebo pri vyhľadávaní, otváraní a skúmaní zásielok, ak sa ich použitím zasahuje do základných ľudských práv a slobôd.

Pre zabezpečovanie informácií dôležitých pre trestné konanie pomocou informačno-technických prostriedkov platí niekoľko charakteristických zásad, z ktorých možno ako najvýznamnejšie spomenúť:

- a) informácie sú získavané prostredníctvom špeciálnej techniky konštrukčne vyrábanej pre tento účel,
- b) použitie resp. využitie v trestnom konaní (schvaľovanie, kontrolný mechanizmus, praktická realizácia) podlieha osobitnému režimu upravenému zákonom,
- c) použitie sa predpokladá v zásade utajovaným spôsobom,
- d) spracúvanie získaných informácií, ich evidencia, dokumentácia, ukladanie a vyradovanie podlieha úprave zákonom.

Ústava Slovenskej republiky prehlasuje vo svojom čl. 1 Slovenskú republiku za zvrchovaný, demokratický a právny štát. Aj z ďalších článkoch vyplýva, že ide o štát založený na úcte k právam a slobodám človeka a občana, čo vyplýva aj z celého radu medzinárodných zmlúv o ľudských právach a slobodách, ktoré boli ratifikované a vyhlásené spôsobom ustanoveným zákonom. Osobitne citlivá je v tomto smere ochrana práva na súkromie, zahrňujúca i ochranu osobnosti a osobných údajov. V tomto zmysle je namieste pripomenúť si, že podľa čl. 8 Európskeho dohovoru o ľudských právach a základných slobodách „každý má právo na rešpektovanie svojho súkromného a rodinného života, obydliá a korešpondencie“, pričom štátny orgán nemôže do výkonu tohto práva zasahovať okrem prípadov, keď je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti najmä v záujme národnej bezpečnosti, verejnej bezpečnosti a predchádzania nepokojov a zločinnosti. Obmedzenia resp. zásahy do osobnostných práv sú aj podľa čl. 13 Ústavy SR možné výlučne len zákonom. Aj občianskoprávna ochrana osobnosti v ustanovení § 12 Občianskeho zákonníka explicitne stanovuje, že písomnosti osobnej povahy,

podobizne, obrazové snímky a obrazové a zvukové záznamy týkajúce sa fyzickej osoby alebo jej prejavov osobnej povahy sa smú vyhotoviť alebo použiť len s jej privolením, zároveň sa však pripúšťa výnimka v podobe tzv. úradnej licencie, kedy sa umožňujú vyhotovovať takéto záznamy bez privolenia dotknutej osoby na úradné účely na základe zákona.

Rekodifikovaný Trestný poriadok (zák. č. 301/2005 Z. z.) precizoval a potvrdil využitie informačno-technických prostriedkov v slovenskom trestnom konaní najmä v ustanoveniach

- § 113 ods. 4 – sledovanie osôb a vecí s použitím ITP
- § 114 vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov
- § 115 odpočúvanie a záznam telekomunikačnej prevádzky.

Skúsenosti zo zahraničia, ale už taktiež zo Slovenska hovoria jednoznačne, že kamerové systémy na monitorovanie osôb v rôznych situáciách a s rôznym účelom, predstavujú mimoriadne rozšírený, ale zároveň jeden z najúčinnějších prostriedkov ochrany života, zdravia, majetku osôb, verejného poriadku a bezpečnosti vôbec. Samozrejme, že efektívne využívanie kamerového systému je podmienené jeho technickou úrovňou, spôsobu spracovania a prenosu signálu, odolnosti voči poveternostným podmienkam, nočným videním atď., ale tieto technické otázky nie sú predmetom tohto príspevku.

Opodstatnenosť a legálnosť kamerového systému je citlivou otázkou, ktorá je riešená vzhľadom na problematiku ochrany osobných údajov, pričom táto má svoj výraz ako v európskej tak domácej legislatíve. V tomto zmysle si treba pripomenúť najmä Smernicu Európskeho parlamentu a Rady 95/46/ES o ochrane osobných údajov, pričom zároveň treba konštatovať, že slovenská právna úprava je s ňou plne kompatibilná. Ide najmä o ust. § 15 ods. 7 zákona upravujúceho monitorovanie priestoru verejnosti prístupného.

Ďalšiu veľmi významnú zmenu, ktorú priniesol rekodifikovaný Trestný poriadok, je treba vidieť v ustanovení § 119 ods. 2, upravujúcom pramene dôkazov využiteľné v trestnom konaní. Za dôkaz sa pripúšťa totiž všetko, čo môže prispieť na náležité objasnenie veci a čo sa získalo z dôkazných prostriedkov podľa Trestného poriadku alebo podľa osobitného zákona. Nóvu v tomto prípade predstavujú dôkazné prostriedky získané podľa osobitného zákona. V súvislosti s osobnými údajmi chránenými právom na súkromie je možné poukázať najmä na tri zákony, ktoré nie sú trestnoprávného charakteru a ktoré vo svojich ustanoveniach výslovne umožňujú využitie poznatkov získaných podľa týchto zákonov ako dôkazu v trestnom konaní.

Prvým je zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov, ktorý zmocňuje používať informačno-technické prostriedky na odpočúvanie a zaznamenávanie telekomunikačných činností a vyhotovovanie a využívanie obrazových, zvukových alebo iných záznamov aj mimo trestného konania Policajný zbor, Slovenskú informačnú službu, Vojenské spravodajstvo, Zbor väzenskej a justičnej stráže a Colnú správu. Ide o zákon upravujúci využívanie informačno-technických prostriedkov pre plnenie úloh uvedených subjektov, pričom sa výslovne deklaruje, že použitie informačno-technických prostriedkov podľa tohto zákona sa nevzťahuje na ich použitie podľa Trestného poriadku. Sú to najmä záujmy zabezpečenia ústavného zriadenia, vnútorného poriadku a zahranično-politických záujmov štátu, bezpečnosti a obrany štátu. V ustanoveniach § 3 až 5 sú uvedené dôvody a povoľovací mechanizmus. Veľmi významné je však ustanovenie § 7 ods. 2 citovaného zákona, ktoré umožňuje trestnoprávne relevantné informácie získané uvedenými subjektami využitím informačno-technického prostriedku použiť ako dôkaz v trestnom konaní. Podľa § 8 použitie informačno-technického prostriedku vyhotovením záznamu alebo skopírovaním záznamu, ktoré sa uskutoční v rozpore s citovaným zákonom, zakladá zodpovednosť štátu ako aj osoby, ktorá zákon porušila tak, že nezákonné správanie nariadila, schválila alebo sa ho inak dopustila.

V tejto súvislosti je potrebné poznamenať, že spoločným charakteristickým rysom vyhotovovania obrazových, obrazovo-zvukových záznamov využitím špeciálnych informačno-technických prostriedkov podľa § 115 Tr. por. a zákona č. 166/2003 Z. z. o ochrane súkromia pred odpočúvaním je monitorovanie osôb a vyhotovovanie príslušného záznamu utajeným spôsobom, teda bez vedomia dotknutých osôb.

Zákon č. 428/2002 Z. z. o ochrane osobných údajov medzi osobitné spôsoby získavania osobných údajov v ustanovení § 10 ods. 7 zaradil i monitorovanie osôb v priestore prístupnom verejnosti. Aj keď zákon pojem monitorovanie *expressis verbis* nedefinuje, možno ho vykladať ako sledovanie (koho, čo) pomocou monitorovacieho zariadenia, v tomto prípade kamerovým systémom a príslušným videozáznamom. Citované ustanovenie zákona umožňovalo monitorovanie len za splnenia troch základných podmienok:

- 1) monitorovať možno len priestor prístupný verejnosti
- 2) monitorovať možno len na stanovený účel:
 - a) zabezpečenie verejného poriadku a bezpečnosti,
 - b) odhaľovanie kriminality alebo
 - c) narušenie bezpečnosti štátu
- 3) zreteľné označenie monitorovaného priestoru.

V prípade splnenia všetkých zákonných podmienok a získania relevantných informácií bolo možné vyhotovený záznam použiť ako dôkaz na účely trestného konania alebo konania o priestupkoch.

Od 1. júla 2013 je v súčasnosti platným a účinným zákon č. 122/2013 Z. z. o ochrane osobných údajov, ktorý nanovo upravil a z časti precizoval inštitút monitorovania priestoru verejnosti prístupného na základe ustanovenia § 15 ods. 7 citovaného zákona.

Právna úprava monitorovania fyzických osôb prostredníctvom kamerového systému vyplýva najmä z § 4 ods. 1 (vymedzenie pojmu osobné údaje), § 4 ods. 3 písm. a) (vymedzenie pojmu spracúvania osobných údajov), § 4 ods. 3 písm. b) (vymedzenie pojmu informačný systém osobných údajov), § 4 ods. 3 písm. j) (vymedzenie pojmu priestor prístupný verejnosti), § 15 ods. 7 a § 17 ods. 7 (podmienky monitorovania priestorov prístupných verejnosti) zákona o ochrane osobných údajov.

Z pohľadu zákona pri prevádzkovaní kamerového systému dochádza k spracúvaniu osobných údajov prostredníctvom snímacích zariadení (kamier). Najbežnejším identifikátorom v týchto prípadoch býva tvár monitorovanej osoby. Prevádzkovanie kamerového systému je informačným systémom, ktorý sa viaže na účel definovaný zákonom a to:

- ochrana verejného poriadku a bezpečnosti,
- odhaľovanie kriminality,
- narušenie bezpečnosti štátu alebo
- ochrana majetku alebo zdravia.

Zákon umožňuje monitorovanie kamerovým systémom výlučne priestor prístupný verejnosti, ktorým sa rozumie priestor, do ktorého možno voľne vstupovať a v ktorom sa možno voľne zdržiavať bez časového obmedzenia alebo v čase vymedzenom prevádzkovateľom. Ďalšou zákonnou podmienkou legálneho monitorovania je povinnosť prevádzkovateľa zreteľne označiť monitorovaný priestor. Zákon ďalej stanovuje 15 dňovú lehotu (kalendárne dni) na uchovávanie záznamu, v prípade nevyužitia záznamu je prevádzkovateľ povinný ho v tejto lehote zlikvidovať. Samozrejme, že prevádzkovateľ by mal dodržiavať aj všeobecné zásady primeranosti a nevyhnutnosti, ako i ďalšie podmienky uvedené v § 6 citovaného zákona. Záznam získaný monitorovaním priestoru prístupného verejnosti možno využiť výlučne za účelom uplatňovania právnej zodpovednosti, teda ako dôkaz v trestnom alebo priestupkovom konaní.

Ďalším úplne novým zákonom upravujúcim monitorovanie osôb kamerovým systémom je zákon č. 1/2014 Z. z. o organizovaní verejných športových podujatí účinný od 1. 2. 2014. Citovaný zákon v ustanovení § 21 ods. 1 priamo ukladá organizátorovi rizikového športového podujatia, ale aj pri futbalovom alebo hokejovom podujatí najvyššej celoštátnej súťaže v kategórii dospelých povinnosť zriadiť kamerový systém na monitorovanie priestorov športového zariadenia a identifikáciu fyzickej osoby alebo iného predmetu a zabezpečiť záznam v digitálnej forme. Tieto priestory musia byť taktiež zreteľne označené ako monitorované. Získané záznamy je možné využiť len na účely trestného konania, priestupkového konania, správneho konania, občianskeho súdneho konania, disciplinárneho konania a pre plnenie úloh na úseku ochrany verejného poriadku a bezpečnosti štátu.

Podrobnosti prevádzkovania kamerového systému na športových podujatiach v zmysle § 21 ods. 5 citovaného zákona upravuje Vyhláška Ministerstva vnútra SR č. 274/2014 Z. z. o podrobnostiach o kamerovom zabezpečovacom systéme.

Uvedené zákony v zásade jasne a presne vymedzujú podmienky monitorovania kamerovým systémom a využitia takto získaných záznamov pre účely trestného konania ako dôkaz podľa § 119 ods. 2 Trestného poriadku.

Skúsenosti zo zahraničia, ale aj na Slovensku hovoria o veľkom rozšírení využívania kamerových systémov na monitorovanie osôb v rôznych situáciách a s rôznym účelom, ktoré sú podmienené aj značným technickým rozvojom kamier a kamerových systémov vôbec.

V ďalšom sa sústredím na špecifickú situáciu monitorovania obydla kamerovým systémom. Pri riešení tejto situácie si treba ujasniť pojem obydla, ktoré používa medzinárodnoprávnu, ústavnú i zákonnú ochranu. Podľa čl. 8 Dohovoru o ochrane ľudských práv a základných slobôd má každý právo na rešpektovanie svojho súkromného a rodinného života, obydla a korešpondencie. Podľa ustanovenia čl. 21 ods. 1 Ústavy SR je obydlie nedotknuteľné. Nie dovolené doň vstúpiť bez súhlasu toho, kto v ňom býva. Kto neoprávnene vnikne do obydla iného alebo tam neoprávnene zotrúva, dopustí sa trestného činu porušovania domovej slobody podľa § 194 Trestného zákona. Zvýšenie ochrany obydla priniesol i rekodifikovaný Trestný zákon v ustanovení § 26 ods. 2 o oprávnenom použití zbrane vo svojom obydli proti tomu, kto do obydla neoprávnene vnikne alebo v ňom neoprávnene zotrúva a nejde o nutnú obranu, pričom túto skutočnosť zaradil medzi okolnosti vylučujúce protiprávnosť činu.

Pre vymedzenie pojmu obydla je vhodné využiť výkladové ustanovenie § 122 ods. 5 Trestného zákona, podľa ktorého sa obydli rozumie dom, byt alebo iný priestor slúžiaci na bývanie vrátane priestorov a pozemkov k nim patriacim, ak sú ako súčasť obydla uzavreté.

Podľa metodického usmernenia Úradu na ochranu osobných údajov č. 5/2016 „Monitorovanie priestorov verejnosti neprístupných“ pri monitorovaní obydla platí, že

- ide o súkromný majetok,
- je verejnosti neprístupné (za verejnosť sa nepovažujú dovolené návštevy, poštár, kuriér a pod.),
- nie je priestorom využívaným na podnikateľské účely,
- ide o priestor vymedzený napr. oplotením, trávnikom, výsadbou, tabuľou s oznamom, že ide o súkromný pozemok a pod.

Monitorovanie obydla je potrebné posudzovať tak z pohľadu charakteru monitorovaného priestoru, ako aj z pohľadu rozsahu monitorovaného priestoru. Vo všeobecnosti platí, že ak dochádza k monitorovaniu priestoru verejnosti neprístupného bez ohľadu na vlastníctvo daného priestoru a monitoruje sa len tento priestor verejnosti neprístupný (t. j. nedochádza k monitorovaniu priestoru verejnosti prístupného napr. verejnej cesty, chodníka, námestia a pod.), tak úrad postupuje v zmysle § 3 ods. 2 písm. a) zákona (zákon sa na tieto činnosti nevzťahuje, ide o spra-

cúvanie údajov výlučne osobných alebo domácich činností). Osoba vykonávajúca monitorovanie v tomto režime nemá voči úradu žiadnu oznamovaciu prípadne evidenčnú povinnosť.

Osoby vykonávajúce monitorovanie obydľia však musia rešpektovať zásady ochrany osobnosti podľa § 12 ods. 2, ods. 1 Občianskeho zákonníka (... obrazové snímky a obrazové a zvukové záznamy týkajúce sa fyzickej osoby alebo jej prejavov osobnej povahy sa smú vyhotoviť alebo použiť len s jej privolením). Samozrejme, že nie je možné monitorovať priestor verejnosti neprístupný iného subjektu napríklad susedné obydľie, susedný pozemok atď. V prípade zverejnenia vyhotoveného záznamu napr. v televízii, na internete a pod. sa osoby na ňom zachytené môžu dovolávať svojich práv na ochranu osobnosti v rámci občianskeho právneho sporu.

Pre účely trestného konania je však významnou otázkou využitie záznamu z monitorovania obydľia, na ktorom je zachytené napr. konanie páchatela, ktorý sa vlámal do obydľia prevádzkovateľa kamerového systému, ktorý neoprávnene vnikol do obydľia, aby tam spáchal trestný čin a pod. Teda využitie záznamu ako dôkazného prostriedku podľa § 119 ods. 2 Tr. por. získaného podľa osobitného zákona.

Takýmto zákonom by mohol byť zákon č. 122/2013 Z. z. ochrana osobných údajov, ktorý podľa ust. § 10 ods. 3 umožňuje spracúvanie osobných údajov bez súhlasu dotknutej osoby aj vtedy, ak

Podľa písm. c) spracúvanie osobných údajov je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby alebo

Podľa písm. g) spracúvanie osobných údajov je nevyhnutné na ochranu práv a právom chránených záujmov prevádzkovateľa alebo tretej strany, najmä ak osobné údaje sú spracúvané v rámci ochrany majetku, finančných alebo iných záujmov prevádzkovateľa a osobné údaje sú spracúvané na zabezpečenie bezpečnosti prevádzkovateľa prostredníctvom kamier alebo obdobných systémov, to neplatí ak pri takomto spracúvaní prevažujú základné práva a slobody dotknutej osoby.

V tejto situácii nastáva konflikt dvoch záujmov pričom zatiaľ bez ďalšej argumentácie zastávam názor, že bude v zásade prevažovať záujem štátu na preukázanie spáchania trestného činu a usvedčenia páchatela nad záujmom páchatela na ochranu jeho osobných údajov a teda záznam z monitorovacieho systému bude využiteľný ako dôkaz v trestnom konaní. Samozrejme, že v takomto prípade sa do efektívneho záveru dotiahne legitímny účel monitorovania obydľia kamerovým systémom (ochrany chránených záujmov) potrestaním páchatela trestného činu.

Tu si však treba uvedomiť, že zákon *expressis verbis* nerieši situácie využiteľnosti záznamu získaného z monitorovania priestoru verejnosti neprístupných ako dôkazu v trestnom konaní na rozdiel od monitorovania priestoru verejnosti prístupných. Tieto prípady bude treba riešiť *ad hoc*, posúdením všetkých okolností prípadu, dodržiavaním všetkých zákonných podmienok monitorovania i porovnaním a posúdením vzniknutého konfliktu. V aplikačnej praxi pri využití záznamu kamerového systému ide vo väčšine prípadov o jediný usvedčujúci dôkaz voči obvinenému, obvinení ďalej v mnohých prípadoch namietajú porušenia niektorej z povinností prevádzkovateľa kamerového systému a vidia v zázname nezákonný dôkaz.

Na ilustráciu si dovoľím uviesť niekoľko prípadov aplikačnej praxe:

Uznesenie Ústavného súdu ČR IV. 2425/09 z 8. 2. 2010

(K neprípustnosti dôkazu získaného bezpečnostným kamerovým systémom pre účely trestného konania vo vzťahu k právu na ochranu súkromia).

Sťažovateľ sa domáhal na ÚS zrušenia právoplatného rozsudku, ktorým bol uznaný vinným z trestného činu poškodzovania cudzej veci z dôvodu porušenia práva na spravodlivý proces podľa čl. 36 ods. 1 Listiny. Namietal, že jediným priamym dôkazom, ktorý ho usvedčoval zo spá-

chania trestného činu bol videozáznam vyhotovený priemyslovou kamerou pri vstupných dverách objektu. Sťažovateľ namietal, že videozáznam bol vyhotovený bez jeho súhlasu, poškodený si nesplnil oznamovaciu povinnosť podľa zákona na ochranu osobných údajov a teda dôkazný prostriedok bol získaný nelegálne a teda bol v trestnom konaní nepoužiteľný.

Podľa názoru ÚS poškodený nainštalovaním kamier sledoval legitímny cieľ, záznam bol použitý pre nevyhnutný účel a nebol zneužitý. V danom prípade konštatoval formálne pochybenie v záležitosti administratívneho charakteru, ktoré však neimplikovalo neoprávnenosť inštalácie kamerového systému či neprípustnosť dôkazu takto zabezpečeného.

Nález Ústavného súdu ČR II. ÚS 2703/14 z 5. 11. 2014

(Prípady vraždy predajcu v spolupáchateľstve, kde právoplatne odsúdení páchatelia namietali prípustnosť dôkazu získaného kamerovým systémom na ÚS ČR).

Kľúčovým priamym dôkazom svedčiacim o vine obvinených je videozáznam z bezpečnostného kamerového systému umiestneného v predajni, kde došlo k incidentu. Sťažovateľ tvrdil, že tento dôkaz je neprípustný, pretože pre jeho použitie neboli dodržané zákonné podmienky.

K prípustnosti dôkazu získaného bezpečnostným kamerovým systémom pre účely trestného konania sa ÚS ČR vyjadril v uznesení sp. zn. IV. ÚS 2425/09. S poukazom na podmienku zachovania procesnej čistoty konštatoval, že „ak pri vyhľadávaní, zabezpečovaní alebo vykonávaní dôkazu došlo k porušeniu právneho predpisu, ktoré malo povahu podstatnej vady konania, ide o dôkaz absolútne neúčinný a teda nepoužiteľný. Pretože trestný poriadok neobsahuje žiadnu kategorizáciu takýchto vád (s výnimkou dôkazu získaného nezákonným donútením alebo hrozbou takéhoto donútenia) je nutné nepoužiteľnosť dôkazu odôvodniť výkladom v každom konkrétnom prípade zvlášť, a to predovšetkým s ohľadom na charakter vady konania, vplyv na konkrétny dôkaz pre konanie. Hoci nesplnenie oznamovacej povinnosti podľa § 16 českého zákona o ochrane osobných údajov je priestupkom, nemožno ho zhodnotiť ako porušenie právneho predpisu takej závažnosti, ktorá by mala za následok absolútnu neúčinnosť dôkazu získaného priemyselnou kamerou. Ide o formálne pochybenie administratívneho charakteru vo vzťahu k správnomu orgánu, ktoré však neimplikuje neoprávnenosť inštalácie záznamového zariadenia či neprípustnosť dôkazného prostriedku takto zabezpečeného“.

Sťažovateľovi možno prisvedčiť, že monitorovanie verejného miesta kamerou a následne vykonanie záznamu spadá pod ústavnú ochranu (čl. 10 Listiny a čl. 8 ods. 1 Dohovoru). Ako však ÚS uviedol v citovanom uznesení, „všeobecne je pre účely hodnotenia, či došlo k nedovolenému zásahu do súkromia, nutné skúmať, či bola zaznamenaná súkromná záležitosť či verejná udalosť a či bol získaný materiál určený pre obmedzené použitie, či mal byť dostupný širokej verejnosti (rozsudok ESLP P. G. a J. H. proti Spojenému kráľovstvu č. 44787/98 z 25. 9. 2001)“. Bežné použitie bezpečnostných kamier samo o sebe, hoci na ulici, alebo na verejných priestranstvách, kde slúži legitímnemu a predvídateľnému cieľu nie je problematické z pohľadu čl. 8 Dohovoru (rozs. ESLP Perry proti Spojenému kráľovstvu č. 63767 z 17. 7. 2003).

Tieto závery sa plne vzťahujú i na prejednávánú vec, pretože poškodený (správca predajne) nainštalovaním priemyselnej kamery v priestoroch predajne sledoval legitímny cieľ – ochranu svojho majetku a odhalenie prípadného páchatela trestného činu, ktorý sa ho osobne dotýkal. Vykonaný záznam bol potom využitý len pre nevyhnutný účel (preukázanie viny sťažovateľa v trestnom konaní) a nebol nijako verejne zneužitý. V prejednávanej veci záujem spoločnosti na objasnení a potrestaní veľmi závažného deliktuálneho konania úplne jasne prevážil nad ochranu osobnostných práv sťažovateľa.

ÚS uzavrel, že záznam kamerového systému je v prípade sťažovateľa úplne legitímnym dôkazom.

Najvyšší Správny súd ČR v rozhodnutí pod. č. 1 AS 113/2012 – 133 zo dňa 25. 2. 2015, riešil prípad občana, ktorý si po viacerých útokoch na svoju osobu a jeho obydlie nainštaloval v roku 2007 na svoj dom kamerový systém. Po ďalšom útoku na jeho majetok sa vďaka kamerovému systému podarilo identifikovať dve podozrivé osoby. Orgány činné v trestnom konaní akceptovali záznam ako dôkaz v trestnom konaní. Jeden z podozrivých dal následne podnet na preverenie podozrenia z porušenia zákona na ochranu osobných údajov pretože kamerový systém snímал nielen objekt poškodeného, ale i ulicu pred ním a vchod do protihľadáneho objektu predajne. Český Úrad na ochranu osobných údajov konštatoval spáchanie priestupku (pretože kamerový systém z časti snímал i priestor verejnosti prístupný) a uložil poškodenému pokutu. Mestský súd v Prahe toto rozhodnutie i sankciu potvrdil.

Najvyšší Správny súd ČR v citovanom rozhodnutí zrušil rozsudok Mestského súdu v Prahe i rozhodnutie Úradu na ochranu osobných údajov. V rozsiahlom odôvodnení okrem iného uviedol:

- Monitorovanie kamerovým systémom za účelom ochrany majetku, zdravia a života nepochybne spĺňa svoj účel len vtedy, pokiaľ správca vykonáva záznam za účelom vyhotovenia dôkazného materiálu, ktorým by identifikoval potenciálneho páchatela trestného činu a slúžil by tak na jeho potrestanie. Pokiaľ zhromaždený záznam obsahuje fakty o trestnom čine, je prirodzené, že ho odovzdá orgánom činným v trestnom konaní.
- Spracovanie údajov vykonané poškodeným je treba hodnotiť podľa zásady proporcionality. V tomto prípade ide o posúdenie konfliktu dvoch záujmov, teda práva na ochranu súkromia na jednej strane a ochrany života a majetku správcu kamerového systému na strane druhej. Toto právo sa prelína so záujmom spoločnosti na ochrane pred deliktuálnym konaním a na tom, aby tieto konania boli odhalené a potrestané.
- Princíp proporcionality sa v judikatúre ÚS ČR posudzuje pri napĺňaní troch kritérií:
 - a) Kritérium vhodnosti určuje, či opatrenie obmedzujúce základné právo umožňuje dosiahnuť sledovaný cieľ. V danom prípade možno priznať, že kamerový systém je prostriedkom, ktorý síce nedokáže zabrániť v dokonaní konkrétneho trestného činu, podstatou jeho činnosti je vyhotoviť záznam takéhoto konania, ktoré následne môže viesť k identifikácii páchatela a eventuálne k odsúdeniu. Kamerový systém predstavuje tiež významný odstrašujúci (preventívny) prvok.
 - b) Kritérium potrebnosti porovnáva zvolený prostriedok s inými do úvahy prichádzajúcimi opatreniami. V konkrétnom prípade, vysvetlenie, že ak by bola kamera „sklopená“ a zaberala len obvodové múry obydlií, funkcia kamery by sa mihla účinkom a potenciálneho útočníka, ktorý strieľal z ulice by nikdy nezaznamenala. Iná, potenciálna varianta napr. platenie si súkromnej bezpečnostnej služby, bola neúnosná.
 - c) Kritérium porovnania určuje závažnosť oboch v kolízii stojacich práv. Hlavnou otázkou bude, či a ako intenzívne zasahoval prevádzkovateľ kamerového systému do súkromného a osobného života iných osôb.

Najvyšší Správny súd tak dospel k záveru, že poškodený prevádzkoval svoj kamerový systém v súlade so zákonom a vôbec nemal byť postihnutý za priestupok.

Na záver poznamenávam, že hoci ide o prípady z aplikačnej praxe v Českej republike, ich riešenia a zdôvodnenia sú využiteľné i na Slovensku, vzhľadom k tomu, že zákonná úprava ochrany osobných údajov i trestného konania je v zásadných smeroch rovnaká resp. iba mierne odlišná.

Úplne na záver sa domnievam, že súčasná zákonná úprava monitorovania kamerovým systémom nie je v súčasnosti úplne vyčerpávajúca, čo si dokonca uvedomuje aj Úrad na ochranu osobných údajov, pretože tento nedostatok čiastočne nahrádza vydávaním svojich metodických usmernení (napr. 3/2013 – Kamerové informačné systémy osobných údajov vo vozidlách,

1/2014 – Monitorovanie priestoru prístupného verejnosti kamerovým systémom, 5/2016 – Monitorovanie priestorov verejnosti neprístupných). U uvedeného plyní, že táto problematika by si vyžadovala komplexnú zákonnú úpravu v samostatnom zákone, podobne ako je tomu aj v iných krajinách EÚ, kde majú špeciálne zákony o získavaní a využívaní záznamov z kamerových systémov. (Belgicko tzv. Camera Act z roku 2007, Francúzsko zákon č. 96-926 z 21. 1. 1995, Švédsko Public Camera Surveillance Act 1998:150, Veľká Británia: CCTV Code of Practice 2000 – Information Commissioner).

Toto platí aj vzhľadom na skutočnosť, že vo vládou schválenej Stratégii prevencie kriminality a inej protispoločenskej činnosti na roky 2016–2020 sa využívaniu a rozvoju monitorovania kamerovými systémami prikladá mimoriadna dôležitosť a podpora.

Použitá literatúra:

1. Ivor J. a kol.: Trestné právo procesné, Bratislava, IURA EDITION, 2010.
2. Ivor J., Záhora J.: Repetitórium trestného práva, Bratislava, Wolters Kluwer, 2016.
3. Ivor J.: Niektoré aktuálne trestnoprocesné problémy boja s organizovanou kriminalitou, Justičná revue č. 5–6/1998.
4. Klimek L., Záhora J., Holcr K.: Počítačová kriminalita v európskych súvislostiach, Bratislava, Wolters Kluwer, 2016.
5. Ivor J.: *Monitorovanie osôb ako dôkazný prostriedok v trestnom konaní* In: Ochrana osobných údajov: zborník z celoštátneho seminára s medzinárodnou účasťou. – Bratislava: Akadémia Policajného zboru, 2007. – ISBN 978-80-8054-419-5.
6. Rozhodnutie ESLP 2/439/93 (Botta proti Taliansku).
7. Rozsudok Najvyššieho správneho súdu ČR 2AS45/2010-68.
8. Nález Ústavného súdu ČR I. ÚS 191/05.
9. Metodické usmernenia Úradu na ochranu osobných údajov č. 3/2013, 1/2014, 5/2016.
10. Stratégia prevencie kriminality a inej protispoločenskej činnosti na roky 2016 – 2020 schválená vládou SR v roku 2016.

K problematice příkazu ke zjištění údajů o uskutečněném telekomunikačním provozu podle § 88a trestního řádu

Problems of the Order to Ascertain Data on Telecommunication Traffic in Accordance with Section 88a of the Criminal Procedure Code

Alexander Nett¹

Abstrakt: Příspěvek se zabývá aplikačními problémy a ústavněprávními limity příkazu ke zjištění údajů o uskutečněném telekomunikačním provozu dle § 88 a) odst. 1 tr. ř. de lege lata. Autor upozorňuje na skutečnost, že jediným způsobem přezkoumání příkazu soudce ke zjištění údajů o uskutečněném telekomunikačním provozu dle § 88a odst. 1 tr. ř., je v podmínkách české právní úpravy pouze a výlučně ústavní stížnost, kdy je přezkoumáván příkaz z hlediska ústavnosti. Právní úprava obsažená v trestním řádu, totiž neobsahuje opravný prostředek, který by byl využitelný pro odstranění případných vad příkazu ke zjištění údajů o uskutečněném telekomunikačním provozu spočívající v jeho nezákonnosti. V důsledku toho vzniká situace, že příkaz soudce nelze zrušit, přestože je nezákonný. Důvodem pro zrušení příkazu soudce je pouze jeho protiústavnost. Proto autor doporučuje v rámci úvah de lege ferenda postup, který by směřoval k možnosti přezkoumat zákonnost příkazu soudce ještě předtím, než bude zkoumána jeho ústavnost.

Abstract: The paper deals with application issues and constitutional law limits of an order to ascertain data on telecommunication traffic under Sec 88a(1) of the Criminal Code de lege lata. The author points out the fact that in the Czech legal system, the only manner of reviewing a court order to ascertain data on telecommunication traffic under Sec 88a(1) of the Criminal Code is only and exclusively by a constitutional complaint, where the order is reviewed from the aspect of constitutionality. That is because legislation contained in the Criminal Code contains no remedy that would be applicable for removing possible flaws in the order to ascertain data on telecommunication traffic resting in its illegality. In consequence of this, the situation arises that a court order cannot be overturned even though it is illegal. The only reason for overturning a court order is its unconstitutionality. Therefore, the author recommends in the framework of considerations de lege ferenda a procedure that would lead towards the possibility of reviewing the legality of the court order before its constitutionality would be examined.

Klíčová slova: Příkaz ke zjištění údajů o uskutečněném telekomunikačním provozu, Příkaz soudce, vada Příkazu, nezákonnost Příkazu, protiústavnost Příkazu.

Keywords: order to ascertain data on telecommunication traffic, court order, flaw in the order, illegality of the order, unconstitutionality of the order.

Úvodem

Příspěvek je reakcí na aplikační problémy týkající se postupu při vydávání příkazu soudce v přípravném řízení trestním ke zjišťování údajů o uskutečněném telekomunikačního provozu dle § 88a odst. 1 tr. ř. (dále jen „Příkaz“).

Platná právní úprava obsažená v trestním řádu neupravuje žádný opravný prostředek, jehož pomocí by bylo možné přezkoumat zákonnost Příkazu soudce vydaného v přípravném řízení trestním. Jedinou možností přezkoumání je ústavní stížnost, jejímž prostřednictvím je přezkoumávána ústavnost takového Příkazu, nikoliv jeho zákonnost.

¹ Doc. JUDr. Alexander Nett, CSc., Katedra trestního práva, Právnická fakulta Univerzity Palackého v Olomouci, Třída 17. listopadu 8, 771 11 Olomouc, e-mail: alexandernett@seznam.cz.

Dále se autor snažil odpovědět na otázku, jakým způsobem je možno v Příkazu stanovit počátek doby zjišťování údajů o skutečném telekomunikačním provozu, neboť právní úprava na tuto otázku nedává žádnou odpověď. Jedná se o problém v trestní praxi nazývaný „Příkaz do minulosti“.

I. Právní úprava obsažená v trestním řádu a zákoně o elektronických komunikacích

Dnem 1. října 2012 nabyl účinnosti zákon č. 273/2012 Sb., jímž byl novelizován jednak zákon č. 127/2005 Sb. a trestní řád, v jehož rámci bylo nově upraveno ustanovení § 88a tr. ř. Původní znění ustanovení § 88a tr. ř. bylo zrušeno nálezem Ústavního soudu pod sp. zn. Pl ÚS 24/2010 v němž bylo mimo jiné uvedeno, že „...primární funkcí práva na respekt k soukromému životu je zajistit prostor pro rozvoj a seberealizaci individuální osobnosti. Právo na respekt k soukromému životu zahrnuje i garanci sebeurčení ve smyslu zásadního rozhodování jednotlivce o sobě samém. Právo na soukromí garantuje rovněž právo jednotlivce rozhodnout podle vlastního uvážení, zda popř. v jakém rozsahu, jakým způsobem a za jakých okolností mají být skutečnosti a informace z jeho osobního soukromí zpřístupněny jiným subjektům“. Uvedený aspekt tohoto práva nachází své výslovné vyjádření v čl. 10 odst. 3 LPS, podle něhož má každý právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě. Tímto způsobem vymezené základní právo, jež lze ve spojení s čl. 13 LPS zkráceně označit jako právo na informační sebeurčení, dotváří spolu se svobodou osobní, svobodou v prostorové dimenzi (domovní), svobodou komunikační a dalšími ústavně garantovanými základními právy osobnostní sféru jedince, jehož individuální integritu je jako zcela nezbytnou podmínku důstojné existence jedince a rozvoje lidského života vůbec nutno respektovat a důsledně chránit.

V Oddíle sedmém trestního řádu je v části nazvané Odposlech a záznam telekomunikačního provozu, a to v ustanovení § 88a v odst. 1 tr. ř. uvedeno, že je-li třeba pro účely trestního řízení vedeného pro úmyslný trestný čin, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně tři roky, pro trestný čin porušení tajemství dopravovaných zpráv (§ 182 trestního zákoníku), pro trestný čin podvodu (§ 209 tr. zák.), pro trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací (§ 230 tr. zák.), pro trestný čin opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 trestního zákoníku), pro trestný čin nebezpečného vyhrožování (§ 353 trestního zákoníku), pro trestný čin nebezpečného pronásledování (§ 354 trestního zákoníku), pro trestný čin šíření poplašné zprávy (§ 357 trestního zákoníku), pro trestný čin podněcování k trestnému činu (§ 364 trestního zákoníku), pro trestný čin schvalování trestného činu (§ 365 trestního zákoníku), nebo pro úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva, kterou je Česká republika vázána, zjistit údaje o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat a nelze-li sledovaného účelu dosáhnout jinak nebo bylo-li by jinak jeho dosažení podstatně ztíženo, nařídí v řízení před soudem jejich vydání soudu předseda senátu a v přípravném řízení nařídí jejich vydání státnímu zástupci nebo policejnímu orgánu soudce na návrh státního zástupce. Příkaz k zjištění údajů o telekomunikačním provozu musí být vydán písemně a odůvodněn, včetně konkrétního odkazu na vyhlášenou mezinárodní smlouvu v případě, že se vede trestní řízení pro trestný čin, k jehož stíhání tato mezinárodní smlouva zavazuje. Vztahuje-li se žádost ke konkrétnímu uživateli, musí být v Příkazu uvedena jeho totožnost, je-li známa.

Podle § 158d odst. 3 tr. ř. 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.

Podle § 158d odst. 4 tr. ř. povolení podle odst. 2 a 3 lze vydat jen na základě písemné žádosti státního zástupce. Žádost musí být odůvodněna podezřením na konkrétní trestnou činnost a, jsou-li známy, též údaje o osobách či věcech, které mají být sledovány. V povolení musí být stanovena doba, po kterou bude sledování prováděno a která nesmí být delší než šest měsíců. Tuto dobu může ten, kdo sledování povolil, na základě nové žádosti písemně prodloužit vždy na dobu nejvýše šesti měsíců. V přípravném řízení Příkaz vydává soudce, který tak činí zásadně na návrh státního zástupce.

Obsah Příkazu vyplývá jeho povahy, jako rozhodnutí svého druhu. Proto v něm musí být mimo obecných náležitostí (§ 134 tr. ř. per analogiam) uloženo sdělení konkrétních údajů o uskutečněném telekomunikačním provozu (podle příslušného ustanovení zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů). Dále se v něm uvede, za jakou dobu mají být tyto údaje sděleny (přitom je nutno vzít v úvahu ustanovení § 97 odst. 3 věta druhá zákona č. 127/2005 Sb.), údaje o osobě, ohledně níž mají být příslušné skutečnosti sděleny, účel zjišťování údajů o uskutečněném telekomunikačním provozu ve formě, zejména údajů o trestném činu, pro který se řízení vede nebo pro který bylo zahájeno trestní stíhání. V Příkazu je třeba uvést i to, jakým způsobem mají být požadované údaje o uskutečněném telekomunikačním provozu sděleny soudu nebo v přípravném řízení státnímu zástupci.

Novelou trestního řádu provedenou zákonem č. 273/2012 Sb., bylo doplněno ustanovení § 314l odst. 2 tr. ř., podle něhož na návrh osoby uvedené v § 88a odst. 2 tr. ř. Nejvyšší soud v neveřejném zasedání přezkoumá zákonnost Příkazu (k tomu srov. nálezy Ústavního soudu ze dne 20. prosince 2011 sp. zn. Pl ÚS 24/2011 – č. 43/2012 Sb.).

Podle § 88 odst. 2 tr. ř. státní zástupce nebo policejní orgán, jehož rozhodnutím byla věc pravomocně skončena, a v řízení před soudem předseda senátu soudu prvního stupně po pravomocném skončení věci informuje o nařízeném zjišťování údajů o telekomunikačním provozu osobu uživatele uvedenou v odstavci 1, pokud je známa. Informace obsahuje označení soudu, který vydal Příkaz k zjištění údajů o telekomunikačním provozu, a údaj o období, jehož se tento Příkaz týkal. Součástí informace je poučení o právu podat ve lhůtě šesti měsíců ode dne doručení této informace Nejvyššímu soudu návrh na přezkoumání zákonnosti Příkazu k zjištění údajů o telekomunikačním provozu. Informaci podá předseda senátu soudu prvního stupně bezodkladně po pravomocném skončení věci, státní zástupce, jehož rozhodnutím byla věc pravomocně skončena, podá informaci bezodkladně po uplynutí lhůty pro přezkoumání jeho rozhodnutí nejvyšším státním zástupcem podle § 174a tr. ř. a policejní orgán, jehož rozhodnutím byla věc pravomocně skončena, podá informaci bezodkladně po uplynutí lhůty pro přezkoumání jeho rozhodnutí státním zástupcem podle § 174 odst. 2 písm. e) tr. ř.

Navrhovatelem je zde osoba, která je uživatelem telekomunikačního zařízení, a byla informována o nařízeném zjišťování údajů o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat, a v rámci této informace byla i poučena o právu podat ve lhůtě šesti měsíců ode dne doručení této informace Nejvyššímu soudu návrh na přezkoumání zákonnosti Příkazu k zjištění údajů o telekomunikačním provozu.

Předpoklady pro podání návrhu na přezkoumání zákonnosti Příkazu k zjištění údajů o telekomunikačním provozu podle § 314l odst. 2 tr. ř. k Nejvyššímu soudu jsou následující. Pravomocné skončení trestní věci, v níž byl vydán takový Příkaz. Dále skutečnost, že předseda sená-

tu soudu prvního stupně, popřípadě státní zástupce nebo policejní orgán, následně informoval o nařízeném zjišťování údajů o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat, osobu oprávněnou k podání tohoto návrhu, která byla uživatelem telekomunikačního zařízení, ohledně něhož byly uvedené údaje zjišťovány, a která je známa.

Návrh na přezkoumání zákonnosti Příkazu tedy nelze podat k Nejvyššímu soudu před pravomocným skončení příslušné věci a bez následného zaslání informace oprávněné osobě. Byl-li přesto takový návrh učiněn, Nejvyšší soud ho podle § 265i odst. 1 písm. a) per analogiám odmítne jako nepřípustný (srov. TR NS 71/2011- T 1339.).

Přezkoumání zákonnosti Příkazu provede Nejvyšší soud v neveřejném zasedání.

Předmětem přezkumu u Příkazu pak bude dodržení všech zákonných ustanovení o nařízení vydání údajů o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat, a jeho provedení ve smyslu § 88a odst. 1 a 4 tr. ř.

V řízení o přezkumu Příkazu k odposlechu a záznamu telekomunikačního provozu podle § 314l a násl. tr. ř. je přezkumná činnost Nejvyššího soudu omezena jen na posouzení zákonnosti vydaného Příkazu k odposlechu a záznamu telekomunikačního provozu. Proto se Nejvyšší soud v tomto řízení nemůže zabývat např. námitkou vztahující se k plnění povinností policejního orgánu podle § 88 odst. 3 tr. ř., ani výhradami vůči hodnocení výsledků odposlechu a záznamu telekomunikačního provozu směřujícími proti odůvodnění rozhodnutí soudu učiněného ve věci samé.

Přezkum Nejvyššího soudu je garancí, aby při ingerenci do ústavních práv občana na respektování soukromého a rodinného života zaručeným v čl. 8 EÚLP a v čl. 13 LPS bylo do nich zasahováno jen v nejnútnejší míře a aby tedy byla občanská práva maximálně šetřena. Stanovení přezkumu tak má mít i určitou preventivní roli v tom smyslu, že uvedená možnost přezkumu Nejvyšším soudem povede orgány činné v trestním řízení k maximální obezřetnosti při dodržování ustanovení o nařízení a provádění odposlechu a záznamu telekomunikačního provozu a tím k naplňování principu zákonnosti, zdrženlivosti a přiměřenosti.

Vysloví-li Nejvyšší soud porušení zákona při vydání nebo při provedení Příkazu, může to být za splnění podmínek § 278 tr. ř. důvodem pro povolení obnovy řízení v původní pravomocně skončené trestní věci. Nejvyšší soud zde vždy rozhoduje formou usnesení, proti kterému není opravný prostředek přípustný.

Tento přístup je v souladu s judikaturou Evropského soudu pro lidská práva navazující na čl. 8 EÚLP, podle kterého vždy, kdy je to možné a kdy to nepopírá smysl tajného odposlechu, musí být osoba dodatečně seznámena s tím, že její rozhovory byly odposlouchávány, popř. byly zjišťovány údaje o telekomunikačním provozu vztahující se k její stanici (telekomunikačnímu zařízení), a musí mít k dispozici účinný opravný prostředek, jímž může namítat nezákonnost nebo bezdůvodnost odposlechu nebo zjišťování údajů o telekomunikačním provozu.

Předmět telekomunikačního tajemství je vymezen v § 88 a násl. zákona č. 127/2005 Sb. (zákon o elektronických komunikacích).

Poskytování údajů je upraveno v § 97 odst. 3 zákona č. 127/2005 Sb. (zákon o elektronických komunikacích) právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna uchovávat po dobu 6 měsíců provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování jejích veřejných komunikačních sítí a při poskytování jejích veřejně dostupných služeb elektronických komunikací. Provozní a lokalizační údaje týkající se neúspěšných pokusů o volání je právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřej-

ně dostupnou službu elektronických komunikací povinna uchovávat pouze tehdy, jsou-li tyto údaje vytvářeny nebo zpracovávány a zároveň uchovávány nebo zaznamenávány. Současně je tato právnická nebo fyzická osoba povinna zajistit, aby při plnění povinnosti podle věty první a druhé nebyl uchováván obsah zpráv a takto uchovávaný dále předáván. Právnická nebo fyzická osoba, která provozní a lokalizační údaje uchovává, je na požádání povinna je bezodkladně poskytnout orgánům činným v trestním řízení pro účely a při splnění podmínek stanovených zvláštním právním předpisem.

Po uplynutí doby podle věty první je právnická nebo fyzická osoba, která provozní a lokalizační údaje uchovává, povinna je zlikvidovat, pokud nebyly poskytnuty orgánům oprávněným k jejich využívání podle zvláštního právního předpisu nebo pokud tento zákon nestanoví jinak (§ 90).

II. Ústavněprávní aspekty

Ústavní soud opakovaně uvádí, že možnost jeho zásahu do přípravného řízení v rámci trestního procesu je nutno vykládat přísně restriktivním způsobem. Ústavní soud se takto cítí být povolán korigovat pouze nejextrémnější excesy, jež jsou výrazem svévole či libovůle orgánů činných v trestním řízení. Vyjádřeno jinými slovy. Jeho kasační intervence do probíhajícího řízení (pravomocně neukončeného trestního stíhání) má své místo pouze v případech zcela zjevného porušení kogentních ustanovení podle ústavního práva, kdy se postup orgánů činných v trestním řízení zcela vymyká ústavnímu, resp. zákonnému procesně právnímu rámci a jím založené vady, případně jejich důsledky, nelze v soustavě orgánů činných v trestním řízení, zejména obecných soudů, v následujících fázích trestního řízení již nijak reparovat (srov. např. usnesení sp. zn. I. ÚS 2532/12 ze dne 28. 8. 2012 nebo usnesení sp. zn. III. ÚS 674/05 ze dne 16. 3. 2006).

Ústavní soud konstatoval, že nelze odhlédnout od skutečnosti, že v této fázi trestního řízení orgány činné v trestním řízení povětšinou nedisponují dostatečnými informacemi o vyšetřovaném jednání, neboť právě prostřednictvím vydaných Příkazů je trestná činnost podrobněji osvětlena. Proto by bylo nelogické, aby byly na orgány činné v trestním řízení kladeny nepřiměřené povinnosti stran popisu dotčené trestné činnosti, neboť toto je často možné právě až jejich realizací.

Ústavní soud dospěl k názoru, že zákon o elektronických komunikacích však nezakazuje poskytnutí dotčených údajů i za delší časové období za situace, kdy jimi dotčené osoby disponují. Žádný právní předpis nelimituje orgány činné v trestním řízení v možnosti požádat o poskytnutí údajů za období delší, než je uvedeno v § 97 odst. 3 zákon č. 127/2005 Sb., (zákon o elektronických komunikacích) který stanoví, že právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna uchovávat *po dobu 6 měsíců*.

III. Úvahy de lege lata

Ustanovení § 158d odst. 4 tr. ř. výslovně nestanoví požadavek, aby návrh (žádost) státního zastupce obsahovala dobu (resp. období) po kterou mělo být sledování prováděno. V návrhu na vydání Příkazu patrně nemusí být uvedeno období, za které mají být údaje poskytnuty. Nicméně se domníváme, že tento požadavek na stanovení doby (resp. období) nepochybně vyplývá z ustanovení § 2 odst. 4 tr. ř. in fine, neboť orgány činné v trestním řízení při provádění úkonů

trestního řízení zasahují do práv osob, jichž se takové úkony dotýkají jen v odůvodněných případech, na základě zákona a v nezbytné míře pro zajištění účelu trestního řízení.

V Příkazu pak nemusí být stanoven počátek období, za nějž mají být poskytnuty údaje. Tento závěr vyplývá z dikce § 158d odst. 4 tr. ř. podle něhož v povolení musí být stanovena doba, po kterou bude sledování prováděno a která nesmí být delší než šest měsíců. Tuto dobu může ten, kdo sledování povolil, na základě nové žádosti písemně prodloužit vždy na dobu nejvýše šesti měsíců.

Soudy zpravidla rozhodují tak, že postup dle § 88a tr. ř. bude aplikován za použití § 158d odst. 3 tr. ř., neboť některé zjišťované údaje jsou údaje o uskutečněném telekomunikačním provozu a některé se týkají zásahu do nedotknutelnosti listovního tajemství, přičemž tímto postupem je také zjišťován obsah jiných písemností a záznamů, uchovávaných v soukromí za použití technických prostředků, jelikož účelem navrhovaného opatření je zajistit dosud nesmazaný obsah e-mailových schránek, který vznikl v důsledku telekomunikačního provozu a nyní je uchovávan v podobě elektronických záznamů v soukromí.

Je tedy otázkou, jakým způsobem má soudce postupovat při stanovení počátku období za nějž mají být poskytnuty údaje o uskutečněném telekomunikačním provozu podle § 88a trestního řádu.

Pro stanovení počátku období je podle našeho názoru rozhodující začátek jednání uvedený v popisu skutku v záznamu o zahájení úkonu trestního řízení. Tento postup má svůj limit spočívající v tom, že dnem 1. října 2012 nabyl účinnosti zákon č. 273/2012 Sb., v jehož rámci bylo nově upraveno ustanovení § 88a tr. ř. (Původní znění ustanovení § 88a tr. ř. bylo zrušeno nálezem Ústavního soudu pod sp. zn. Pl ÚS 24/2010). Budeme-li tento limit akceptovat, pak v případě, že začátek jednání uvedený v popisu skutku nastal před 1. 10. 2012, nelze jako rozhodující považovat datum začátku jednání uvedeného v popisu skutku v záznamu o zahájení úkonu trestního řízení, ale datum 1. 10. 2012.

Další problém do této úvahy vnáší zákon č. 127/2005 Sb. (zákon o elektronických komunikacích) který v ust. § 97 odst. 3 stanoví, že právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna uchovávat *po dobu 6 měsíců*. Touto dobou je vázána právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací.

Je tedy otázkou, zda jsou orgány činné v trestním řízení oprávněny nad rámec takto stanovené zákonné lhůty vyžadovat na základě Příkazu data za období delší než 6 měsíců zpětně od data vydání Příkazu.

K této otázce se vyjádřil Ústavní soud a dospěl k závěru, že zákon o elektronických komunikacích nezakazuje poskytnutí dotčených údajů i za delší časové období za situace, kdy jimi povinné osoby disponují. Rovněž žádný jiný právní předpis nelimituje orgány činné v trestním řízení v možnosti požádat o poskytnutí údajů za období delší, než je uvedeno v § 97 odst. 3 zákon č. 127/2005 Sb., (zákon o elektronických komunikacích).

Podle § 314l odst. 2 tr. ř., Nejvyšší soud v neveřejném zasedání přezkoumá zákonnost Příkazu k zjištění údajů o telekomunikačním provozu. Přezkumná činnost Nejvyššího soudu je omezena jen na posouzení zákonnosti vydaného Příkazu. Proto se Nejvyšší soud v tomto řízení nemůže zabývat např. námitkou vztahující se k plnění povinností policejního orgánu podle § 88 odst. 3 tr. ř., ani výhradami vůči hodnocení výsledků odposlechu a záznamu telekomunikačního provozu směřujícími proti odůvodnění rozhodnutí soudu učiněného ve věci samé.

Z podaného je zřejmé, že tato zákonná úprava sehrává určitou preventivní roli v tom smyslu, že uvedená možnost přezkumu Nejvyšším soudem povede orgány činné v trestním říze-

ní k maximální obezřetnosti při dodržování ustanovení o nařízení a provádění odposlechu a záznamu telekomunikačního provozu a tím k naplňování principu zákonnosti, zdrženlivosti a přiměřenosti.

Nicméně platná právní úprava obsažená v trestním řádu neupravuje žádný opravný prostředek, jehož pomocí by bylo možné přezkoumat zákonnost Příkazu soudce vydaného v přípravném řízení trestním.

IV. Úvahy de lege ferenda

V rámci úvah de lege ferenda dávám ke zvážení možnost doplnění ustanovení § 158d odst. 4 tr. ř. tak, aby povinnou náležitostí návrhu (žádosti) státního zástupce byl i počátek doby zjišťování údajů o uskutečněném telekomunikačním provozu. Rovněž, aby tento údaj byl povinnou náležitostí Příkazu. Domníváme se, že tento požadavek vyplývá z ustanovení § 2 odst. 4 tr. ř. in fine, neboť orgány činné v trestním řízení při provádění úkonů trestního řízení zasahují do práv osob, jichž se takové úkony dotýkají jen v odůvodněných případech, na základě zákona a v nezbytné míře pro zajištění účelu trestního řízení. Taková právní úprava odstraní výkladové problémy týkající se např. otázky, zda počátek doby zjišťování údajů o uskutečněném telekomunikačním provozu může být stanoven před dnem 1. 10. 2012, kdy nabyl účinnosti zákon č. 273/2012 Sb., jímž byl novelizován jednak zákon č. 127/2005 Sb. a trestní řád, v jehož rámci bylo nově upraveno ustanovení § 88a tr. ř.

Podle § 314l odst. 2 tr. ř., Nejvyšší soud v neveřejném zasedání přezkoumá zákonnost Příkazu. Přezkumná činnost Nejvyššího soudu je omezena jen na posouzení zákonnosti vydaného příkazu k odposlechu a záznamu telekomunikačního provozu. Proto se Nejvyšší soud v tomto řízení nemůže zabývat např. námitkou vztahující se k plnění povinností policejního orgánu podle § 88 odst. 3 tr. ř., ani výhradami vůči hodnocení výsledků odposlechu a záznamu telekomunikačního provozu směřujícími proti odůvodnění rozhodnutí soudu učiněného ve věci samé.

Platná právní úprava obsažená v trestním řádu ovšem neupravuje žádný opravný prostředek, jehož pomocí by bylo možné přezkoumat zákonnost Příkazu soudce vydaného v přípravném řízení trestním.

V rámci úvah de lege ferenda dále dávám ke zvážení možnost přijmout novou právní úpravu, jejímž účelem by bylo přezkoumání případných vad Příkazu vydaného soudcem v přípravném řízení trestním. Nová právní úprava by mohla být vybudována na principu dvojinstančnosti. Zákonnost Příkazu soudce v přípravném řízení by přezkoumával nadřízený soud v neveřejném zasedání. O zákonnosti Příkazu by rozhodoval formou usnesení. V případě zjištění podstatných vad Příkazu by došlo k jeho zrušení pro nezákonnost. Současně by rozhodnutí soudu obsahovalo i výrok o tom, že důkaz získaný Příkazem nesmí být použit v předmětném trestním řízení.

Literatura:

- Zákon č. 141/1961 Sb., trestní řád, ve znění pozdějších předpisů
- Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
- Šámal, P. a kol.: Komentář k trestnímu řádu C. H. Beck, 2013, 7. vydání, 4720 s.
- Vantuch, P.: Trestní řízení z pohledu obhajoby. Praha: C. H. Beck, 2014, 1072 s.
- <http://www.judikaty.info/cz/nejvyssi-soud-ceske-republiky/nscr/>
- <http://nalus.usoud.cz/Search/Search.aspx>

K aplikačním problémům týkajícím se odposlechu, zjišťování údajů z telekomunikačního provozu a sledování osob a věcí v České republice

Application Problems of Interception of Telecommunications, Ascertain Data on the Telecommunications and Surveillance of Persons and Items in the Czech Republic

Miroslav Růžička¹

Abstrakt: Příspěvek se věnuje sporným otázkám výkladu ustanovení § 88, § 88a a § 158d trestního řádu o odposlechu a záznamu telekomunikačního provozu, zjišťování údajů z telekomunikačního provozu a sledování osob a věcí v České republice. Zaměřuje pozornost především na výkladové stanovisko č. 1/2015 Sbírky výkladových stanovisek Nejvyššího státního zastupitelství. To vzniklo jako důsledek úsilí kriticky přezkoumat dřívější výkladové stanovisko č. 4/2005 Sbírky výkladových stanovisek Nejvyššího státního zastupitelství. Potvrdilo se, že dřívější stanovisko plně ob stojí. Byly však řešeny některé nově vzniklé aplikační problémy týkající se výkladu ustanovení trestního řádu, jimiž se velmi závažným způsobem v trestním řízení zasahuje do ochrany soukromí prostředky elektronických komunikací. Zásadní řešení dané problematiky představuje až rekodifikace trestního práva procesního v České republice.

Abstract: The contribution deals with questionable problems of interpretation section 88, 88a and 158d of the Criminal Procedure Code on the Interception and Recording of Telecommunications, Ascertain data on the Telecommunications service and Surveillance of Persons and Items in the Czech Republic. The article concentrates attention generally to the Opinion No. 1/2015 of the Collection of opinions of the Supreme Public Prosecutor's Office. It has come in force as consequence of effort about critically revision of the Opinion 4/2005 of the Collection of opinions of the Supreme Public Prosecutor's Office. It has confirmed that Opinion No. 4/2005 of the Collection of opinions of the Supreme Public Prosecutor's Office fully succeeded. There was solved some newly arisen application problems relating to interpretation of sections of the Criminal Procedure Code significantly intervened to Protection of Privacy by means electronic communication in the Criminal Proceedings. Fundamental solving of these problems introduces re-codification of the Criminal Adjective La in the Czech Republic.

Klíčová slova: Právo na soukromí, odposlech a záznam telekomunikačního provozu, zjišťování údajů z telekomunikačního provozu, sledování osob a věcí, rekodifikace trestního práva procesního.

Key words: Protection of Privacy, Interception and Recording of Telecommunications, Ascertain data on the Telecommunications service and Surveillance of Persons and Items, Re-codification of the Criminal Adjective Law.

Úvod

Tento příspěvek je věnován institutům odposlechu a záznamu telekomunikačního provozu, zjišťování údajů z telekomunikačního provozu (§ 88 a 88a tr. ř.), v úzké souvislosti s tím i sledování osob a věcí (§ 158d tr. ř.), a to ve spojení se stanovisky vydanými v souladu s ustanovením § 12 odst. 2 zákona o státním zastupitelství č. 4/2005 Sb. v. s. NSZ a zejména č. 1/2015 Sb. v. s. NSZ, proti nimž jsou vyslovovány četné oponentní názory.

¹ JUDr. Miroslav Růžička, Ph.D., Nejvyšší státní zastupitelství ČR, Brno, Jezuitská 4, e-mail: mruzicka@nsz.brn.justice.cz.

První dva vyjmenované instituty byly poměrně výrazně dotčeny novelami provedenými zákonem č. 177/2008 Sb. (ohledně odposlechu a záznamu telekomunikačního provozu) a č. 273/2012 Sb. (ohledně zjišťování údajů z telekomunikačního provozu), jakkoli této problematiky se dotkly i jiné novely trestního řádu, případně pak zvláště některé nálezy Ústavního soudu. Z těchto novel (či vůbec z aplikace trestně procesní úpravy) vyplynuly četné aplikační problémy. Je v této souvislosti pozoruhodné, že sledování osob a věcí se zatím žádná novela trestního řádu tak podstatně nedotkla (přitom zde máme tak závažný institut, jakým je „prostorový odposlech“).

Statistika představuje mnohdy jen „přesný soubor nepřesných čísel“, zde to však možná nebude tak úplně od věci, a to i z pohledu dvou zásadních momentů, jež je zde nutno vzít v úvahu – jde často o neodkladné nebo neopakovatelné úkony a platí tu úprava v § 160 odst. 4 poslední věty tr. ř. A v neposlední řadě – zásadní je náležité zdůvodnění i povolení (příkazu k provedení) samotných těchto úkonů. Jinak hrozí nebezpečí jejich zásadního zpochybnění kdykoli v budoucnu.²

Obsah platné právní úpravy v trestním řádu již neodpovídá terminologii v „jiných právních předpisech“, především v zákoně č. 127/2005 Sb., o elektronických komunikacích. Ustanovení § 215 až 217 návrhu trestního řádu³ předpokládá označení těchto procesních institutů „Odposlech a záznam obsahu zpráv“ a „Zjišťování údajů o zprávách přenášených technickými prostředky“.⁴

² Srov. např. webové odkazy: <http://www.parlamentnilisty.cz/arena/monitor/David-Rath-a-ovoce-ze-zakazaneho-stromu-Mame-dokument-k-nejvetsi-politicke-kauze-468791>, nebo <http://www.ceskenoviny.cz/zpravy/soud-vratil-policii-druhou-cast-rathovy-kauzu-kvuli-odposlechum/1455969>.

³ Jednalo se o pracovní verzi z června 2011.

⁴ Nejvyšší státní zastupitelství zpracovalo dne 6. 8. 2015 legislativní návrh na změnu dotčených institutů. Námět na úpravu předmětných ustanovení trestního řádu vzešel z analýzy problematiky zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek. Obecně lze konstatovat, že terminologie použitá v § 88 a § 88a tr. ř. již zcela neodpovídá službám poskytovaným v sítích elektronických komunikací – k tomu srov. i § 136 odst. 20 zákona č. 127/2005 Sb., o elektronických a o změně některých souvisejících zákonů, ve znění pozdějších předpisů. Použitelnost § 88a tr. ř. je v současné podobě právní úpravy velmi omezená a neumožňuje zjišťovat obsah uskutečněné elektronické komunikace. Pro účely zjišťování obsahu uskutečněné elektronické komunikace nelze považovat za dokonalou pro její nejednoznačnost ani právní úpravu § 158d tr. ř. Bylo by tedy možno uvažovat o tom, aby v § 88 a § 88a tr. ř. byl pojem „telekomunikační provoz“ nahrazen termínem „zprávy (v širším slova smyslu, tj. nejen textové a obrazové, ale i hlasové ve formě volání) přenášené v síti elektronických komunikací“. V případě, že ke zjištění aktuálního obsahu e-mailové schránky je zapotřebí součinnost poskytovatele služby, mohl by být text § 88a odst. 1 tr. ř. (při vědomí, že § 88a odst. 1 tr. ř. je, na rozdíl od univerzální použitelnosti § 158d tr. ř., pokud jde o úmyslné trestné činy, použitelný jen ohledně v něm uvedených trestných činů), „údaje o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat“ nahrazen textem „údaje o zprávách přenesených v síti elektronických komunikací podléhající utajení, uživatelem [k tomu srov. § 2 písm. b) zákona č. 127/2005 Sb. i § 2 písm. e) zákona č. 480/2004 Sb.] v soukromí uchovávané, odeslané, doručené, rozepsané a nikoli trvale odstraněné elektronické zprávy nebo elektronické zprávy uskutečněné v době, kdy se s nimi uživatel nemohl seznámit“ (pozn. čímž by bylo ošetřeno zjišťování elektronické komunikace uskutečněné po zajištění datového nosiče orgány činnými v trestním řízení). „Příkaz k zjištění údajů o telekomunikačním provozu“ by měl být změněn na „příkaz k zjištění údajů o elektronických zprávách“.

Pokud ke zjištění aktuálního obsahu e-mailové schránky není zapotřebí součinnost poskytovatele, byť § 158d odst. 9 tr. ř. ji nevylučuje, pak by pro právní jistotu postačovalo do § 158d odst. 3 tr. ř. vložit text „elektronických zpráv“ vedle textu „jiných písemností a záznamů“. Dále by mohl být § 158d odst. 9 tr. ř. upraven tak, že na místo „Provozovatelé telekomunikační činnosti“ byl uveden „Subjekt poskytující služby v sítích elektronických komunikací“. Tímto subjektem by se rozuměl jednak operátor ve smyslu zákona č. 127/2005 Sb. a jednak poskytovatel ve smyslu zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů. Vhodné by bylo i pozměnit § 158d odst. 4 tr. ř. tak, že „povolení podle odstavce 3 lze vydat je na základě písemné žádosti státního zástupce“, což bude odpovídat současné praxi a korespondovat, s ohledem na obdobný zásah do ústavně zaručených práv, se změnou, ke které došlo v § 88a tr. ř. (novelou č. 273/2012 Sb.).

S tím, že pojem „odposlech a záznam telekomunikačního provozu“ již neodpovídá ani terminologii, ale ani obsahu příslušné navazující právní úpravy, jež je dnes zahrnuta do zákona č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů, jsou také spojeny nejrůznější aplikační problémy, jež se zdaleka netýkají pouze samotného odposlechu a záznamu telekomunikačního provozu, ale např. i úkonu upraveného po novele č. 265/2001 Sb. v ustanovení § 88a tr. ř.

Skutečností ovšem zůstává, že použití termínu „odposlech a záznam telekomunikačního provozu“ korespondovalo nejen zákonu č. 151/2000 Sb., jenž byl v účinnosti poměrně dlouhou dobu, po kterou probíhalo uplatňování tohoto úkonu, ale především zákonu č. 110/1964 Sb., o telekomunikacích, pocházejícímu ještě z éry socialismu. Novela trestního řádu provedená s účinností od 1. 7. 1990 vložila do § 88 tr. ř. (paradoxně na místo, kde až do novely č. 57/1965 Sb. existovala úprava zajišťovacích úkonů bezpečnostními orgány ve stadiu před zahájením vyšetřování) nový institut s označením „Odposlech telefonních hovorů“, a až novela trestního řádu č. 292/1993 Sb. (účinná dnem 1. 1. 1994) použila poprvé označení „Odposlech a záznam telekomunikačního provozu“.

Není však ničím neobvyklým, vychází-li určitý právní předpis (a vztahuje se to plně i na kodexy) z terminologie a obsahu souvisejících právních předpisů podle doby svého vzniku, z pochopitelných důvodů nemůže příliš přihlížet k možnému vývoji v dané oblasti.

Výklad příslušných pojmů musí být prováděn vždy v souladu nejen s účelem a smyslem právní úpravy tak, jak je v daném zákoně uvedena a odůvodněna v rámci důvodových zpráv, vystoupení předkladatele normy, pozměňovacích návrhů v průběhu legislativního procesu, atd., ale také v kontextu se souvisejícími právními předpisy, které mohou nabýt účinnosti případně i s velkým časovým odstupem po vydání zákona, o jehož aplikaci v konkrétním případě jde.

Dnes je třeba vycházet plně z ustanovení zákona č. 127/2005 Sb., o elektronických komunikacích. Totéž se týká i úkonu upraveného v § 88a tr. ř. I sám citovaný zákon provádí v rámci přechodného ustanovení zpřesnění, jež je i jistým unikátem.⁵ Dokonce – i kdyby byl vytvořen takový modernistický právní předpis, jenž by v předstihu reagoval na očekávaný vývoj týkající se předmětu své úpravy, nepochybně by se setkával se závažnými problémy při aplikaci, protože by vůbec neodpovídal znění souvisejících zákonů.

Možná i proto je osud legislativního návrhu vypracovaného Nejvyšším státním zastupitelstvím poměrně komplikovaný a nejasný.

I. Statistiky a analýzy

Na základě požadavku ministra vnitra č. j. OBP-383-4/P-2007 ze dne 17. prosince 2007 a v souladu s § 98 odst. 3 zákona č. 273/2008 Sb., o Policii České republiky, byla Policejním prezidiem ČR zpracována „Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob

Elektronickou zprávou by se přitom měla rozumět textová, hlasová, zvuková nebo obrazová zpráva přenášená prostřednictvím sítě elektronických komunikací.

Ohledně návrhu pak probíhaly diskuse v rámci pracovní skupiny Ministerstva spravedlnosti k tzv. e-důkazům, kde se řešily i četné další otázky fenoménu nazývaného elektronické důkazy. Zatím se k definitivní podobě návrhu novelizace trestního řádu nedospělo a do konce volebního období (v září či říjnu 2017 se budou v ČR konat parlamentní volby) zřejmě už ani nedospěje.

⁵ Srov. § 136 odst. 20 zákona č. 127/2005 Sb., z něhož vyplývá, že 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, c) telekomunikační službě, rozumí se tím služba elektronických komunikací podle tohoto zákona, d) telekomunikační síti, rozumí se tím síť elektronických komunikací podle tohoto zákona.

a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2012“ (dále jen „Analýza“). Přestože to zákon č. 273/2008 Sb., o Policii ČR nepožaduje, zveřejňují se ve zprávě rovněž údaje o využívání výpisu o telekomunikačním provozu Policií ČR dle § 88a tr. ř. Nově i o sledování osob a věcí.

Takové zprávy jsou publikovány od roku 2007.

Ze zpráv lze zjistit např. i interní předpisy Policie České republiky týkající se odposlechů, jmenovitě závazný pokyn policejního prezidenta č. 186/2011, o vyžadování odposlechu a záznamu telekomunikačního provozu a údajů o uskutečněném telekomunikačním provozu, účinný od 7. října 2011, ve znění novely č. 139/2012 Sb., stejně tak jako závazný pokyn č. 209/2008, kterým se upravuje postup při vyžadování sledování osob a věcí pro účely trestního řízení, ve znění pozdějších změn.

Ve zprávě se zmiňuje postup policejních orgánů při provádění úkonů podle § 88 a § 88a tr. ř. Dále též podle § 158d tr. ř.

Obdobně zprávy zpracovává i Generální inspekce bezpečnostních sborů.

Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR je zpracována i za rok 2015, nikoli ještě za rok 2016.

Všechny tyto analýzy obsahují velice podnětné údaje k vývoji počtu úkonů podle § 88, 88a a 158d tr. ř.⁶

Zprávy o činnosti státního zastupitelství za uplynulý rok rovněž obsahují důležité údaje.⁷

V minulosti byly zpracovány i zvláštní zprávy analyzující fenomén odposlechu a záznamu telekomunikačního provozu a zjišťování údajů z něj.⁸

⁶ Srov. následující webové odkazy: <http://www.mvcr.cz/clanek/odposlechy-zaznamy-telekomunikacniho-provozu-a-sledovani-osob.aspx>.

<http://www.langer.cz/data/publikace/analiza-odposlechy-2007.pdf>

http://www.gibs.cz/ostatni/analiza_ukonu_2015.pdf

<http://www.ceska-justice.cz/2016/07/analiza-uooz-nasazuje-stale-vice-odposlechu-na-korupci/>.

⁷ Srov. <http://www.nsz.cz/index.php/cs/udaje-o-cinnosti-a-statisticke-udaje/zprava-o-innosti>.

⁸ Byly to:

1. Zvláštní zpráva obsahující vyhodnocení odposlechu a záznamu telekomunikačního provozu a zjišťování údajů z telekomunikačního provozu v roce 2002 a 2003 v České republice

2. Zvláštní zpráva obsahující vyhodnocení odposlechu a záznamu telekomunikačního provozu, zjišťování údajů z telekomunikačního provozu a využívání operativně pátracích prostředků v roce 2005 a 2006.

Porovnávat statistické podklady státního zastupitelství a Policie ČR nelze; každé z vyhodnocení vychází ze zcela odlišného souboru údajů. Je nutné také vzít v úvahu i odchylnou metodiku zjišťování počtu odposlechů.

K otázce nevyhovění návrhu na vydání příkazu k odposlechu a záznamu telekomunikačního provozu nebo návrhu na prodloužení provádění takového odposlechu ze strany soudce bylo uvedeno zejména toto:

Jedná se tu o otázku, která bývala v diskusích, jež ohledně odposlechů probíhají přinejmenším od roku 2003, posuzována někdy v poněkud absurdní rovině: Předmětem kritiky se stala nezhřídka skutečnost, že počty případů, kdy soudci návrhům státních zástupců nevyhověli, je zcela minimální. Tento fakt se – aniž by byla provedena věcná analýza – často kladl do souvislosti s tím, že údajně „soudci jsou pod tlakem policie“, nemají dostatek času na prostudování předložených spisových materiálů, a přesto příkazy k odposlechu vydávají.

Obdobně to bylo konstatováno i nedávno v souvislosti s kauzou D. R.

Proto se jak zvláštní zpráva z roku 2007, tak i předchozí zvláštní zpráva z roku 2004, zvláště zajímala o případy, kdy návrh státního zástupce na nařízení odposlechu je soudcem odmítnut. Bez opravdu věcné analýzy podložené konkrétními fakty totiž nepřichází v úvahu náležité zhodnocení daného problému.

Nevyhovění návrhu soud zdůvodňoval tím, že 1. se nejednalo o dostatečně odůvodněné podezření z některého trestného činu uvedeného v § 88 odst. 1 tr. ř. včetně případů, kdy nebyl policejním orgánem sepsán záznam o zahájení úkonů trestního řízení, 2. nebylo doloženo, že odposlechem a záznamem telekomunikačního provozu budou sděleny skutečnosti významné pro trestní řízení, 3. nebyla doložena souvislost mezi účastníkem telefonní stanice a osobou důvodně podezřelou ze spáchání trestného činu nebo předmětem trestního řízení, 4. došlo k ukončení

II. Nezbytnost řádného zdůvodnění nařízení odposlechu a záznamu telekomunikačního provozu, příkazů ke zjištění údajů z telekomunikačního provozu a příkazu ke sledování osob a věcí

Usnesení velkého senátu trestního kolegia Nejvyššího soudu ze dne 26. 6. 2013, sp. zn. 15 Tdo 510/2013 (č. 13/2014 Sb. rozh. tr.) mj. konstatuje (srov. bod III. judikátu), že:

„Soud před vydáním příkazu k domovní prohlídce (§ 83 odst. 1 tr. ř.) je povinen bedlivě zkoumat, zda v posuzované věci jsou pro nařízení domovní prohlídky splněny všechny zákonné podmínky, které je v odůvodnění příkazu povinen náležitě a zřetelně vyložit. Jestliže je příkaz k domovní prohlídce vydáván ve stadiu „prověřování podezřelého“, nikoli tedy ve stadiu trestního stíhání obviněného, je třeba v odůvodnění vysvětlit, proč jde o úkon neodkladný nebo neopakovatelný, popř. to uvést v protokolu o domovní prohlídce (§ 160 odst. 4 tr. ř.), což by mělo být z logiky věci obsaženo již v návrhu státního zástupce.

V případě, že takové zdůvodnění příkaz nebo protokol neobsahuje, lze odstranit nedostatek formálních podmínek příkazu nebo protokolu (tedy i o neodkladném úkonu), v dalším řízení, a to např. výslechem osob, které se provedení úkonu zúčastnily, popř. jej provedly (v postavení svědka). Smyslem a účelem povinnosti vyložit věcné důvody pro neodkladnost a neopakovatelnost úkonu v protokolu je totiž zaručit transparentnost trestního řízení a jeho kontrolovatelnost, tj. zajistit náležitou přezkoumatelnost těchto úkonů. Jestliže při následném posouzení a po zvážení všech souvislostí lze konstatovat, že věcné důvody pro neodkladnost či neopakovatelnost úkonu byly splněny, pak neexistence zdůvodnění neodkladnosti nebo neopakovatelnosti – byť je vadou řízení – nevede k závěru o nezákonnosti příslušných meritorních rozhodnutí, neboť jde ve své podstatě o vadu toliko formální, bez vlivu na věcnou správnost provedení neodkladného či neopakovatelného úkonu.“

Za řádné zdůvodnění je možné určitě považovat, na což koneckonců výslovně pamatuje zákon (§ 160 odst. 4 věta poslední tr. ř.), pokud jsou skutečnosti, na základě nichž byla domovní prohlídka, resp. prohlídka jiných prostor a pozemků považována za úkon neodkladný nebo neopakovatelný, uvedeny v protokolu.

Nicméně i kdyby tyto skutečnosti v protokolu uvedeny nebyly, s oporou doktríny materiálního právního státu by to nemuselo automaticky znamenat vybočení z ústavněprávních mezí. Viz usnesení Ústavního soudu ze dne 26. 3. 2009 sp. zn. I. ÚS 3108/08, publikované pod č. 9/2009 Sb. n. u. US [dostupný z ASPI, verze 502]: „Smyslem a účelem požadavku existence protokolu o provedení neodkladného či neopakovatelného úkonu je především vytvoření prostoru pro představení věcných důvodů pro neodkladnost a neopakovatelnost úkonu v protokolu. [Ostatně zřejmě právě proto trestní řád explicitně uvádí (v § 160 odst. 4 in fine trestního řádu), – a tím zdůrazňuje – povinnost uvést v protokolu o provedení neodkladného či neopakovatelného úkonu, na základě jakých skutečností byl úkon za neodkladný nebo neopakovatelný považován (tato povinnost by byla vyvoditelná z trestního řádu i bez takové výslovné úpravy).]. Smyslem a účelem povinnosti vyložit věcné důvody pro neodkladnost a neopakovatelnost úkonu v protoko-

odposlechu a záznamu telekomunikačního provozu probíhajícího v jiné trestní věci, aniž by byly zjištěny jakékoli rozhodné skutečnosti, 5. jiné důvody.

Lze tedy klást otázku, zda tato skutečnost svědčí pro vysokou kvalitu a odůvodněnost návrhů státních zástupců, nebo je důsledkem nepříliš důsledného postupu soudů. Poznatky zvláštní zprávy svědčí spíše pro první variantu, názory, jež vycházejí z varianty druhé, jsou v soustavě státního zastupitelství zcela ojedinělé.

Podle toho, co se v této zvláštní zprávě uvádí (případně v dalších analytických materiálech, na něž tu bylo již poukázáno), lze spíše usuzovat, že nízký výskyt případů nevyhovění návrhu státního zástupce soudcem plyne spíše ze zlepšené kvality těchto návrhů; pro závěr, že soudci postupují jen formálně a bez znalosti spisu, nebyly k dispozici žádné relevantní informace.

lu je – vzhledem k charakteru neodkladných a neopakovatelných úkonů (výrazným způsobem limitujících zejména realizaci práva na obhajobu podezřelých osob) – zaručit transparentnost trestního řízení a jeho kontrolovatelnost, tj. zajistit náležitou přezkoumatelnost těchto úkonů ex post (srov. obdobně usnesení Ústavního soudu sp. zn. III. ÚS 1033/07).

Z vyložené teleologie věci plyne, že jestliže při následné kontrole a po zvážení všech souvislostí lze konstatovat, že věcné důvody pro neodkladnost či opakovanost úkonu byly splněny, pak neexistence zdůvodnění sama o sobě – byť je vadou řízení – nedosahuje ústavněprávní roviny, která by měla být důvodem pro rušení příslušných meritorních rozhodnutí. Jde pak totiž ve své podstatě o vadu toliko formální, bez vlivu na věcnou správnost provedení neodkladného či neopakovatelného úkonu. Takový právní názor je projevem v judikatuře Ústavního soudu deklarované doktríny materiálního právního státu. Tím méně pak – z logiky věci – může dosahovat Ústavněprávní intenzity neexistence pouze formálních náležitostí protokolu o provedení neodkladného úkonu. Ostatně, ústavně konformní je rovněž názor o možnosti odstranit nedostatek formálních podmínek protokolu sepsaného o jakémkoliv úkonu trestního řízení (tedy i o neodkladném úkonu), a to např. výsledkem osob, které se provedení úkonu zúčastnily, popř. jej provedly (v postavení svědka).“

Zase jiné judikáty Ústavního soudu vyzvedly názor, že soud, resp. orgán činný v trestním řízení, je povinen – tj. nejen v protokolu o domovní prohlídce, resp. prohlídce jiných prostor a pozemků – v příkazu k domovní prohlídce, resp. prohlídce jiných prostor a pozemků, uvést, že jde o neodkladný nebo neopakovatelný úkon, a přezkoumatelným způsobem vysvětlit, proč byla domovní prohlídka, resp. prohlídka jiných prostor a pozemků, vykonána jako neodkladný nebo neopakovatelný úkon.⁹

⁹ V tomto směru je rozšiřován okruh standardních náležitostí příkazu k domovní prohlídce. Srov. např. nález Ústavního soudu ze dne 10. 3. 2011 sp. zn. II. ÚS 3073/10, publikovaný pod č. 41/2011 Sb. n. u. US [dostupný z ASPI, verze 502]: „Ústavní soud v minulosti dovedl, že pokud ještě nebylo zahájeno trestní stíhání konkrétní osoby, musí být příkaz k provedení domovní prohlídky vydán s odůvodněním toho, že jde o úkon neodkladný nebo neopakovatelný. Napadený příkaz k domovní prohlídce vůbec neuvádí, že by se mělo jednat o úkon neodkladný a neopakovatelný, natož z jakých důvodů. Tento příkaz přitom finalizuje oprávnění policejního orgánu, coby orgánu veřejné moci, k zásahu do základního práva podle čl. 12 Listiny. To je dáno tím, že právě příkazem k domovní prohlídce je konstatována důvodnost, resp. zákonnost její realizace, a to včetně případných podmínek, za kterých musí být vykonána. Tuto přezkumnou a do značné míry i dozorčí funkci soudu nad průběhem trestního řízení na sebe nemůže převzít sám policejní orgán tím, že v protokolu o provedení domovní prohlídky vzdor mlčení soudního příkazu k domovní prohlídce tuto označí za úkon neodkladný a neopakovatelný, jak se stalo v daném případě. Obecný soud porušil základní práva stěžovatele podle čl. 12 odst. 1 a 2 a čl. 36 odst. 1 Listiny, když vydal příkaz k domovní prohlídce bytu užívaného stěžovatelem, aniž by se zabýval tím, zda se jedná o úkon neodkladný či neopakovatelný, a z jakého konkrétního důvodu.“

Že sice příkaz k domovní prohlídce, resp. prohlídce jiných prostor a pozemků, má obsahovat odůvodnění, že byl vydán jako neodkladný nebo neopakovatelný úkon, avšak postačí odůvodnění v minimálním rozsahu, aniž by se zakládal ústavněprávní deficit, vyplývá např. z nálezu Ústavního soudu ze dne 25. 8. 2008 sp. zn. IV. ÚS 1780/07, publikovaného pod č. 147/2008 Sb. n. u. US [dostupný z ASPI, verze 502]: „Ústavní soud v nálezu sp. zn. II. ÚS 298/05 vyvodil, že „Orgán, který takový úkon provádí, je povinen se otázkou, na základě jakých skutečností byl úkon za neodkladný nebo neopakovatelný považován, zabývat a přezkoumatelným způsobem svůj závěr vysvětlit. V důsledku toho shledal, že postup Policie ČR, při němž ve fázi před zahájením trestního stíhání, kdy ještě není jasně vymezen skutek ani stanoven okruh osob podezřelých, provedla úkon upravený v hlavě čtvrté trestního řádu – prohlídku jiných prostor – jako běžný úkon způsobem výše popsáním, jímž došlo k dotčení ústavně zaručených práv třetí osoby – stěžovatelky (čl. 2 odst. 2, čl. 11 odst. 1 a odst. 4 Listiny), aniž by přezkoumatelným způsobem zdůvodnila, proč provedení úkonu nebylo možné odložit na pozdější stadium trestního řízení, vybočuje z mezí ústavnosti. Argumentací a minori ad maius ve spojení s argumentem ad absurdum nutno daný ústavně konformní výklad předmětného normativního rámce vztáhnout i na domovní prohlídku ve smyslu § 83 odst. 1 ve spojení s § 82 odst. 1 trestního řádu, a to jak z hlediska věcného, tak i orgánu (obecného soudu), který se na ní v prvopočátku (vydáním příkazu k domovní prohlídce) výkonem své pravomoci podílí.“

Vždy musí být rozlišovány dvě modelové situace. Za prvé, k provedení domovní prohlídky, resp. prohlídky jiných prostor a pozemků (nebo jiného zásahu), jako neodkladného nebo neopakovatelného úkonu, absentuje důvod, a tak není ani uveden v protokolu (či příkazu). Za druhé, k vykonání domovní prohlídky, resp. prohlídky jiných prostor a pozemků, jako neodkladného nebo neopakovatelného úkonu, je sice založen důvod, ale není (pouze) v protokolu o jejím vykonání uveden.¹⁰

Zcela zásadní je v této souvislosti nález Ústavního soudu sp. zn. I. ÚS 615/06, který uvádí:

„Z hlediska ústavního pořádku je porušení tajemství zpráv, podávaných telefonem, možné jen v případech a způsobem stanoveným zákonem. Zákonná úprava zásahu do tohoto práva musí být formulována tak, aby nebyla popřením tohoto základního lidského práva, a tomu musí také odpovídat i její interpretace. Podústavní právo v § 88 tr. ř. umožňuje bez souhlasu majitele či oprávněného uživatele telefonní stanice provádět odposlech jeho komunikace jen v trestním řízení, vedeném pro zvláště závažný úmyslný trestný čin nebo pro jiný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva, pokud lze důvodně předpokládat, že jím budou sděleny významné skutečnosti pro trestní řízení. Soudní příkaz k odposlechu a záznamu telekomunikačního provozu musí být podle téhož zákonného ustanovení písemný a odůvodněný. Z toho vyplývá, že musí být vydán ve vztahu k určité osobě, proti níž se již trestní stíhání pro uvedené trestné činy vede, nebo vůči níž je důvodné podezření, že se takových trestných činů dopustila. Pokud je řízení vedeno pouze na základě důvodného podezření, musí být v odůvodnění vyloženo, o jaké indicie se takový závěr opírá. Pouhé trestní oznámení samo o sobě, není-li doloženo alespoň indiciemi, z nichž lze důvodně podezření dovozovat, nepostačuje k nařízení odposlechů, neboť totiž nepostačuje ani k zahájení řízení k objasnění a prověřování skutečností důvodně nasvědčujících tomu, že byl spáchán trestný čin podle § 158 tr. ř. Může tedy být vydán jen v řádně zahájeném trestním řízení pro zákonem kvalifikovanou trestnou činnost, a musí být podložen relevantními indiciemi, z nichž lze dovodit důvodné podezření ze spáchání takového trestného činu. Příkaz musí být individualizován ve vztahu ke konkrétní osobě, která je uživatelem telefonní stanice. Pokud tato skutečnost nevyplývá ze zjištění, že se jedná o majitele telefonní stanice, musí být zdůvodněno, na základě jakých zjištění je dovozováno, že ji má v držení a že ji skutečně používá, nebo ji v minulosti v nikoliv nepodstatné míře používala, a že tak bude s vysokou pravděpodobností činit i v budoucnu. Konečně musí příkaz alespoň v minimální míře konkrétně uvést, jaké skutečnosti významné pro trestní řízení mají být takto zjištěny, a z čeho je to vyvozováno.“

Ze striktního požadavku odůvodnění úkonů podle § 88, 88a a 158d odst. 2 a 3 tr. ř. vychází i připravovaná interní úprava pro státní zástupce.¹¹

¹⁰ Srov. i rozh. č. 38/2013 Sb. rozh. tr.: „V protokolu o provedení neodkladného nebo neopakovatelného úkonu musí být vždy uvedeno, na základě jakých skutečností lze považovat úkon za neodkladný nebo neopakovatelný. Pokud v tomto protokolu ani v příkazu k prohlídce jiných prostor a pozemků nebyla odůvodněna neodkladnost úkonu, pak je nutné povahu tohoto pochybení zvažovat i z materiálního hlediska, tedy zda i přes chybějící odůvodnění existují v konkrétním případě podmínky pro provedení tohoto úkonu uvedené v § 160 odst. 4 trestního řádu.“ Dopadá na situaci, kdy k vykonání prohlídky jiných prostor a pozemků, resp. domovní prohlídky, jako neodkladného nebo neopakovatelného úkonu, je založen důvod, ale není jen v protokolu o jejím vykonání uveden. Jsou-li tak zákonné podmínky pro provedení těchto úkonů splněny, chybějící odůvodnění není vadou neodstranitelnou, a proto je ji nutno hodnotit materiálně.“

¹¹ Jedná se o pokyn obecné povahy, o postupu státních zástupců v trestním řízení, jenž má nahradit stále ještě platný pokyn obecné povahy č. 8/2009.

Příkladem lze uvést návrh na odposlech: „Státní zástupce před podáním návrhu na odposlech a záznam telekomunikačního provozu (dále jen „odposlech“) nebo návrhu na jeho prodloužení soudci ověří, zda je trestní řízení vedeno pro trestný čin, pro který lze tento úkon nařídit. Učiní tak zejména posouzením, zda užitá právní kvalifikace odpovídá skutku popsanému v záznamu o zahájení úkonů trestního řízení nebo v usnesení o zahájení

III. Výkladové stanovisko č. 1/2015 Sb. v. s. NSZ – vzájemný vztah institutů odposlechu a záznamu telekomunikačního provozu, zjišťování údajů z něj a sledování osob a věcí

Stanovisko ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek obsahuje následující právní věty:

„I. Právní závěry výkladového stanoviska poř. č. 4/2005 Sb. v. s. Nejvyššího státního zastupitelství lze mít s výjimkou použitelnosti § 88a tr. ř. nadále za aktuální a použitelné nejen na v souladu s trestním řádem zajištěné mobilní telefony, ale i jiné datové nosiče, které mohou obsahovat údaje o různých formách uskutečněné elektronické komunikace.¹²

II. Zjišťování obsahu elektronické komunikace uskutečněné po zajištění datového nosiče orgánem činným v trestním řízení je možné v reálném čase postupem podle § 88 trestního řádu, nikoli už podle § 88a tr. ř.

III. Aktuální obsah e-mailové schránky je určován vůlí uživatele a lze jej zjišťovat postupem podle § 158d odst. 3 tr. ř., který je možno považovat za zákonnou licenci prolamující ústavně zaručené právo na ochranu soukromí v e-mailové schránce se nacházejících záznamů, a to podle platné právní úpravy v případě trestního řízení pro kterýkoli úmyslný trestný čin.

IV. Zjišťování e-mailové komunikace v reálném čase je možné jen postupem podle § 88 odst. 1 tr. ř., neboť se stejně jako telekomunikační provoz uskutečňuje rovněž v síti elektronických komunikací. Postup podle § 88a trestního řádu není v takovém případě možný.“

Odůvodnění výkladového stanoviska č. 1/2015 Sbírky výkladových stanovisek vyhodnotilo i aplikační praxi státních zastupitelství do doby jeho vydání.

V případě zákonným způsobem zajištěných mobilních telefonů a jejich součástí (což mohou být nejen SIM karty, ale i v mobilních telefonech vložené paměťové karty) se státní zástupci nadále i s ohledem na čl. 46 odst. 2 pokynu obecné povahy nejvyššího státního zástupce č. 8/2009, o trestním řízení, ve znění pozdějších pokynů [citovaná interní úprava plně vycházela a vychází

trestního stíhání. Při tom je nutno vycházet z konkrétních skutkových okolností věci v době, kdy má být takový návrh podán; je třeba prověřit, zda odposlechem mohou být zjištěny významné skutečnosti pro trestní řízení a že sledovaného účelu nelze dosáhnout jinak nebo by jeho dosažení jinak bylo podstatně ztíženo; takové skutečnosti musí být v návrhu popsány. Vždy se uvede i odůvodnění, z jakých důvodů je úkon, jehož nařízení se navrhuje, považován za neodkladný nebo neopakovatelný (§ 160 odst. 4 poslední věta tr. ř.).“

¹² Jen pro bližší informaci výkl. stan. č. 4/2005 Sb. v. s. NSZ:

Stanovisko ke sjednocení výkladu zákonů a jiných právních předpisů k postupu v případech, kdy je třeba pro účely trestního řízení zjistit obsah údajů uložených v nalezeném, vydaném či odňatém mobilním telefonu, včetně údajů uložených na SIM kartě:

Způsob zjišťování obsahu údajů uložených v nalezeném, vydaném či odňatém mobilním telefonu v přípravném řízení vychází z toho, zda tyto informace (jejich obsah) jsou orgány činnými v trestním řízení zjišťovány za součinnosti subjektu, jenž je ohledně nich vázán zvláštní povinností mlčenlivosti vyplývající ze zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), v podobě důvěrnosti zpráv a s nimi spojených provozních a lokalizačních údajů, které se přenášejí prostřednictvím veřejné komunikační sítě a veřejně dostupných služeb elektronických komunikací, či nikoli, a proto

a) pokud bude třeba obsah těchto údajů zjistit v době jejich přenosu od volajícího k volanému, tedy v době, kdy uvedená zvláštní povinnost mlčenlivosti trvá, a přitom ke zjištění těchto údajů bude zapotřebí součinnosti subjektů poskytujících telekomunikační služby, musí mít orgány činné v trestním řízení k takovému úkonu příslušný příkaz soudce vydaný podle § 88, resp. § 88a tr. ř.,

b) pokud budou takovými údaji jen údaje již zprostředkované (doručené) volanému (oprávněnému účastníku telekomunikačního provozu) před tím, než mobilní telefon získaly do své moci orgány činné v trestním řízení, není třeba ke zjištění jejich obsahu vyžadovat příkaz soudce, jestliže orgány činné v trestním řízení zajistily mobilní telefon jako věc důležitou pro trestní řízení postupem odpovídajícím trestnímu řádu (např. podle § 78, § 79, § 82 a násl., § 113 tr. ř.).

ze závěrů stanoviska č. 4/2005 Sbírky výkladových stanovisek; aktuálně se však zpracovává zcela nový pokyn obecné povahy) ve většině případů při zjišťování jejich obsahu řídí výkladovým stanoviskem poř. č. 4/2005 Sb. v. s. NSZ. Jeho obecná použitelnost je přitom akceptována i ohledně obsahu paměti výpočetní techniky (částí počítačového systému jako tzv. harddisky) a jiných nosičů informací (např. USB disky), které mohou obsahovat různé formy elektronické komunikace [ve smyslu textových, hlasových (vč. záznamů volání), zvukových nebo obrazových zpráv přenášených prostřednictvím sítě elektronických komunikací].

Pouze ojediněle, s ohledem na rozhodnutí Vrchního soudu v Olomouci ze dne 15. 6. 2010 sp. zn. 5 To 42/2010,¹³ zejména pokud jde o státní zástupce činné v obvodu jeho působnosti, státní zástupci před zjišťováním obsahu mobilních telefonů a jejich součástí (SIM karty či paměťové karty) s pozitivním výsledkem navrhuji vydání příkazů podle § 88 či § 88a tr. ř.

Vrchní státní zastupitelství v Praze pak s ohledem na změnu § 88a tr. ř. od vydání předmětného výkladového stanoviska shledávalo potřebu jej rozvést ohledně úvah, zda a jakým zákonným způsobem lze dosáhnout zpřístupnění SMS zpráv, které byly doručeny na mobilní telefon až poté, co již jej mají v souladu se zákonem v moci orgány činné v trestním řízení.

Ohledně zákonných možností zajišťování e-mailové komunikace ze soustavy státního zastupitelství pak vyplývá naléhavý požadavek na sjednocení výkladu právních předpisů vztahujících se k dané problematice, protože právní názory a od nich se odvíjející praxe jsou roztržštěny. K úvaze je dáváno případně i iniciování legislativní změny. Krajské státní zastupitelství v Praze by se přiklábělo alespoň k iniciování sjednocení rozhodovací praxe soudů, podle kterého by se pak odvíjela návrhová činnost státních zástupců. Soudy totiž v současné době zpravidla akceptují různé návrhy státních zástupců za účelem zajišťování e-mailové komunikace. Návrhy jsou přitom podávány podle § 88 odst. 1, 2 tr. ř. v případě zajišťování e-mailové komunikace do budoucna. Vrchní státní zastupitelství v Olomouci v tomto případě nevylučuje ani možnost postupu podle § 158d odst. 1, 3 tr. ř. s ohledem na skutečnost, že ani v tomto případě není zapotřebí součinnosti poskytovatele služby e-mailové pošty. V případě zpětného zajišťování e-mailové komunikace převažují návrhy na povolení sledování osob a věci podle § 158d odst. 1, 3 tr. ř.

Odbor trestního řízení NSZ ve svém vyjádření rozvedl, proč je tento postup jediným možným a správným a připomněl usnesení Ústavního soudu ČR ze dne 3. 10. 2013 sp. zn. III. ÚS 3812/2012 jako doposud jediné s danou problematikou související rozhodnutí, ze kterého by bylo možno analogicky dovozovat použitelnost § 158d odst. 3 trestního řádu ke zjišťování obsahu e-mailových schránek.

V rámci sledování elektronických zařízení z povahy věci plyne, že předmětem sledování budou právě data na těchto zařízeních uložená, jejichž otisk lze pořídit za využití utajené operativně pátrací techniky. Pořízení otisku elektronických dat lze povolit postupem dle § 158d odst. 3 tr. ř., pokud jde o data na sledovaných počítačích již uložená, nikoli o data telekomunikačního provozu. Z uvedeného textu rozhodnutí přímo vyplývá, že se naopak předpokládá sledování dle § 158d tr. ř. formou jednorázového „otisku“ dat na zařízení již uložených.

Využívány však jsou i návrhy na soudní příkaz podle § 88a odst. 1 tr. ř. V případě těchto návrhů státní zástupci argumentují tím, že podle § 88a odst. 1 tr. ř. zjistitelné „údaje o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje

¹³ Tímto rozhodnutím byla zamítnuta stížnost státního zástupce proti prvostupňovému soudnímu rozhodnutí o vrácení věci k došetření, přičemž stížnostní soud shledal závažnou procesní vadu mj. v tom, že znalecký posudek z oboru kybernetika, odvětví výpočetní techniky, kterým byl zjištěn obsah paměti SIM karet zajištěných mobilních telefonů obviněných, o který se obžaloba opírá jako o jeden ze stěžejních důkazů, byl podán bez předchozího soudního příkazu podle § 88a tr. ř. Na podporu tohoto závěru byla označena rozhodnutí Ústavního soudu ČR sp. zn. II. ÚS 502/2000 a II. ÚS 789/2006.

ochrana osobních a zprostředkovacích dat“, nelze omezovat jen na provozní a lokalizační údaje podle zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů. Někteří státní zástupci ohledně použitelnosti § 88a tr. ř. zastávají právní názor, že sledování osob a věcí podle § 158d tr. ř. nelze realizovat pro získávání poznatků o osobách a věcech zpětně, ale jen v reálném čase v době trvání povolení. O tuto argumentaci se opírají zatím ale jen ojedinělá soudní rozhodnutí, kterými nebylo návrhům státních zástupců na povolení sledování podle § 158d odst. 3 tr. ř. ohledně konkrétních e-mailových schránek (účtů) vyhověno.

Jako na nikoli nepodstatnou právně významnou skutečnost pak bylo poukázáno i na to, že e-mailovou komunikaci jako službu mohou poskytovat nejen subjekty podle zákona č. 127/2005 Sb., ale i podle zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů, na které nedopadá povinnost uchovávat provozní a lokalizační údaje podle zákona č. 127/2005 Sb. Nabízí se proto ze strany některých státních zástupců úvaha, zda ve vztahu k těmto subjektům by nemohlo přicházet v úvahu získávání údajů o e-mailové komunikaci, včetně jejího obsahu, podle § 8 odst. 1, popř. podle § 8 odst. 5 tr. ř.¹⁴

Tuto otázku řešilo Nejvyšší státní zastupitelství samostatně a přípisem ze dne 31. 8. 2015 sp. zn. 1 SL 728/2015 uvedlo mj., že ve stanovisku č. 1/2015 Sb. v. s. Nejvyššího státního zastupitelství ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek je podrobně vyloženo, proč by měla být e-mailová komunikace považována za jednu z forem elektronické komunikace i ve smyslu zákona č. 127/2005 Sb., o elektronických komunikacích a vyloženy možnosti jejího zjišťování do budoucna (§ 88 odst. 1 trestního řádu) a zpětně (zjištění aktuálního obsahu e-mailové schránky v konkrétní e-mailové schránce), kde předmětné výkladové stanovisko připouští možnost povolení sledování osob a věcí soudem podle § 158d odst. 1, 3 trestního řádu.

V případě fyzické nebo právnické osoby poskytující služby elektronickými prostředky (tzv. informační společnost), která není současně podnikatelem v elektronických komunikacích v souladu s § 8 odst. 2 zákona č. 127/2005 Sb., o elektronických komunikacích je otázkou, zda a v jakém rozsahu jsou na ní vymahatelné povinnosti uložené zákonem č. 127/2005 Sb., o elektronických komunikacích, mimo jiné umožnit soudem nařízený odposlech a záznam zpráv

¹⁴ Analytický a legislativní odbor NSZ řešil nedávno velmi zajímavý aplikační problém.

Policejní orgán nejprve požádá provozovatele schránky (tj. např. společnost Seznam.cz, a. s.) postupem podle § 8 odst. 1 tr. ř. o provedení zálohy obsahu schránky s termínem provedení ihned a současně požádá o vyrozumění o provedení této zálohy, a následně postupem podle § 8 odst. 5 tr. ř., tj. se souhlasem soudu, je následně takto provedená záloha vyžádána. Další možnou variantou postupu k provedení a vyžádání obsahu e-mailové komunikace je podle žadatele postup, kdy: Policejní orgán nejprve požádá provozovatele schránky postupem podle § 8 odst. 1 tr. ř. o provedení zálohy obsahu schránky s termínem provedení ihned, a postupem podle § 158d odst. 1, 3 tr. ř. vyžádá sledování takto provedené zálohy.

Zásadní zde byla otázka, zda lze zajistit zálohu obsahu e-mailové schránky (tzv. freezing), ať už na žádost policejního orgánu podle § 8 odst. 1 trestního řádu či na základě jiného instrumentu.

Stanovisko Útvaru zvláštních činností konstatuje, že v současné době není známa žádná speciální právní úprava, která by umožňovala zajistit zálohu obsahu e-mailové schránky tak, aby mohlo být zabráněno manipulaci s daty. Suplování absence zmocnění k provádění zálohy e-mailové schránky aplikací ustanovení § 8 odst. 1 tr. ř., za situace, kdy tu není žádná speciální právní úprava takovýto postup umožňující, je vnímána jako velmi sporná.

Ustanovení § 8 odst. 1 trestního řádu zakotvující obecnou povinnost vyhovovat dožádání orgánů činných v trestním řízení neobsahuje zákonnou úpravu (licenci) umožňující prolomení ústavně zaručeného práva na ochranu soukromí, vztahujícího se jak na obsah e-mailové schránky, tak i na zálohu jejího obsahu.

II. Orgány činné v trestním řádu se proto nemohou po poskytovateli služeb zajišťující přenos zpráv do e-mailové schránky a z ní, domáhat postupem podle § 8 odst. 1 trestního řádu obsahu e-mailových zpráv, ani provedení zálohy obsahu e-mailové schránky.

a uchovávat provozní a lokalizační údaje podle § 97 odst. 1, 3 zákona č. 127/2005 Sb., o elektronických komunikacích. Jak již bylo uvedeno i ve výkladovém stanovisku, k této právní otázce Nejvyššímu státnímu zastupitelství nepřísluší přijímat stanovisko či výklad. O takový subjekt se jedná mj. v případě obchodní společnosti SEZNAM.CZ, a. s., která jako provozovatel freemailové služby „Seznam Email“ však přesto tyto údaje uchovává, byť primárně pro účely vyúčtování a reklamace jí poskytovaných služeb.

Možnost jak získat údaje o telekomunikačním provozu od subjektu, na který nedopadají povinnosti podle zákona č. 127/2005 Sb., o elektronických komunikacích, za situace, že údaj disponuje (resp. uchovává), byť primárně pro účely vyúčtování a reklamace jim poskytovaných služeb, se však spatřují v postupu podle § 8 odst. 5 tr. ř., nikoli tedy v postupu podle § 88a tr. ř. Samozřejmě postup podle § 8 odst. 5 tr. ř. je doporučením a současně se uznává, že rozhodovací praxe soudů může být v této otázce odlišná.¹⁵

Z citovaných právních vět výkladového stanoviska lze dovozovat, že k důkazní použitelnosti SMS zpráv, které budou doručeny na zajištěný mobilní telefon¹⁶ až v době, kdy bude v držení orgánů činných v trestním řízení, se kterými se tedy nebude mít možnost jejich adresát (příjemce) seznámit, je nezbytný příkaz soudce podle § 88a tr. ř.

S ohledem na technický pokrok a vývoj v oblasti komunikačních technologií je třeba při posuzování aktuálnosti předmětného výkladového stanoviska vzít v úvahu, že uživatelé mobilních telefonů v nich za použití internetu využívají vedle telekomunikačního provozu (realizovaného prostřednictvím veřejných pevných a mobilních telefonních sítí) i jiné formy elektronické komunikace přes různé internetové sociální sítě a aplikace, např. Facebook, Skype, ICQ, Viber, Messenger, WhatsApp a další, jejichž prostřednictvím lze uskutečnit nejen volání, ale i posílat si textové zprávy či zprávy s datovými přílohami obrazového nebo textového charakteru, rovněž i komunikovat v rámci diskusních fór (tzv. chat). Prostřednictvím mobilních telefonů lze při vy-

¹⁵ Citované ustanovení § 8 odst. 5 tr. ř. zní: Nestanoví-li zvláštní zákon podmínky, za nichž lze pro účely trestního řízení sdělovat informace, které jsou podle takového zákona utajovány, nebo na něž se vztahuje povinnost mlčenlivosti, lze tyto informace pro trestní řízení vyžadovat po předchozím souhlasu soudce. Tím není dotčena povinnost mlčenlivosti advokáta podle zákona o advokacii.

Podle stanoviska Nejvyššího soudu sp. zn. Tpjn 303/2005 ze dne 28. 6. 2006 souhlas podle § 8 odst. 5 tr. ř. není soudce povinen udělit, naopak jemu samotnému přísluší v konkrétním případě posoudit, zda je průlom do povinnosti mlčenlivosti přípustný a v jakém nezbytném rozsahu (§ 2 odst. 4 a § 52 tr. ř., čl. 4 odst. 4 a čl. 10 Listiny základních práv a svobod a čl. 8 Úmluvy o ochraně lidských práv a základních svobod), aby se zabránilo tomu, aby vyžadování utajovaných informací nebo údajů, na něž se vztahuje povinnost mlčenlivosti, nebylo zneužíváno.

Rozh. č. 46/2006 Sb. rozh. tr.: Ustanovení § 8 odst. 5 tr. ř. se vztahuje pouze na případy, kdy zvláštní zákon nestanoví podmínky, za nichž lze informace (před 1. 1. 2006 „skutečnosti“), které jsou podle takového zákona utajovány, nebo na něž se vztahuje povinnost mlčenlivosti, sdělovat orgánům činným v trestním řízení. Nedostatek zákonných podmínek ve zvláštním zákoně nahrazuje souhlasem soudce, jemuž samotnému přísluší v konkrétním případě posoudit, zda je průlom do povinnosti mlčenlivosti přípustný a v jakém nezbytném rozsahu (§ 2 odst. 4 a § 52 tr. ř., čl. 4 odst. 4 a čl. 10 Listiny základních práv a svobod a čl. 8 Úmluvy o ochraně lidských práv a základních svobod).

Vydání souhlasu soudce s vyžadováním informací uvedených v § 8 odst. 5 tr. ř. pro trestní řízení není podmíněno předchozím neúspěšným pokusem orgánů činných v trestním řízení o jejich získání od subjektu, který je takovou povinností vázán, na základě jejího zproštění oprávněnou osobou.

¹⁶ Zajištěným mobilním telefonem se rozumí mobilní telefon, který se dostane do dispozice orgánů činných v trestním řízení v souladu s trestním řádem, tj. zejména na základě vydání nebo odnětí věci podle § 78 a § 79 tr. ř. [srov. novelu č. 55/2017 Sb., jež v uvedené oblasti učinila zásadní změny a zejména odlišila režim zajištění věcí pro účely důkazní a zajištění jako nástroje či výnosu z trestné činnosti], při domovní prohlídce nebo prohlídce jiných prostor a pozemků podle § 83 a § 83a tr. ř., při osobní prohlídce podle § 83b tr. ř. a nálezem při ohledání místa činu podle § 113 tr. ř.

užívání internetového připojení rovněž odesílat a přijímat e-maily, tedy využívat tzv. e-mailovou poštu, kterou lze považovat za jednu z forem elektronické pošty.¹⁷

Vše pochopitelně je rovněž chráněné ve sféře soukromí jako ústavně zaručeného práva podle článku 7 odst. 1, článku 10 odst. 1, 2, 3, a článku 13 Listiny základních práv a svobod a článku 8 odst. 1 Úmluvy o ochraně lidských práv a základních svobod (publikována pod č. 209/1992 Sb.).

Terminologie trestního řádu v § 88 a § 88a tr. ř. „telekomunikační provoz“ tedy již zcela nepostihuje všechny v úvahu přicházející formy elektronických komunikací realizovaných v sítích elektronických komunikací, mezi které v souladu se zákonem o elektronických komunikacích patří nejen telekomunikační provoz prostřednictvím veřejných telefonních sítí (mobilních a pevných), ale i jiné služby elektronických komunikací, realizované prostřednictvím veřejných komunikačních sítí [§ 2 písm. h), i) a k) zákona č. 127/2005 Sb.], založených na přenosu informací, tj. zejména služby realizované prostřednictvím internetu, jehož legální definici tento zákon a ani jiný právní předpis v našem právním řádu ale neobsahuje. Podle § 8 odst. 2 zákona č. 127/2005 Sb. oprávnění k podnikání v elektronických komunikacích vzniká k tomu způsobilým právníkům nebo fyzickým osobám dnem doručení oznámení podnikání Českému telekomunikačnímu úřadu. I bez tohoto oprávnění mohou služby elektronickými prostředky poskytovat fyzické nebo právnické osoby podle zákona č. 480/2004 Sb. Podle tohoto zákona je služba poskytnuta elektronickými prostředky, pokud je odeslána prostřednictvím sítě elektronických komunikací a vyzvednuta uživatelem z elektronického zařízení pro ukládání dat [§ 2 písm. a) tohoto zákona]. V § 2 písm. b) cit. zákona je pak i obsažena v našem právním řádu definice elektronické pošty, kterou se rozumí textová, hlasová, zvuková nebo obrazová zpráva poslaná prostřednictvím veřejné sítě elektronických komunikací, která může být uložena v síti nebo v koncovém zařízení uživatele, dokud ji uživatel nevyzvedne.¹⁸

Pokud jde o aktuální znění § 88a odst. 1 tr. ř., ve spojení s § 97 a § 136 odst. 20 písm. b) zákona č. 127/2005 Sb.,¹⁹ nelze přisvědčit právnímu závěru, že text § 88a odst. 1 tr. ř. „údaje o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat“ by bylo možno interpretovat i tak, že na základě § 88a odst. 1 tr. ř. by bylo možno navrhnout vydání soudního příkazu ke zjištění jiných, než provozních a lokalizačních údajů uchovávaných podle § 93 odst. 3, 4 zákona o elektronických komunikacích, tj. i ke zjištění obsahu elektronické komunikace. Osobními a zprostředkovacími daty nelze rozumět údaje spočívající v obsahu zpráv. Obsah zpráv totiž není podnikatel v elektronických komunikacích oprávněn uchovávat a tudíž ani oprávněn poskytnout. Doručením zprávy příjemci je služba elektronických komunikací (důvěrnosti podléhající komunikační provoz či elektronický přenos) příslušným podnikatelem dokončena a se zprávou je v rámci ústavně zaručeného práva na ochranu soukromí oprávněn nakládat výlučně její příjemce. Podle platné právní úpravy lze proto ke zjištění obsahu zpráv požadovat součinnost od podnikatele poskytujícího služby elektronické komunikace stejně jako v případě odposlechu pouze v době jejich přenosu na základě příkazu podle § 88 odst. 1 tr. ř.

¹⁷ Z § 2 písm. b) zákona č. 480/2004 Sb. plyne, že elektronickou poštou se rozumí textová, hlasová, zvuková nebo obrazová zpráva poslaná prostřednictvím veřejné sítě elektronických komunikací, která může být uložena v síti nebo v koncovém zařízení uživatele, dokud ji uživatel nevyzvedne, ...

¹⁸ Shodně elektronickou poštu definuje v čl. 2 (h) implementovaná Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. 7. 2002, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích).

¹⁹ Podle § 136 odst. 20 písm. b) cit. zákona obsahuje-li zvláštní právní předpis ustanovení o údajích o telekomunikačním provozu, rozumí se tím provozní a lokalizační údaje související s přenášenou zprávou podle tohoto zákona.

Pokud tedy bude orgán činný v trestním řízení předpokládat, že by se v době po zajištění mobilního telefonu či jiného datového nosiče mohla ve vztahu k němu, jako technickému zařízení, uskutečnit pro objasnění věci důkazně významná elektronická komunikace, se kterou ale nebude mít příjemce možnost se seznámit, bude muset být vydán soudní příkaz podle § 88 tr. ř. k odposlechu a záznamu telekomunikačního provozu pro možnost jejího zajištění během jejího přenosu nejen v případě elektronické komunikace ve formě zprávy hlasové (volání), ale i v případě zprávy textové, obrazové či datové. Pochopitelně pouze v řízení o trestných činech uvedených v § 88 odst. 1 tr. ř.

Standardně je však mobilní telefon či jiný datový nosič (zejména počítač) po jeho zajištění policejním orgánem uveden mimo provoz a předán, někdy i s odstupem nikoli jen dnů, ale i týdnů, k odbornému zjištění jeho obsahu prostřednictvím odborného vyjádření či znaleckého posudku z odvětví výpočetní techniky a až při analýze zjištěných údajů může vyjít najevo telekomunikační provoz, popř. jiná forma elektronické komunikace, která se uskutečnila až po zajištění datového nosiče (např. na mobilní telefon došly nové zprávy), aniž by byl po zajištění vydán soudní příkaz podle § 88 tr. ř. k odposlechu a záznamu telekomunikačního provozu. V tomto případě by s ohledem na stav platné právní úpravy a výše vyloženou nemožnost postupu podle § 88a odst. 1 tr. ř. mohlo být zjištění dodatečně došlých zpráv a hlasových zpráv uložených v hlasové schránce, při absenci souhlasu uživatele podle § 88 odst. 5, resp. § 88a odst. 4 tr. ř., možné jen na základě případného souhlasu soudce podle § 8 odst. 5 tr. ř., z důvodu trvání důvěrnosti (mlčenlivosti) elektronické komunikace.

Postup podle § 88a odst. 1 tr. ř. per analogiam by byl nepřipustně extenzivní.

K e-mailové komunikaci je možno uvést zejména toto:

E-mailová pošta je jednou z forem elektronické komunikace i ve smyslu zákona č. 127/2005 Sb., byť tento její vymezení neobsahuje. Splňuje totiž kritéria služby uskutečňované v sítích elektronických komunikací, v rámci které dochází k přenosu zpráv, které lze považovat za elektronickou poštu ve smyslu § 2 písm. b) zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů, ve znění pozdějších právních předpisů.

Z vyhlášky č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů, která byla přijata k provedení zákona č. 127/2005 Sb. (jeho § 97 odst. 4), pak jednoznačně vyplývá dopad tohoto zákona i na e-mailovou poštu jako jednu z forem elektronické pošty, neboť podle § 2 odst. 3 písm. c), d) ukládá povinnost uchovávat mj. údaje u služby přístupu ke schránce elektronické pošty a u služby přenosu zpráv elektronické pošty.

Stejně jako zprávy SMS nebo MMS, jsou i e-mailové zprávy mezi odesílatelem a příjemcem přenášeny v sítích elektronických komunikací a s ohledem na jejich obdobný charakter jim musí prospívat ústavní ochrana v souladu s článkem 7 odst. 1, článkem 10 odst. 1, 2, 3 a článkem 13 Listiny základních práv a svobod a článkem 8 odst. 1 Úmluvy ochrany lidských práv a základních svobod, prolomitelná jen na základě zákona.

V e-mailové schránce (někdy označované také jako e-mailový účet) se přitom mohou nacházet zprávy uživatelem odeslané, rozepsané (tzv. koncepty) a doručené, a to již přečtené, ale i nepřečtené, včetně jejich příloh. Rovněž i zprávy odstraněné do tzv. koše, ale neodstraněné trvale. Krajské státní zastupitelství v Ústí nad Labem pak přílehlavě poznamenalo, že do e-mailové schránky může mít přístup i více uživatelů, kteří zde mohou komunikovat prostřednictvím pouze rozepsaných zpráv, ohledně kterých nedojde k elektronickému přenosu, nicméně jsou rovněž obsahem e-mailové schránky. Obsah e-mailové schránky uživatele je přitom odvislý výlučně od vůle uživatele. Sama e-mailová schránka má fakticky charakter virtuálního soukromého prostoru (quasi datového internetového úložiště) a její provoz je realizován v souladu se smluvními podmínkami mezi uživatelem a poskytovatelem této služby. Poskytovatel služby zajišťující

přenos zpráv do e-mailové schránky a z ní, který může, ale nemusí být podnikatelem podle § 8 odst. 2 zákona č. 127/2005 Sb., není podle žádného zákonného ustanovení oprávněn uchovávat a jinému poskytovat obsah přenesených e-mailových zpráv.

Orgány činné v trestním řádu se proto nemohou po poskytovateli domáhat obsahu e-mailových zpráv postupem podle § 8 odst. 1 tr. ř., které neobsahuje zákonnou úpravu (licenci) umožňující prolomení ústavně zaručeného práva na ochranu soukromí, vztahujícího se i na obsah e-mailové schránky. Rovněž ani na základě soudního příkazu ke zjištění údajů o telekomunikačním provozu podle § 88a tr. ř., který jak bylo již výše vyloženo, je použitelný jen ke zjištění provozních a lokalizačních údajů ve smyslu zákona o elektronických komunikacích.

Pro objasnění věci v trestním řízení přitom může mít důkazní hodnotu ohledně zájmového uživatele e-mailové schránky jednak e-mailová komunikace budoucí, tak i ta, co již proběhla a nachází se nadále ještě v e-mailové schránce. Tudíž je namístě se zabývat aplikovatelností jednak § 88 tr. ř. upravujícího odposlech a záznam telekomunikačního provozu, použitelný však jen ohledně trestných činů uvedených v § 88 odst. 1 tr. ř., a jednak § 158d tr. ř. upravujícího sledování osob a věcí.

Sledování osob a věcí je přitom operativně pátrací prostředek podle platné právní úpravy použitelný v trestním řízení o kterémkoli úmyslném trestném činu, který se ve shodě s odposlechem a záznamem telekomunikačního provozu realizuje utajovaným způsobem. Ze znění § 158d odst. 9 tr. ř. lze dovozovat jeho přípustnost i ohledně elektronických komunikací.²⁰

Každá z těchto v úvahu přicházejících forem zjišťování obsahu e-mailové komunikace má pak i odlišný proces realizace po stránce technické (z hlediska potřeby a formy součinnosti od poskytovatele služby).

Ke zjišťování e-mailové komunikace přitom doposud neexistuje žádná publikovaná judikatura. Dílem s danou problematikou souvisí pouze usnesení Ústavního soudu ČR ze dne 3. 10. 2013 sp. zn. III. ÚS 3812/2012, na které lze brát v rámci aplikační praxe zřetel. V rámci něho byl konkrétně vysloven právní názor, že pořízení otisku elektronických dat lze povolit postupem podle § 158d odst. 3 tr. ř., pokud jde o data na sledovaných počítačích již uložená, nikoli o data telekomunikačního provozu. Z dikce § 158d tr. ř., kterým je zákonem upraveno sledování osob a věcí za účelem získání poznatků o osobách a věcech prováděné utajovaným způsobem nebo jinými prostředky, podle Ústavního soudu ČR jasně vyplývá, že v rámci tohoto úkonu lze pořizovat záznamy nejružnějšího druhu a se souhlasem soudce může být v přiměřené míře zasahováno do práva na soukromí dotčených osob. Z hlediska ústavněprávní kontroly bylo v předmětné trestní věci podstatné, že byl jasně specifikován okruh sledovaných počítačů. Přičemž v rámci sledování elektronických zařízení z povahy věci plyne, že předmětem sledování budou právě data na těchto zařízeních uložená, jejichž otisk lze podřadit za využití utajené operativně pátrací techniky.

V intencích citovaného rozhodnutí Ústavního soudu ČR lze připustit možnost povolení sledování osob a věcí soudem podle § 158d odst. 1, 3 tr. ř. ke zjištění aktuálního stavu e-mailové schránky, tj. v ní uložených dat v rozsahu specifikovaném v soudním rozhodnutí, neboť je lze považovat za jiné záznamy uchovávané v soukromí za použití technických prostředků.

E-mailovou schránku je namístě považovat za soukromý prostor srovnatelný s každým jiným prostorem, ohledně kterého lze podle § 158d odst. 3 tr. ř. povolit sledování osob a věcí ve formě tzv. prostorového odposlechu. Zjištění aktuálního stavu e-mailové schránky, tj. v ní uložených

²⁰ Podle § 158d odst. 9 tr. ř. jsou provozovatelé telekomunikační činnosti, jejich zaměstnanci a jiné osoby, které se na provozování telekomunikační služby podílejí, jakož i pošta nebo osoba provádějící dopravu zásilek, povinny bezúplatně poskytovat policejnímu orgánu provádějícímu sledování podle jeho pokynů nezbytnou součinnost. Přitom se nelze dovolávat povinnosti mlčenlivosti stanovené zvláštními zákony.

dat, se přitom z povahy tohoto operativně pátracího úkonu přípustného na základě soudního povolení k prolomení ústavně zaručených práv mj. na ochranu záznamů uchovávaných v soukromí, může vztahovat nejen na v e-mailové schránce se aktuálně nacházející zprávy odeslané, ale i (nikoli trvale) odstraněné, rozepsané a přijaté (doručené), včetně těch, které si příjemce doposud nepřčetl, pokud tuto možnost objektivně měl (mohl se do e-mailové schránky přihlásit a učinit rozhodnutí, zda doručenou zprávu si v ní uchová nebo ji trvale odstraní). Pokud nikoli, např. z důvodu jeho zadržení, pobytu ve vazbě nebo ve výkonu trestu odnětí svobody, jednalo by se zde o stejnou právní situaci jako v případě elektronické komunikace, která se uskuteční po zajištění mobilního telefonu nebo jiného datového nosiče. Tudíž podle platné právní úvahy by obsah takové zprávy bylo možno dodatečně zjistit jen na základě souhlasu soudce podle § 8 odst. 5 tr. ř. I zde je však nutné upozornit, že nelze dopředu předjímat rozhodovací praxi soudů.

Odesílání a přijímání e-mailových zpráv je stejně jako telekomunikační provoz jednou z forem elektronické komunikace. Odposlech a záznam telekomunikačního provozu je přitom při splnění podmínek subsidiarity a přiměřenosti (naplnění zásady proporcionality) ve smyslu § 2 odst. 4 tr. ř. možný jen na základě soudního příkazu podle § 88 odst. 1 tr. ř. po dobu v něm stanovenou a navíc jen ohledně v § 88 odst. 1 tr. ř. uvedených trestných činů. I s přihlédnutím k výše citovanému obsahu usnesení Ústavního soudu ČR, kterým je nepřímě připomenut specifický charakter telekomunikačního provozu, nelze v zájmu předejití obcházení účelu zákona, konkrétně § 88 odst. 1 tr. ř., podle platné právní úpravy ani budoucí e-mailovou elektronickou komunikaci zjišťovat jinak, než na základě soudního příkazu podle § 88 odst. 1 tr. ř.

Příloha k výkladovému stanovisku:

Zjištění obsahu datového nosiče (mobilní telefon, tablet či jiná výpočetní technika)

A. Zjištění obsahu údajů nacházejících se v zajištěném datovém nosiči v době jeho zajištění orgány činnými v trestním řízení

I. Ke zjištění obsahu údajů nacházejících se v zajištěném (např. podle § 78, § 79, § 82 a násl., § 113 tr. ř.) datovém nosiči v době jeho zajištění orgány činnými v trestním řízení není třeba příkazu soudce podle § 88 tr. ř.

B. Zjištění obsahu údajů doručených na zajištěný datový nosič v době po jeho zajištění orgány činnými v trestním řízení (tzn. on-line)

I. Ke zjištění obsahu údajů doručených na zajištěný datový nosič v době po jeho zajištění orgány činnými v trestním řízení, je třeba po zajištění datového nosiče příkazu soudce podle § 88 tr. ř. (pokud již předmětný příkaz nebyl vydán před zajištěním datového nosiče a doba jeho platnosti stále trvá)

II. Zpětné zjištění obsahu údajů doručených na zajištěný datový nosič v době po jeho zajištění postupem je podle ustanovení § 88a tr. ř. vyloučeno

Zjištění obsahu e-mailových schránek, resp. e-mailové elektronické komunikace

A. Budoucí e-mailová komunikace (on-line)

I. Ke zjištění obsahu budoucí e-mailové elektronické komunikace (on-line) je třeba soudního příkazu podle § 88 odst. 1 tr. ř.

B. Zjištění obsahu e-mailové elektronické komunikace v zajištěném datovém nosiči uskutečněné do doby jeho zajištění orgány činnými v trestním řízení

I. Ke zjištění obsahu elektronické komunikace v zajištěném (např. podle § 78, § 79, § 82 a násl., § 113 tr. ř.) datovém nosiči uskutečněné do doby jeho zajištění orgány činnými v trestním řízení není třeba příkazu soudce podle § 88 tr. ř.

C. Zjištění obsahu e-mailové elektronické komunikace v zajištěném datovém nosiči uskutečněné v době po jeho zajištění orgány činnými v trestním řízení (tzn. on-line)

I. Ke zjištění obsahu e-mailové elektronické komunikace uskutečněné v době po zajištění datového nosiče orgánem činným v trestním řízení je třeba příkazu soudce podle § 88 tr. ř. (pokud již předmětný příkaz nebyl vydán před zajištěním datového nosiče a doba jeho platnosti stále trvá)

II. Postup podle § 88a tr. ř. je vyloučen

D. Zjištění obsahu již uskutečněné e-mailové komunikace, tj. v e-mailové schránce uložených dat

I. Ke zjištění aktuálního obsahu e-mailové schránky v konkrétní e-mailové schránce lze připustit možnost povolení sledování osob a věcí soudem podle § 158d odst. 1, 3 tr. ř.

Citované výkladové stanovisko není aplikační praxí přijímáno jednoznačně.

Je konstatována jen doporučující povaha stanovisek vydaných podle § 12 odst. 2 zákona o státním zastupitelství i pro státní zástupce.²¹

Zde se naznačuje zásadně odlišné stanovisko vůči výkladovému stanovisku č. 1/2015 Sb. v. s. NSZ, tam vyslovený názor je možno vykládat za velice přesvědčivý.

V podstatě jde o analogickou aplikaci ještě § 88 odst. 1 tr. ř.

Otázkou tedy je, jak daný aplikační problém vyřešit, zda v duchu výkladového stanoviska č. 1/2015 Sb. v. s. NSZ, nebo v duchu právního názoru Městského soudu v Praze. Pro každé pojetí lze nepochybně snést řadu argumentů.

V této souvislosti lze ocitovat rozhodnutí Nejvyššího soudu sp. zn. 7 Tz 9/2000-I. (ASPI) k problematice ochrany tajemství zpráv dopravovaných v telekomunikačním provozu.

I. S ohledem na znění § 78 odst. 2 tr. ř. nelze k prolomení ochrany tajemství zpráv přepravovaných v poštovním nebo telekomunikačním provozu v době, kdy jsou přepravovány k jejich adresátovi vystačit s aplikací institutů vydání a odnětí věci. Pro zjištění obsahu těchto zpráv je nezbytné použít postup předpokládaný § 86, § 87 a § 88 tr. ř.²²

II. V případě, že zpráva již příjemci byla předána – je v jeho dispozici, zvýšená ochrana, kterou požívala v průběhu přepravy, končí. Je pouze na příjemci zprávy, jak s ní naloží. To platí jak pro listovní zásilky, tak pro zprávy, jejichž obsah je zachycen na záznamovém zařízení hmotného nosiče zprávy, např. mobilního telefonu.

III. Hmotné nosiče zpráv mohou být věci důležitou pro trestní řízení, a tedy listinným či věcným důkazem. Vzhledem k tomu, že osoba, která je má v této etapě u sebe nemá ve vztahu k jejich obsahu povinnost mlčenlivosti, nic nebrání aplikaci postupu podle ustanovení § 78 a § 79 tr. ř., které jsou dostatečným zákonným podkladem předpokládaným čl. 13 Listiny základních práv a svobod pro prolomení ochrany tajemství takových zpráv, pokud jsou uchovávány v soukromí.

Základní rozdíl mezi ustanoveními § 88 tr. ř. o odposlechu a záznamu telekomunikačního provozu (elektronické komunikace) a § 88a tr. ř. o zjišťování údajů o uskutečněném telekomunikačním provozu (elektronické komunikace) je v tom, že § 88 směřuje do budoucna, zatímco § 88a tr. ř. se týká již uskutečněného telekomunikačního provozu (elektronické komunikace). Podle toho je třeba v konkrétním případě použít příslušný příkaz, a to buď k odposlechu a zá-

²¹ Zákon č. 283/1993 Sb., o státním zastupitelství, až do novely provedené zákonem č. 14/2002 Sb., která nabyla účinnosti dne 1. 3. 2002, neobsahoval v tomto směru žádnou výslovnou úpravu. Přesto Nejvyšší státní zastupitelství vydávalo ke sjednocení praxe uplatňování norem trestního práva hmotného i procesního (případně i netrestních norem) výkladová stanoviska.

Novela zákona o státním zastupitelství provedená zákonem č. 14/2002 Sb. v nově formulovaném ustanovení § 12 odst. 2 upravila oprávnění nejvyššího státního zástupce vydávat pro státní zastupitelství stanoviska ke sjednocení výkladu zákonů a jiných právních předpisů při výkonu působnosti státního zastupitelství.

²² Tehdy ještě neexistoval v platné úpravě institut zjišťování údajů z telekomunikačního provozu podle § 88a tr. ř.

znamu telekomunikačního provozu podle § 88 odst. 1, 2 tr. ř. či nařízení k odposlechu a záznamu telekomunikačního provozu podle § 88 odst. 5 (se souhlasem uživatele odposlouchávané stanice), anebo k zjištění údajů o uskutečněném telekomunikačním provozu podle § 88a odst. 1, resp. § 88a odst. 4 (se souhlasem uživatele telekomunikačního zařízení). Tzv. vedlejšími údaji (volající a volané číslo, použitá služba, datum, čas, doba trvání komunikace a místo připojení, připojení základových stanic zajišťujících hovor v případě mobilních telefonů) není obsah zpráv přepravovaných nebo jinak zprostředkovaných telekomunikačními zařízeními, k jejich zjišťování je vyhrazen odposlech a záznam telekomunikačního provozu (§ 88 tr. ř.).²³

Provozními a lokalizačními údaji jsou zejména údaje vedoucí k dohledání a identifikaci zdroje a adresáta komunikace a dále údaje vedoucí ke zjištění data, času, způsobu a doby trvání komunikace. Rozsah provozních a lokalizačních údajů uchovávaných, formu a způsob jejich předávání orgánům oprávněným k využívání podle zvláštního právního předpisu a způsob jejich likvidace stanoví prováděcí právní předpis.

Podnikatelé zajišťující veřejné komunikační sítě nebo poskytující veřejně dostupné služby elektronických komunikací jsou povinni zajistit technicky a organizačně důvěrnost zpráv a s nimi spojených provozních a lokalizačních údajů, které se přenášejí prostřednictvím jejich veřejné komunikační sítě a veřejně dostupných služeb elektronických komunikací. Zejména nepřipustí odposlech, ukládání zpráv nebo jiné druhy zachycení nebo sledování zpráv a s nimi spojených údajů osobami jinými, než jsou uživatelé, bez souhlasu dotčených uživatelů, pokud zákon nestanoví jinak. To nebrání technickému ukládání údajů, které je nezbytné pro přenos zpráv, aniž by byla dotčena zásada důvěrnosti (§ 89 odst. 1 zákona č. 127/2005 Sb.).

Provozními údaji se rozumí jakékoli údaje zpracovávané pro potřeby přenosu zprávy sítě elektronických komunikací nebo pro její účtování.

Lokalizačními údaji se rozumí jakékoli údaje zpracovávané v síti elektronických komunikací nebo službou elektronických komunikací, které určují zeměpisnou polohu telekomunikačního koncového zařízení uživatele veřejně dostupné služby elektronických komunikací (srov. § 91 odst. 1 zákona č. 127/2005 Sb.).

A znovu již citovaný § 136 odst. 20 písm. b) zákona č. 127/2005 Sb. o elektronických komunikacích [přechodná ustanovení]: Obsahuje-li zvláštní právní předpis ustanovení o telekomunikačním provozu, rozumí se tím přenášená zpráva podle tohoto zákona, údajích o telekomunikačním provozu, rozumí se tím provozní a lokalizační údaje související s přenášenou zprávou podle tohoto zákona, telekomunikační službě, rozumí se tím služba elektronických komunikací podle tohoto zákona, telekomunikační síti, rozumí se tím síť elektronických komunikací podle tohoto zákona.

Znovu se vracíme k e-mailové komunikaci. Lze odmítnout zcela jako možný postup podle § 8 odst. 1 věty první tr. ř. Tato úprava zde k prolomení tajemství elektronických komunikací nepostačuje. Použitelnost § 8 odst. 5 tr. ř. by byla dána, pokud by žádný právní předpis neupravoval prolomení tajemství elektronických komunikací pro účely trestního řízení (tak tomu zřejmě bude právě v případech uvedených v zákoně č. 480/2004 Sb.).

Je třeba zásadně oddělovat údaje o (uskutečněném) telekomunikačním provozu (provozu elektronických komunikací) a obsah takového provozu.

Vztah mezi odposlechem, zjišťováním údajů a sledováním osob a věcí lze vymezit následovně:

²³ Srov. Šámal, P., Musil, J., Kuchta, J. Trestní právo procesní. Praha: C. H. Beck, 2013, 4. přepracované vydání, s. 330.

Tyto tři druhy úkonů vykazují řadu společných rysů – jde vždy o získání skutečností důležitých pro trestní řízení, jejich získání by bylo nemožné nebo podstatně ztížené. Alespoň první dva úkony by měly být upraveny ne jako úkony týkající se zajištění věcí, ale spíše se jedná o získání informací, procesní úprava v trestním řádu není přesná, proto se někdy hovoří o tzv. e-důkazech, čili elektronických důkazech. Přicházela by tedy v úvahu i samostatná úprava spolu se sledovanou zásilkou, popř. v rámci dokazování nebo společně s operativně pátracími prostředky (které ale také nejsou v trestním řádu systematicky zařazeny správně). Její součástí by nepochybně byl i institut uchování a ochrany dat a prohlídka a vydání dat a znemožnění přístupu k nim.

Ve všech případech se počítá s použitím technických prostředků; úkony jsou prováděny utajeně. V případě sledování osob a věcí je zasahování do telekomunikačního tajemství jednou s možností sledování. Ve všech případech také mají uloženy právnícké a fyzické osoby, které vykonávají telekomunikační činnost, uloženy určité součinnostní povinnosti na vlastní náklady (vůči orgánům činným v trestním řízení).

Ve všech případech je třeba písemného povolení, příkazu či nařízení (rozhodnutí „svého druhu“), jež ve všech případech vydává soudce [v případě uvedeném v § 158d odst. 3 tr. ř., pokud jde o sledování osob a věcí]. Osoba, do jejíž práv a svobod má být úkonem zasahováno [nikoli předpokládaný pachatel], může k provedení úkonu dát výslovný souhlas (§ 88 odst. 5, § 88a odst. 4 a § 158d odst. 6 tr. ř.).

Komunikace mezi obviněným s obhájcem [nikoli však analogicky v jiných případech, tj. např. v případě vztahu mezi osobou a jejím právním zástupcem] podléhá ve všech případech zvláštní ochraně a úkon je třeba ihned ukončit, záznam zničit, poznatky z nich vyplývající nelze v dalším řízení nikterak použít.

Záznamy se dají za stanovených podmínek využít jako důkaz (§ 88 odst. 6, § 88a odst. 4, § 158d odst. 6 tr. ř.).

Odposlech a záznam provozu elektronických komunikací, pokud jej takto nazveme (či použijeme termínu „elektronická zpráva“) je výhradní úkon, který je určen pro zjišťování obsahu přepravovaných a zprostředkovaných zpráv, jež jsou předmětem telekomunikačního tajemství, resp. tajemství provozu elektronických komunikací (pokud lze vůbec tímto úkonem obsah těchto zpráv zjišťovat).

Zjišťování údajů z telekomunikačního provozu se týká oněch „vedlejších“, „doprovodných“ údajů, zásadně však nikoli obsahu.

Podstatný rozdíl je ve zmírněných podmínkách úkonu podle § 158d odst. 3 tr. ř., kde je to však dáno spíše tím, že se ještě nestačila přijmout příslušná právní úprava.²⁴

Odposlech a záznam a sledování mají společné to, že jejich provádění probíhá směrem od současnosti do budoucnosti (e-mailové zprávy ovšem mohou podléhat i sledování v čase, jakkoli se to jeví sporné), zjišťování údajů směrem od současnosti do minulosti.

Úkony podle § 88 a § 88a tr. ř. jsou zajišťovací, kdežto úkon podle § 158d tr. ř. operativně pátracím prostředkem; to je však dáno platnou právní úpravou a nevhodným systematickým zařazením po novelách (předběžná opatření byla také nevhodně umístěna za § 88a tr. ř., ač patří zjevně před vazbu). Takových zřejmých nelogičností je však v trestním řádu více.

²⁴ V případě tzv. bytových odposlechů je to otázka velmi krátké doby. Pochybnosti se týkají úprava fakticky „bytového odposlechu“, kde ač se jedná o zásah do dvou ústavně zaručených práv (na ochranu soukromí podle čl. 10 odst. 2 Listiny a nedotknutelnosti obydlí podle čl. 12 Listiny základních práv a svobod), a lze důvodně očekávat, že při něm budou pod dojmem „bezpečí domova“ sděleny mnohdy intimnější a závažnější informace než při telekomunikačním provozu, jsou pravidla pro zásah v § 158d tr. ř. nastavena výrazně mírněji.

Důležité je konstatování citované učebnice trestního práva procesního,²⁵ o kterém však lze nepochybně diskutovat, že „...zajišťovací úkony podle § 88 a § 88a tr. ř. jsou vůči operativně pátracímu prostředku podle § 158d tr. ř. v poměru speciality“.

Velice významné je i to, že v případech sledování, při kterém bude věnována pozornost určité osobě a věci při jejich pohybu a jednání směrem do budoucnosti s předem neznámým výsledkem výskytu poznatků a jejich charakteru, bude nutno, v okamžiku, kdy vznikne podnět k provedení některého ze zajišťovacích úkonů, tento úkon bude potřebný a pro jeho provedení budou splněny všechny zákonné podmínky, rozhodnout o nařízení odposlechu a záznamu nebo o zjišťování údajů z telekomunikačního provozu. Za těchto předpokladů účelu těchto úkonů pokračováním ve sledování osob a věci nelze. Sledování však nemusí být jako celek ukončeno, může v zákonných mezích dále pokračovat.²⁶

Sledování se zásadně povoluje do budoucnosti, i kdyby se týkalo komunikace, která probíhala v minulosti.²⁷

Kacířská poznámka „do vlastních řad“ a „jakoby v neprospěch výkladového stanoviska č. 1/2015 Sb. v. s. NSZ“:

De lege ferenda bude na místě podrobnější úprava, jež by vzala v úvahu, že byť se jedná o operativně pátrací prostředky, při kterých se může jednat o prověřování vzdáleného prvotního podezření (ale proč se tedy přenášely ze zákona o policii do trestního řádu?), vyžadují alespoň některé zásahy přísnější regulaci a kontrolu (možná obdobnou jako u použití agenta), přinejmenším ze strany státního zástupce, lze však očekávat, že to skončí povolovacím režimem ze strany soudu a za obdobných podmínek jako u úkonů podle § 88 a § 88a tr. ř. (kterážto úprava je však v Evropě unikátní

Tyto úkony mohou zasáhnout i osoby, jichž se vůbec podezření ze spáchání trestného činu netýká – to je otázka nastavení zásady zdrženlivosti a přiměřenosti (§ 2 odst. 4 tr. ř.). Mělo by tedy zde být omezení obdobné jako u úkonů uvedených v § 88 a § 88a tr. ř., následné neprodlené informování dotčených osob nejpozději poté, co odpadnou obavy z vyzrazení výsledků úkonu a zmaření trestního řízení, a o průběžné informování státního zástupce o průběhu a výsledcích úkonu, aby bylo možno rozhodnout o okamžitém ukončení v odůvodněných případech. Úprava úkonů podle § 88, § 88a a § 158d tr. ř. by měla být sjednocena.

Domnívám se však, že sice chápu nevyvážený a neproporcionální vztah mezi úpravou v dotčených ustanoveních, opravdu ale platí, že aktuální obsah e-mailové schránky je určován vůli uživatele a lze jej zjišťovat postupem podle § 158d odst. 3 tr. ř., který je možno považovat za zákonnou licenci prolamující ústavně zaručené právo na ochranu soukromí v e-mailové schránce se nacházejících záznamů, a to podle platné právní úpravy v případě trestního řízení pro kterýkoli úmyslný trestný čin. Nedostatek platné právní úpravy neshledávám ústavně nekonformním (jinak by bylo nutno trestní stíhání přerušit a věc předložit Ústavnímu soudu, což přichází v úvahu i per analogiam, jeví se to však v těchto poměrně urgentních případech jen těžko představitelné). Nelze jej podle mne řešit cestou kombinace obou procesních postupů (§ 88a trestního řádu zde použít nelze), tedy podle § 158d odst. 3 tr. ř. a analogií § 88 odst. 1 tr. ř. Analogii nelze použít, pokud výslovná právní úprava existuje. Nahrazovat nedostatky právní úpravy tímto postupem není možné. Úprava v § 8 odst. 5 tr. ř. zde je nepoužitelná (jakkoli by se mohlo jevit, že by to bylo optimální řešení problému, ač tento postup je možný prakticky u podezření z jakéhokoli trestného činu, je zde však široký prostor pro úvahu soudce, jak je na tom založeno

²⁵ Tamtéž, s. 332.

²⁶ Tamtéž, s. 332–333.

²⁷ Podle § 158d odst. 3 tr. ř.: „Pokud má být sledováním zasahováno do nedotknutelnosti obydlí, do listovního tajemství nebo zjišťován obsah jiných písemností a záznamů uchovávaných v soukromí...“

stanovisko trestního kolegia NS ČR sp. zn. Tpjn 303/2005 ze dne 28. 6. 2006 citované výše). Zjišťování e-mailové komunikace v reálném čase je možné zásadně jen postupem podle § 88 odst. 1 tr. ř., neboť se stejně jako telekomunikační provoz uskutečňuje rovněž v síti elektronických komunikací. Postup podle § 88a tr. ř. není v takovém případě možný.

IV. Závěr

Jak je vidět, jde tu o velice komplikovanou problematiku. Stále přetrvává obava z legislativního řešení, protože to by nakonec mohlo vést k omezení nástrojů k eliminaci trestné činnosti a k dokazování. Často se objevují výhrady, že se odposlechů (i ostatních institutů) nadužívá, pokud se však podíváme na reálnou účinnost těchto úkonů, zjistíme, že není zdaleka zanedbatelná.²⁸ Je však zjevné, že definitivní řešení poskytne až připravovaná rekodifikace trestního práva procesního.

²⁸ To ostatně dokumentovaly i zvláštní zprávy zmíněné v bodě II., i zprávy o činnosti, a velmi podrobně to dokladují analýzy policejní i Generální inspekce bezpečnostních sborů.

Možnosti a limity využití informačně-technických prostředků při vyšetřování kybernetické kriminality

Possibilities and Limits of Using Information-technical Means in the Investigation of Cyber Crime

Vladimír Smejkal¹

Viktor Porada²

Abstrakt: Příspěvek se zabývá problematikou informačně-technických prostředků, postupů a operací používaných orgány činnými v trestním řízení za účelem sledování osob a věcí, monitorování obsahu elektronické komunikace a zjišťování provozních a lokalizačních údajů ze sítí a služeb elektronických komunikací v prostředí kyberprostoru vzhledem ke zvláštnímu charakteru dat v zařízeních informační a komunikační techniky (ICT).

Abstract: The paper deals with the issue of information-technical means, procedures and operations used by law enforcement authorities to track people and objects, monitor the content of electronic communications and ascertain of traffic and location data of electronic communications networks and services in the area of cyberspace because of the special nature of the data in the facilities of the information and communication technology (ICT).

Klíčová slova: informačně-technické prostředky, operativně pátrací prostředky, informační a komunikační technologie, kybernetická kriminalita, kyberprostor, orgány činné v trestním řízení, policie, zpravodajské služby, zákon o kybernetické bezpečnosti.

Key words: information and technical resources, operatively-search resources, information and communications technology, cybercrime, cyberspace, law enforcement authorities, police, intelligence service, law on cyber security.

Definice informačně-technických prostředků

Existuje zásadní rozdíl mezi Českou a Slovenskou republikou. V roce 2003 byl v SR přijat zákon č. 166/2003 Z. z., o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním), nyní ve znění ve znění pozdějších předpisů. Tento zákon definuje informačně-technické prostředky (dále také jen „ITP“) příkladným výčtem v ust. § 2 odst. 1:

„Informačno-technickými prostriedkami na účely tohto zákona sú najmä elektrotechnické, rádiodiotechnické, fototechnické, optické, mechanické, chemické a iné prostriedky a zariadenia alebo ich súbory používané utajeným spôsobom na

- a) vyhľadávanie, otváranie, skúmanie a vyhodnocovanie poštových zásielok a iných dopravovaných zásielok,
- b) získavanie obsahu správ prenášaných prostredníctvom elektronických komunikačných sietí vrátane odpočúvania telefónnej komunikácie,
- c) vyhotovovanie obrazových, zvukových, obrazovo-zvukových alebo iných záznamov.“

¹ Prof. Ing. Vladimír Smejkal, CSc., LL.M., Moravská vysoká škola Olomouc, e-mail: vladimir.smejkal@mvso.cz.

² Prof. JUDr. Ing. Viktor Porada, DrSc., Vysoká škola finanční a správní, Praha, e-mail: viktor.porada@mail.vsfz.cz.

Z obecné a široké definice elektronických komunikačních sítí v ust. § 2 odst. 1 zákona č. 351/2011 Z. z. o elektronických komunikacích, ve znění pozdějších předpisů³ vyplývá, že získávání obsahu zpráv lze pomocí ITP provádět v jakýchkoliv typech sítí – interních (typu LAN), externích (WAN), případně veřejných (Internet). K diskusi nicméně je, zda se definice vztahuje i na monitorování činností počítače uvnitř něj (např. nahráním nějakého software) nebo na snímání elektromagnetického vyzařování z takového přístroje).

Další technická podmínka, kterou zákon ukládá ve vztahu k vlastnostem ITP, pak zní: „*Pri odpočúvaní a zaznamenávaní telekomunikačnej služby sa môže použiť len taký informačno-technický prostriedok, ktorý umožní okamžite identifikovať koncové telekomunikačné zariadenie, ktoré bolo použité na odpočúvanie a zaznamenávanie telekomunikačnej služby, ktorý neumožní vymazanie údajov identifikujúcich toto zariadenie a ktorý neumožňuje vymazanie času odpočúvania a zaznamenávania telekomunikačnej služby.*“.

V České republice takovou právní úpravu nenajdeme a musíme vycházet z definic nacházejících se v „tradičních“ právních předpisech upravujících trestní řízení, činnost policie a zpravodajských služeb atd. Podle nich můžeme rozlišovat:

1. **Operativně pátrací prostředky**, které obecně řečeno jsou definované jako souhrn opatření policejních orgánů uskutečňovaných podle trestního řádu a v souladu s dalšími právními předpisy, jejichž účelem je předcházení, odhalování a objasňování trestné činnosti, jakož i pátrání po skrývajících se pachatelích, pátrání po hledaných nezvěstných osobách a pátrání po věcných důkazech.⁴ Jsou popsány v ust. § 158b až § 158f tr. řádu ČR⁵ (a dále pak ve speciálních ust. § 88 a § 88a – viz dále), přičemž o použití ITP se bude jednat zejména v případě činnosti podle ust. § 158d – **Sledování osob a věcí**, čímž se rozumí „získávání poznatků o osobách a věcech prováděné utajovaným způsobem technickými nebo jinými prostředky“. Odst. 2 předpokládá, že bude docházet mj. i k zasahování do nedotknutelnosti obydlí, do listovního tajemství nebo k zjišťování obsahu jiných písemností a záznamů uchovávaných v soukromí za použití technických prostředků. Nebude se týkat získávání poznatků souvisejících s přenosem zpráv, a to bez ohledu na dikci odst. 9 „*Provozovatelé telekomunikační činnosti, jejich zaměstnanci a jiné osoby, které se na provozování telekomunikační činnosti podílejí, jakož i pošta nebo osoba provádějící dopravu zásilek jsou povinny bezúplatně poskytovat policejnímu orgánu provádějícímu sledování podle jeho pokynů nezbytnou součinnost.*“. K tomu slouží zmíněné § 88 a § 88a. Konečně podle § 158b odst. 3 *Zvukové, obrazové a jiné záznamy získané při použití operativně pátracích prostředků způsobem odpovídajícím ustanovením tohoto zákona lze použít jako důkaz.*

Z výše uvedeného lze dovodit, že se jedná tedy o použití různých nástrojů z kategorie ITP, jako jsou odposlechy, získávání obrazových a zvukových záznamů o činnosti sledovaných osob, zařízení ke zjišťování obsahu korespondence a jiných písemností uchovávaných v soukromí, monitorování telekomunikační činnosti apod.

³ Elektronická komunikačná sieť je funkčne prepojená sústava prenosových systémov, a ak je to potrebné, prepájaných alebo smerovacích zariadení, vrátane sieťových prvkov, ktoré nie sú aktívne, ktoré umožňujú prenos signálov po vedení, rádiovými, optickými alebo inými elektromagnetickými prostriedkami, vrátane družicových sietí, pevných sietí s prepájaním okruhov a s prepájaním paketov, internetu a mobilných pozemských sietí, sietí na rozvod elektrickej energie v rozsahu, v ktorom sa používajú na prenos signálov, sietí pre rozhlasové a televízne vysielanie a káblových distribučných systémov bez ohľadu na druh prenášaných informácií.

⁴ ŠÁMAL, P., NOVOTNÝ, F., RŮŽIČKA, M., VONDRUŠKA, F., NOVOTNÁ, J. *Přípravné řízení trestní*. 2. podstatně přepracované vydání, Praha: C. H. Beck, 2003, s. 247.

⁵ Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.

Činnosti prováděné podle ust. § 158b až § 158f tr. řádu jsou předmětem jak rozsáhlé judikatury,⁶ tak odborných diskusí. Z našeho pohledu jde především o získávání informací ze zařízení výpočetní a komunikační techniky (dále jen „ICT“), čímž se budeme zabývat dále.

Zvláštním případem činností patřících do této kategorie prostředků je **odposlech a záznam telekomunikačního provozu** podle ust. § 88 – § 88a trestního řádu ČR. Odposlech a záznam telekomunikačního provozu podle § 88 přichází v úvahu pro vybrané trestné činy uvedené v odst. 1 a 5.

Ve všech citovaných ustanoveních s pracuje s termíny „telekomunikační provoz“ a „telekomunikační činnosti“. Je otázkou, zda můžeme dát rovnítko mezi telekomunikační službou a službou elektronických komunikací podle platného zákona o elektronických komunikacích. Podle § 2 odst. 7 zákona č. 151/2000 Sb., o telekomunikacích a o změně dalších zákonů, ve znění pozdějších předpisů se telekomunikační službou rozumí „*služba, jejíž poskytování spočívá zcela nebo zčásti v přepravě nebo směřování informací telekomunikačními sítěmi třetím osobám. Touto službou je i pronájem telekomunikačních okruhů*“. Podle současného zákona č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů, § 2 písm. n) se službou elektronických komunikací rozumí „*služba obvykle poskytovaná za úplatu, která spočívá zcela nebo převážně v přenosu signálů po sítích elektronických komunikací, včetně telekomunikačních služeb a přenosových služeb v sítích používaných pro rozhlasové a televizní vysílání a v sítích kabelové televize, s výjimkou služeb, které nabízejí obsah prostřednictvím sítí a služeb elektronických komunikací nebo vykonávají redakční dohled nad obsahem přenášeným sítěmi a poskytovaným službami elektronických komunikací; nezahrnuje služby informační společnosti, které nespočívají zcela nebo převážně v přenosu signálů po sítích elektronických komunikací*“. Podle názoru autorů ano, protože při monitorování telekomunikační činnosti jde o monitorování přenášených informací, tj. *signálů po sítích elektronických komunikací*, a to bez ohledu na druh a formu služby, kterou jsou tyto informace zpracovány. Dokonce to výslovně říká EKZ v přechodných ustanoveních, kde v § 136 odst. 20 se praví: „*Obsahuje-li zvláštní právní předpis ustanovení o*

- a) telekomunikačním provozu, rozumí se tím přenášena zpráva podle tohoto zákona,*
- b) údajích o telekomunikačním provozu, rozumí se tím provozní a lokalizační údaje související s přenášenou zprávou podle tohoto zákona,*
- c) telekomunikační službě, rozumí se tím služba elektronických komunikací podle tohoto zákona,*
- d) telekomunikační síti, rozumí se tím síť elektronických komunikací podle tohoto zákona.“*

Ust. § 88a se vztahuje na jiné informace, a to **údaje o telekomunikačním provozu**, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat. Jedná se o tzv. provozní a lokalizační údaje – viz níže. Ty je možné zjišťovat kromě jiných trestných činů uvedených v odst. 1 také výslovně v případě trestního řízení vedeného pro trestný čin porušení tajemství dopravovaných zpráv (§ 182 TrZ⁷), pro trestný čin podvodu (§ 209 TrZ), pro trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací (§ 230 TrZ), pro trestný čin opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 TrZ), pro trestný čin nebezpečného vyhrožování (§ 353 TrZ), pro trestný čin nebezpečného pronásledování (§ 354 TrZ), pro trestný čin šíření poplašné zprávy (§ 357 TrZ), pro trestný čin podněcování k trestnému činu (§ 364 TrZ), pro trestný čin schvalování trestného činu (§ 365 TrZ).⁸

⁶ Viz např. nálezy Ústavního soudu ČR sp. zn. II. ÚS 615/06, I. ÚS 3038/07, II. ÚS 2806/08.

⁷ Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů (dále také jen „TrZ“).

⁸ Ke skutkovým podstatám viz SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015. 636 s. ISBN 978-80-7380-501-2.

O jaké údaje se jedná, lze dovodit dnes pouze z dikce EKZ, neboť Soudní dvůr Evropské unie v roce 2014 rozhodl, že směrnice Evropského parlamentu a Rady č. 2006/24/ES, o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí (směrnice o uchovávání údajů), je neplatná.⁹ Národní právní úpravy mezitím přijaté na základě zrušené směrnice ale nebyly tímto dotčeny a staly se většinou předmětem přezkumu příslušnými ústavními soudy jednotlivých zemí EU.

Podle § 97 odst. 3 českého EKZ právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna uchovávat po dobu 6 měsíců provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování jejích veřejných komunikačních sítí a při poskytování jejích veřejně dostupných služeb elektronických komunikací. Jde tedy o plošné monitorování a ukládání dat o všech uživateli, resp. jimi realizovaných spojení. Provozní a lokalizační údaje týkající se neúspěšných pokusů o volání je právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací povinna uchovávat pouze tehdy, jsou-li tyto údaje vytvářeny nebo zpracovávány a zároveň uchovávány nebo zaznamenávány. Současně je tato právnická nebo fyzická osoba povinna zajistit, aby při plnění povinnosti podle věty první a druhé nebyl uchováván obsah zpráv a takto uchovávaný dále předáván. Právnická nebo fyzická osoba, která provozní a lokalizační údaje uchovává, je na požádání povinna je bezodkladně poskytnout:

- a) orgánům činným v trestním řízení pro účely a při splnění podmínek stanovených zvláštním právním předpisem (tr. řádem),
- b) Policii České republiky pro účely zahájeného pátrání po konkrétní hledané nebo pohřešované osobě, zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly, předcházení nebo odhalování konkrétních hrozeb v oblasti terorismu nebo prověřování chráněné osoby a při splnění podmínek stanovených zvláštním právním předpisem (zákonem č. 273/2008 Sb., o Policii České republiky a zákonem č. 137/2001 Sb., o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízením),
- c) Bezpečnostní informační službě pro účely a při splnění podmínek stanovených zvláštním právním předpisem (podle § 6 až 8 zákona č. 154/1994 Sb., o Bezpečnostní informační službě),
- d) Vojenskému zpravodajství pro účely a při splnění podmínek stanovených zvláštním právním předpisem (podle § 9 a 10 zákona č. 289/2005 Sb., o Vojenském zpravodajství),
- e) České národní bance pro účely a při splnění podmínek stanovených zvláštním právním předpisem (zákonem č. 15/1998 Sb., o dohledu v oblasti kapitálového trhu).

Údaje, které měly být předmětem uchovávání podle směrnice č. 2006/24/ES, jsou tzv. provozní údaje a lokalizační údaje a související údaje nezbytné k identifikaci účastníka nebo uživatele podle čl. 2 odst. 2 písm. a) dnes již neplatné směrnice. Klíčový je proto v tomto případě prováděcí právní předpis,¹⁰ který stanoví rozsah provozních a lokalizačních údajů uchovávaných podle odstavce 3, formu a způsob jejich předávání orgánům oprávněným k jejich využívání podle zvláštního právního předpisu a způsob jejich likvidace. Tento rozsah je extrémně široký a lze hovořit o plošném monitorování celého obyvatelstva.¹¹

⁹ Rozsudek Soudního dvora EU ze dne 8. 4. 2014 ve spojených věcech C-293/12 a C-594/12.

¹⁰ Vyhláška č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů.

¹¹ Viz NOVÁK, J. ml. K uchovávání provozních a lokalizačních údajů v České republice ve světle rozhodnutí Soudního dvora Evropské unie. *Bulletin advokacie*, 2015, č. 5, s. 36–41.

Rozsah uchovávání provozních a lokalizačních údajů podle § 2 vyhlášky zahrnuje:

(1) U veřejných telefonních sítí s přepojováním okruhů: a) telefonní číslo volajícího a volaného, telefonní čísla, která se zúčastnila konferenčního volání, identifikátor telefonní karty použité ve veřejném telefonním automatu, b) datum a čas zahájení komunikace, c) délka komunikace, d) datum a čas odeslání textové zprávy SMS, e) použitá telefonní služba podle § 1 písm. m), f) stav komunikace.

(2) U veřejných mobilních telefonních sítí se uchovávají údaje uvedené v odst. 1 s výjimkou identifikátoru telefonní karty. Dále se uchovává a) identifikátor IMSI volajícího a volaného, b) identifikátor mobilního přístroje volajícího a volaného, c) datum a čas odeslání multimediální zprávy MMS, d) označení základnové stanice Start a základnové stanice Stop.¹²

(3) U sítí elektronických komunikací s přepojováním paketů se uchovávají tyto údaje

- a) u služby přístupu k internetu z pevného připojení: 1. typ připojení, 2. telefonní číslo nebo označení uživatele, 3. identifikátor uživatelského účtu, 4. adresa MAC¹³ zařízení uživatele služby, 5. datum a čas zahájení a ukončení připojení k internetu, 6. označení přístupového bodu u bezdrátového připojení k internetu, 7. adresa IP a číslo portu, ze kterých bylo připojení uskutečněno;
- b) u služby přístupu k internetu z mobilního připojení: 1. typ připojení, 2. telefonní číslo uživatele, 3. identifikátor mobilního zařízení, 4. datum a čas zahájení a ukončení připojení k internetu, 5. označení základnové stanice Start a základnové stanice Stop, 6. adresa IP a číslo portu, ze kterých bylo připojení uskutečněno;
- c) u služby přístupu ke schránce elektronické pošty: 1. adresa IP a číslo portu, ze kterých bylo připojení uskutečněno, 2. identifikátor uživatelského účtu, 3. datum a čas zahájení připojení ke schránce elektronické pošty, 4. datum a čas ukončení připojení ke schránce elektronické pošty, 5. identifikátor protokolu elektronické pošty;
- d) u služby přenosu zpráv elektronické pošty: 1. adresa IP a číslo portu zdroje a cíle přenášené zprávy, 2. datum a čas odeslání zprávy, 3. adresa elektronické pošty odesílatele, 4. adresy elektronické pošty příjemců, 5. stav přenosu zprávy, 6. identifikátor protokolu elektronické pošty;
- e) u služby IP telefonie: 1. adresa IP a číslo portu zdrojového zařízení, 2. adresa IP a číslo portu cílového zařízení, 3. transportní protokol, 4. datum a čas zahájení a ukončení komunikace, 5. doplňující údaje uvedené v odstavci 4, nejsou-li k dispozici údaje identifikující volajícího nebo volaného účastníka nebo některý z údajů podle odstavce 5;
- f) u služby přístupu k internetu podle písmene a) nebo b) s překladem adres IP: 1. privátní adresa IP, 2. veřejná adresa IP a číslo portu, nebo přidělený rozsah portů, 3. datum a čas zahájení překladu adres, 4. datum a čas ukončení překladu adres.

(5) U sítí uvedených v odstavcích 1 až 3 se dále uchovává jméno, popřípadě jména a příjmení a adresa účastníka nebo registrovaného uživatele uvedená ve smlouvě nebo adresa umístění telekomunikačního koncového zařízení.

(6) Dále se uchovávají

- a) údaje o všech veřejných telefonních automatech s uvedením jejich telefonního čísla, evidenčního čísla, geografických souřadnic ve Světovém geodetickém referenčním systému 1984 (WGS84) a slovního popisu umístění,

¹² Stanice, kde byl zahájen a kde byl ukončen hovor.

¹³ MAC adresa (Media Access Control) je celosvětově jedinečný identifikátor síťového zařízení, který je přiřazován síťovému zařízení (hardware) bezprostředně při výrobě, proto se jí také někdy říká fyzická adresa. U současných zařízení ji lze ve většině případů softwarově změnit.

- b) údaje o všech základnových stanicích s uvedením jejich označení, popřípadě všech dalších používaných identifikátorů, geografických souřadnic v souřadnicovém systému WGS 84, azimutu směřování antén a slovního popisu umístění,
- c) údaje o vzájemných vazbách mezi telefonními čísly a identifikátory IMSI a identifikátory mobilních zařízení,¹⁴
- d) u předplacených služeb datum a čas aktivace služby a označení základnových stanic, v jejichž dosahu byla aktivace provedena,
- e) údaje o všech přístupových bodech s uvedením jejich označení, popřípadě všech dalších používaných identifikátorů, dále geografických souřadnic v souřadnicovém systému WGS 84, azimutu směřování antén a slovního popisu umístění.

Je třeba nicméně zdůraznit, že uvedené postupy se vztahují na komunikaci veřejnou komunikační sítí nebo prostřednictvím veřejně dostupné služby elektronických komunikací. V některých případech se tedy uvedená ustanovení nepoužijí (soukromé sítě), v některých to bude záležet na přesné specifikaci služby (cloudové služby mohou mít jak soukromý, tak veřejný charakter).¹⁵ Hodnými zvláštního zřetele pak budou situace, kdy bude sledovaná osoba přistupovat do soukromého cloudu prostřednictvím veřejné sítě elektronických komunikací.

K diskusi ještě je, zda zaznamenávání provozních a lokalizačních údajů nepředstavuje stejnou úroveň ohrožení soukromí jako odposlechy. Možnosti automatizovaného zpracování údajů o telekomunikačním provozu, jejich vzájemné propojování a další operace typu „big data“ činí tuto kategorii údajů přinejmenším stejně ohrožující. I toto je zřejmě důvodem, proč SDEU zrušil směrnici 2006/24/ES.

2. Druhá kategorie bývá někdy označována jako **práce s informacemi** nebo **podpůrné operativně pátrací prostředky**, kde zákonná úprava je provedena zákonem č. 273/2008 Sb. o Policii České republiky, a to v ust. § 62 až § 71a, resp. v § 72 až § 77. Práce s informacemi zahrnuje:

- pořizování zvukových, obrazových nebo jiných záznamů osob a věcí nacházejících se na místech veřejně přístupných a zvukových, obrazových nebo jiných záznamů o průběhu úkonu (§ 62),
- získávání informací potřebných ke ztotožnění osoby snímáním daktyloskopických otisků, zjišťováním tělesných znaků, měřením těla, pořizováním obrazových, zvukových a jiných záznamů a odebíráním biologických vzorků umožňujících získání informací o genetickém vybavení (§ 63, § 65),
- získávání informací z evidencí podle § 66 zahrnuje poskytnutí informací z evidence provozované na základě jiného právního předpisu (výčet viz odst. 2), dále pak **poskytnutí provozních a lokalizačních údajů způsobem umožňujícím dálkový a nepřetržitý přístup podle EKZ** (odst. 3, rovněž podle § 68 odst. 2, § 71),
- pro účely zahájeného pátrání po konkrétní hledané nebo pohřešované osobě získávání dat od banky o době a místě použití elektronického platebního prostředku hledané nebo pohřešované osoby a od zdravotní pojišťovny nebo poskytovatele zdravotních služeb poskytnutí informací o době a místě poskytnutí zdravotních služeb této osobě (§ 68 odst. 3, za účelem předcházení a odhalování konkrétních hrozeb v oblasti terorismu podle § 71).

¹⁴ IMSI je International Mobile Subscriber Identity – unikátní číslo přidělené mobilním operátorem pro SIM kartu v mobilní síti. IMSI je mobilním telefonem odesláno mobilnímu operátoru a v interních systémech operátora slouží k dohledání detailů o uživateli. Identifikátorem mobilního zařízení se myslí pravděpodobně IMEI – International Mobile Equipment Identity. Jde o unikátní číslo přidělené výrobcem mobilnímu telefonu. Lze říci, že IMEI identifikuje zařízení, IMSI kartu SIM.

¹⁵ SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015, s. 55 an.

Podpůrné operativně pátrací prostředky zahrnují podle § 76 zabezpečovací techniku, čímž se rozumí technické prostředky, zařízení a jejich soubory používané za účelem předcházení nebo odstranění ohrožení veřejného pořádku a bezpečnosti.

3. Také **zpravodajské prostředky** mají charakter ITP. Podle § 7 – § 8 zákona č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů mezi zpravodajské prostředky patří: a) zpravodajská technika, b) krycí doklady, c) krycí prostředky, d) sledování osob a věcí. Přitom podle § 8 odst. 1 zpravodajskou technikou se pro účely tohoto zákona rozumějí technické prostředky a zařízení, zejména elektronické, fototechnické, chemické, fyzikálně-chemické, radio-technické, optické, mechanické anebo jejich soubory, používané utajovaným způsobem, pokud je jimi zasahováno do základních práv a svobod při

- a) vyhledávání, otevírání, zkoumání nebo vyhodnocování dopravovaných zásilek,
- b) odposlouchávání, popřípadě zaznamenávání telekomunikačního, radiokomunikačního nebo jiného obdobného provozu, popřípadě zjišťování údajů o tomto provozu,
- c) pořizování obrazových, zvukových nebo jiných záznamů,
- d) vyhledávání použití technických prostředků, které by mohly znemožnit nebo znesnadnit plnění úkolů v rámci působnosti Vojenského zpravodajství,
- e) identifikaci osob nebo předmětů, popřípadě při zjišťování jejich pohybu za použití zabezpečovací a nástrahové techniky.

Podle ust. § 9 je Vojenské zpravodajství oprávněno v rozsahu potřebném pro plnění konkrétního úkolu požadovat od právnické nebo fyzické osoby zajišťující veřejnou komunikační síť anebo poskytující veřejně dostupnou službu elektronických komunikací

- a) zřízení, popřípadě zabezpečení rozhraní pro připojení koncového telekomunikačního zařízení pro odposlech nebo záznam zpráv v určených bodech jejich sítě, a
- b) poskytnutí provozních nebo lokalizačních údajů způsobem, ve formě a v rozsahu stanoveném zvláštním právním předpisem (§ 97 EKZ).

K tomu je třeba nicméně uvést, že **podle nálezu Ústavního soudu ČR odposlechů (byť legálně) získaných podle předchozího zákona o Vojenském obranném zpravodajství, nelze použít v trestním řízení jako důkazu**, neboť jsou prováděny v rámci jiného zákonného rámce a nikoli za účelem opatření důkazu v trestním řízení.¹⁶

Identická právní úprava je provedena v ust. § 7, § 8 a § 8a zákona č. 154/1994 Sb., o Bezpečnostní informační službě, ve znění pozdějších předpisů.

Velmi kusá právní úprava v ust. § 17 až § 19 zákona č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů pak poskytuje bez dalšího upřesnění právo Úřadu pro zahraniční styky a informace pro ochranu činností, které koná na území České republiky, a jestliže je to nezbytné pro plnění úkolů v jeho působnosti, používat sledování osob a věcí, krycí doklady, nástrahovou a zabezpečovací techniku a využívat osob jednajících v jeho prospěch. (Využívat služeb osob jednajících ve prospěch zpravodajské služby mohou i výše uvedené služby, tj. Bezpečnostní informační služba a Vojenské zpravodajství). Úřad pro zahraniční styky a informace je oprávněn žádat technické zabezpečení použití sledování osob a věcí a nástrahové a zabezpečovací techniky pro vlastní potřebu i od jiných, k této činnosti oprávněných orgánů.

Co se týká získávání informací, pak podle § 16 odst. 4 zákona o Bezpečnostní informační službě může Bezpečnostní informační služba, stejně jako podle § 20 odst. 2 Vojenské zpravo-

¹⁶ Nález Ústavního soudu ČR sp. zn. I. ÚS 3038/07-1 ze dne 29. 2. 2008.

dajství zákona o Vojenském zpravodajství informace a informační systémy sdružovat a získávat informace pod krytím jiným účelem nebo jinou činností.

Kyberprostor a jeho charakter

Podle českého zákona o kybernetické bezpečnosti¹⁷ (dále také jen „ZKB“) se rozumí kybernetickým prostorem *digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací*. Pojem kybernetického prostoru je podle důvodové zprávy k návrhu ZKB definován jako *informační prostředí k realizaci informačních transakcí, které je vytvořeno technologiemi, jejichž definice a podmínky užívání upravují zvláštní zákony, tj. informačními systémy, službami a sítěmi elektronických komunikací*. Jedná se přitom i o takové informační systémy, služby a síť elektronických komunikací, které nejsou připojeny k veřejné síti, tj. k Internetu.

Jako dostatečně obecná definice kyberprostoru, která je vhodná i pro účely tohoto příspěvku, se jeví tato: *„Kyberprostor je globální a vyvíjející se doména popisovaná užíváním elektrických sítí a elektromagnetického spektra, jejíž smysl je vytvářet, uchovávat, upravovat, vyměňovat, sdílet, vybírat, používat či vymazávat informace. Kyberprostor zahrnuje: a) fyzická i telekomunikační zařízení, která umožňují spojení technologií a komunikaci sítí systému, chápáno obecně (SCADA zařízení, smartphony/tablety, počítače, servery atd.), b) počítačové systémy a komplementární software, který zaručuje spojení a funkčnost systému, c) spojení počítačových sítí, d) uživatelské vstupy a uzly zprostředkovatelů spojení, e) informace – uživatelská data.“*¹⁸

S termínem „kyberprostor“, resp. „kybernetický prostor“ (a „kyberkriminalita“) pracuje i Evropská unie – např. v rámci Europolu bylo počátkem roku 2013 zřízeno Evropské centrum pro boj proti kyberkriminalitě (EC3).¹⁹ Tyto termíny najdeme coby notoriety v řadě dokumentů,²⁰ aniž by nějaká definice mimo intuitivní vnímání, že něco jako kyberprostor existuje,²¹ byla provedena. Objevuje se i omezení na „kybernetický prostor Evropské unie“,²² mohli bychom zřejmě hovořit i o kyberprostoru České nebo Slovenské republiky. Nutno ovšem upozornit že vzhledem k možnosti maskování a falšování údajů o umístění jednotlivých zařízení v síti Internet (zejména IP adres), je teritoriální omezení kyberprostoru dáno spíše množinou ohrožených či

¹⁷ Zákon č. 181/2014 Sb., o kybernetické bezpečnosti.

¹⁸ MAYER, M., MARTINO, L., MAZURIER, P., TZVETKOVA, G. *How would you define Cyberspace?* First Draft Pisa, 19. 5. 2014. Dostupné na https://www.academia.edu/7096442/How_would_you_define_Cyberspace.

¹⁹ Viz <https://www.europol.europa.eu/ec3>.

²⁰ Viz např. Sdělení Komise Evropskému parlamentu a Radě: Druhá zpráva o provádění strategie vnitřní bezpečnosti Evropské unie COM (2013) 0179 ze dne 10. 4. 2013.

²¹ Podle stanoviska Evropského hospodářského a sociálního výboru k návrhu rozhodnutí Evropského parlamentu a Rady o zavedení víceletého programu Společenství pro ochranu dětí využívajících internet a jiné komunikační technologie KOM (2008) 106 v konečném znění 2008/0047 (COD), Úřední věstník (2008/C 224/13) „*Internet není vlastněn ani řízen velkými nadnárodními společnostmi, které by měly kontrolu nad jeho obsahem. Sestává ze stovek milionů stránek provozovaných obrovským množstvím subjektů, a proto je sledování nebo kontrola nedovoleného obsahu obtížná. Jednat je však možné z místní úrovně (domácnosti) směrem na úroveň národní a mezinárodní (včetně kyberprostoru) s cílem omezit dostupnost nedovoleného obsahu prostřednictvím spolupráce mezi všemi zúčastněnými stranami.*“

²² Usnesení Evropského parlamentu ze dne 15. 6. 2010 o řízení internetu: další kroky [2009/2229(INI)]. Úřední věstník (2011/C 236 E/05) nebo Usnesení Evropského parlamentu ze dne 5. 5. 2010 o nové digitální agendě pro Evropu: 2015.eu (2009/2225(INI)), Úřední věstník (2011/C 81 E/08).

napadených zařízení, nežli celou bezpečnostní situací (incidentem). Kyberprostor je dnes chápán i jako (pátá) válečná doména (kromě země, vody, vzduchu a kosmického prostoru).²³

Kyberprostor sestává tedy z různých druhů sítí a v nich připojených zařízení. Základní rozdělení je na lokální síť (Local Area Network, LAN) a vzdálené nebo také rozlehlé síť (Wide Area Network, WAN), přičemž existuje ještě dělení zahrnující síť PAN (Personal Area Network, tj. osobní síť u určitého uživatele, např. v domácnosti), kterou můžeme chápat jako malou síť lokální (LAN), a MAN (Metropolitan Area Network, metropolitní síť), což je síť propojující lokální síť v městské zástavbě a můžeme ji zařadit mezi síť typu WAN. Nutno říci že rozdělení sítí na LAN, MAN, WAN atd. se stává záležitostí spíše akademickou. Technologickým pokrokem došlo do značné míry ke sjednocení použitých technologií a jejich vlastností a hranice mezi osobními, lokálními a rozlehlými sítěmi se stírají.²⁴

Důležitou vlastností kyberprostoru je, že žádná jediná centrální moc nekontroluje všechny síť, které tvoří tuto doménu, tudíž nekontroluje kyberprostor, a to přesto, že je důsledně hierarchicky uspořádán, což je podmínkou jeho funkčnosti.²⁵

Kyberprostor můžeme tedy nějakým způsobem rozčlenit na vrstvu veřejnou (kdokoliv může přistoupit a používat služby, např. na Internetu) a neveřejnou (s omezeným přístupem, soukromou, případně státní). Ještě jednodušeji můžeme rozdělit kyberprostor na „uvnitř“ a „vně“, bez ohledu na to, kudy ono rozhraní (interface) povedeme, a to je to, co nás zajímá z hlediska ITP. Nicméně jak je již uvedeno výše, vzhledem k charakteru kyberprostoru, který je tvořen zjednodušeně řečeno všemi zařízeními, které mají svoji IP adresu, a vztahy, resp. komunikací mezi nimi, prolínání veřejného a soukromého je intenzivní a obtížně oddělitelné.

Je proto vhodné uplatnit systémový přístup, kdy předmět našeho zájmu v kyberprostoru definujeme jako systém, popsáný množinou prvků a vazeb mezi nimi (ve vzájemné interakci), které vykazují jako celek určité vlastnosti, funkce nebo chování.²⁶ Tento systém je obvykle otevřený (má definovány vnější vazby), dynamický (jeho stav se v čase mění), z hlediska technického a programového vybavení deterministický (chování je jednoznačně určeno okamžitým stavem systému a podmínky působících na vstupech), z hlediska interakce s uživateli pak ovšem stochastický (jeho chování může při téže stavu a stejných vstupech vykazovat více alternativních variant chování, a to v závislosti na pravděpodobnostech výskytu těchto variant).

Míra podrobnosti zkoumání je tedy dána systémovým přístupem ke sledování dějů, kdy provedeme dekompozici systému na nejvyšší úrovni za účelem jeho rozkladu na dílčí části, a to podle určitých hledisek a s určitým cílem (zjistit, jaké informace jsou mezi určitými prvky sdělovány, případně identifikovat jednotlivé prvky systému, resp. subsystému). Příkladem budiž komunikace mezi bankou a mezinárodním zúčtovacím střediskem, kde mohou být sledovány transakce vyznačující se určitou charakteristikou, např. pro podezření z praní špinavých peněz. Následně bude provedena dekompozice na obou stranách komunikačních toků za účelem identifikování účtů a jejich majitelů, což se může odehrát jak v rámci banky, tak v rámci na ní napojených prostředků dálkového přístupu klientů. Pokaždé se bude jednat o jiné použití ITP a za jiných podmínek.

²³ BASTL, M., GRUBEROVÁ, Z. Kyberprostor jako „pátá doména“? *Vojenské rozhledy*, 2013, roč. 22 (54), č. 4, s. 10–21.

²⁴ SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015, s. 45 an.

²⁵ CENTRE FOR INTERNATIONAL GOVERNANCE INNOVATION AND THE ROYAL INSTITUTE OF INTERNATIONAL AFFAIRS. *Research Volume Two – Global Commission on Internet Governance. Who Runs the Internet? The Global Multi-stakeholder Model of Internet Governance*. Waterloo, ON, Canada, 2016. Dostupné na <https://www.cigionline.org/sites/default/files/documents/GCIG%20Volume%202.pdf>.

²⁶ Viz BERTALANFFY, L. von. *General System Theory: Foundations, Development, Applications*. New York: George Braziller, 1968, nebo VESELÝ, J. *Systémové nástroje řízení*. Praha: Institut řízení, 1982.

Zvláštní charakter dat v kyberprostoru ve vztahu k oprávněním OČTŘ a zpravodajských služeb

Kdy se dají používat informačně-technické prostředky (ITP)?

- a) obecně pro odhalování a dokazování trestné činnosti,
- b) speciálně pro trestné činy kybernetické.

V obou případech pak jde o získávání informací o obsahu telekomunikačního provozu a o lokalizačních a provozních údajích, jakož i o procesech probíhajících v kyberprostoru, v zařízeních výpočetní a komunikační techniky a v sítích přenášejících data mezi nimi.

Je třeba rozlišit monitorování provozu ICT, které probíhá na základě rozhodnutí správce a provozovatele příslušného systému, které může být sice realizováno na základě požadavků vyplývajících z určitého zákona (ZKB, zákon o bankách, zákon o ochraně osobních údajů, resp. Nařízení GDPR apod.), ale vždy v soukromoprávním režimu. Jde např. o nasazení technických opatření podle ust. § 5 odst. 3 ZKB, písm. f) nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů, g) nástroj pro detekci kybernetických bezpečnostních událostí a písm. h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí.²⁷ V takovém případě nebudeme hovořit o nasazení ITP ve smyslu výše uvedených právních předpisů. Půjde spíše o opatření preventivní.²⁸

V určitý moment se při monitorování procesů v rámci prevence (zajišťování kybernetické bezpečnosti) zjistí, že jde o útok (tr. čin) nebo přípravu k němu a v ten moment by se mělo monitorování procesů změnit v monitorování osob a věcí.

Uvedené nástroje tedy mohou být 1. jedním ze zdrojů informací (podnětů) o připravované nebo spáchané trestné činnosti, 2. stejně jako zdrojem důkazů pro následné vyšetřování. Na základě informací ad 1. může dojít k nasazení ITP, ovšem „spouštěcím mechanismem“ může být stejně jakýkoliv jiný poznatek získaný OČTŘ na základě vlastní činnosti nebo obdrženého oznámení.

Pokud mají být použity ITP pro odhalování a vyšetřování kybernetické kriminality,²⁹ pak je třeba před vlastním zahájením příslušného řízení za účelem povolení k nasazení ITP splnit požadavky, které jsou pregnantně formulovány v řadě nálezů Ústavního soudu ČR, případně ESLP, např. takto: „*Soudní příkaz k odposlechu a záznamu telekomunikačního provozu musí být podle téhož zákonného ustanovení písemný a odůvodněný. Z toho vyplývá, že musí být vydán ve vztahu k určité osobě, proti níž se již trestní stíhání pro uvedené trestné činy vede, nebo vůči níž je důvodné podezření, že se takových trestných činů dopustila. Pokud je řízení vedeno pouze na základě důvodného podezření, musí být v odůvodnění vyloženo, o jaké indicie se takový závěr opírá. Pouhé trestní oznámení samo o sobě, není-li doloženo alespoň indiciemi, z nichž lze důvodné podezření dovozovat, nepostačuje k nařízení odposlechů, neboť totiž nepostačuje ani k zahájení řízení k objasnění a prověřování skutečností důvodně nasvědčujících tomu, že byl spáchán trestný čin podle § 158 trestního řádu. Může tedy být vydán jen v řádně zahájeném trestním řízení pro zákonem kvalifikovanou trestnou činnost, a musí být podložen relevantními indiciemi, z nichž lze dovodit*

²⁷ Podrobně je upraveno v prováděcí vyhlášce č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti.

²⁸ SMEJKAL, V. Analýza rizik jako nástroj prevence kybernetické kriminality. In: Bradáč, A., Křížák, M. (eds.). *Sborník příspěvků XXVI. mezinárodní vědecké konference Expert Forensic Science 2017*. ÚSI VUT v Brně, Brno 2017, s. 504–515.

²⁹ Skutkové podstaty jsou podrobně popsány zejm. In SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015.

důvodné podezření ze spáchání takového trestného činu. Příkaz musí být individualizován ve vztahu ke konkrétní osobě, která je uživatelem telefonní stanice. Pokud tato skutečnost nevyplývá ze zjištění, že se jedná o majitele telefonní stanice, musí být zdůvodněno, na základě jakých zjištění je dovozováno, že ji má v držení a že ji skutečně používá, nebo ji v minulosti v nikoliv nepodstatné míře používala, a že tak bude s vysokou pravděpodobností činit i v budoucnu. Konečně musí příkaz alespoň v minimální míře konkrétně uvést, jaké skutečnosti významné pro trestní řízení mají být takto zjištěny, a z čeho je to vyvozováno.³⁰

V případě kyberprostoru pak můžeme rozlišit situaci, kdy bude sledována komunikace vnější – pak by se mělo jednat o odposlech a záznam telekomunikačního provozu podle § 88 tr. řádu, kam bude spadat i komunikace mezi zařízeními ICT, akceptujeme-li výkladový posun od sledování telekomunikačního provozu k monitorování přenášených informací, tj. signálů po sítích elektronických komunikací. Pokud by se mělo jednat o sledování toho, co se děje v počítačovém systému uvnitř (v paměti, na discích apod.), pak by se mělo jednat o režim podle ust. § 158d tr. řádu, upravujícího sledování osob a věcí. Jak uvedl Ústavní soud ČR, „Z dikce zákona jasně vyplývá, že v rámci tohoto úkonu lze pořizovat záznamy nejrůznějšího druhu a se souhlasem soudce může být v přiměřené míře zasahováno do práva na soukromí dotčených osob. Z hlediska ústavněprávní kontroly je podstatné, že soud ve svém povolení dostatečně jasně specifikoval okruh počítačů, které mají být sledovány. V rámci sledování elektronických zařízení z povahy věci plyne, že předmětem sledování budou právě data na těchto zařízeních uložená, jejichž otisk lze pořídit za využití utajené operativně pátrací techniky. Pořízení otisku elektronických dat lze povolit postupem dle § 158d odst. 3 tr. řádu, pokud jde o data na sledovaných počítačích již uložená, nikoli o data telekomunikačního provozu.“³¹

Zde se jednalo o pořízení otisku z počítače (zřejmě bitové kopie), což bylo alternativou k jinému možnému postupu v podobě vydání či odnětí věci (počítače či disků) podle § 78 – § 79 tr. řádu.

Situace nicméně není jednoduchá úměrně tomu, jak stále složitější jsou používané technologie. Typicky jde o problematiku zjištění obsahu e-mailové korespondence, kde je třeba zásadně rozlišit doručovanou a doručenou korespondenci, a to bez ohledu na její formu (podobně jak je tomu u listovní korespondence). **Ochrana podle ust. § 239 tr. zákoníku je tedy dopravované zprávě poskytována v době jejího doručování**, podobně jako zpráva obsažená v listovní zásilce doručované poštou je chráněna po dobu její přepravy. Jedná se o proces, jehož počátek je možno ohraničit odesláním zprávy z počítače odesílatele (nebo z jiného počítače, se kterým právě odesílatel pracuje). Konec procesu je pak nutno vnímat v okamžiku doručení zprávy do e-mailové schránky příjemce. Tímto okamžikem je totiž proces dopravy zprávy ukončen a v této schránce zpráva také zůstává, není-li adresátem smazána.³² K tomu uvedl NS ČR, že „Pokud jde o etapu přepravy zpráv v poštovním nebo telekomunikačním provozu, zákonodárce stanovil zprísňené podmínky pro ochranu tajemství těchto zpráv (§ 16 zák. č. 29/2000 Sb., upravující poštovní tajemství a § 84 a násl., zák. 151/2000 Sb., upravující telekomunikační tajemství a ochranu osobních a zprostředkovacích dat). Jedná se vlastně o zákonem stanovenou povinnost mlčenlivosti pro osoby vymezené v citovaných ustanoveních. Za této situace s ohledem na znění odst. 2 § 78 tr. ř. nelze k prolomení ochrany tajemství těchto zpráv v době, kdy jsou přepravovány k jejich adresátovi vystačit s aplikací institutů vydání a odnětí věci. Pro zjištění obsahu těchto zpráv je nezbytné použít postup předpokládaný § 86, § 87 a § 88 tr. ř. Avšak v případě, že zpráva již příjemci byla předá-

³⁰ Nález Ústavního soudu ČR sp. zn. II. ÚS 615/06 ze dne 23. 5. 2007. Podobně také Usnesení Ústavního soudu ČR sp. zn. 4 Pzo 14/2016-21 ze dne 15. 11. 2016.

³¹ Usnesení Ústavního soudu ČR sp. zn. III. ÚS 3812/12-1 ze dne 3. 10. 2013.

³² SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015, s. 239.

na – je v jeho dispozici, zvýšená ochrana, kterou požívala v průběhu přepravy, končí. Je pouze na příjemci zprávy, jak s ní naloží.“³³

Jak uvádí komentář,³⁴ „Smyslem ustanovení § 88 tr. řádu je možnost seznámit se s obsahem dopravovaných zpráv v elektronické podobě, tedy s obsahem tzv. telekomunikačního provozu. Problémem je, že zákonné sousloví „telekomunikační provoz“ již dnes nepostihuje všechny v úvahu přicházející formy elektronických komunikací uskutečňovaných v sítích elektronických komunikací, kam náleží nejen komunikace prostřednictvím veřejných telefonních sítí, ale i jiné služby elektronických komunikací, zejména ty, které se uskutečňují prostřednictvím internetových sociálních sítí či aplikací (Facebook, Skype etc.). Při nedostatku speciální právní úpravy pro různé formy elektronické komunikace používáme toto obecné ustanovení i pro zjištění obsahu e-mailů došlých a uschovaných v e-mailové schránce, a to i včetně fotografií, buď v určitém okamžiku nebo v určitém období. Pro tento účel se podle našeho názoru nepoužije ustanovení § 158d odst. 3 tr. řádu, které míří na jiné případy.

Je-li e-mailová zpráva vytištěna, jde o listinnou podobu telekomunikačního provozu. Takovou listinu lze vyžádat (§ 78) nebo odejmout (§ 79). Telekomunikační provoz zahrnuje nejen komunikaci s využitím telefonu, telefaxu, mobilního telefonu, vysílačky a jiného telekomunikačního zařízení, ale i zaslání zpráv elektronickou poštou, přičemž prostřednictvím mobilních telefonů lze při využívání internetového připojení rovněž odesílat a přijímat e-maily, tedy využívat jednu z forem elektronické pošty.“

V článku L. Vávry³⁵ se doporučuje, aby pro získání obsahu již přepravených e-mailových zpráv byl použit postup podle § 158d odst. 3 tr. řádu, ovšem za použití § 88 odst. 1 tr. řádu per analogiam, tedy povolení ke sledování osob a věcí za splnění omezujících podmínek uvedených v § 88 odst. 1 tr. řádu. „Takové řešení zajišťuje technickou možnost získat obsah uložených zpráv, současně zaručuje dostatečnou ochranu základnímu lidskému právu na tzv. listovní tajemství. Policie by měla u soudce uspět pouze a jen v případě, že je vedeno řízení pro v § 88 odst. 1 tr. řádu uvedený trestný čin a návrh je pochopitelně náležitě a konkrétně odůvodněn.“

Přitom ale doručená zpráva může být uložena v zařízení, které je pod fyzickou kontrolou určité osoby (v jejím počítači či na firemním serveru), ale i mimo ni (např. v cloudu nacházejícím se mimo území Evropy). Je otázkou, zda jakýkoliv výše uvedený postup povede k požadovanému cíli, tj. zda stopa nacházející se mimo danou jurisdikci bude pro OČTŘ dostupná.³⁶ V takovém případě by mohl vést k úspěchu pouze odposlech a záznam telekomunikačního provozu podle ust. § 88 tr. řádu prováděný na území ČR.

Digitální stopy související s činností ITP

Důkazy a jejich nalezení, zajištění, vytěžení a provedení v rámci trestního řízení hrají při vyšetřování trestné činnosti v kyberprostoru významnou roli, a to vzhledem ke svému specifickému charakteru. Na rozdíl od důkazů klasických – hmotných jsou důkazy spočívající v záznamu dat a procesů probíhajících v počítačových systémech a sítích obtížněji zjištěitelné a hůře zaznamatelné, snadno ovlivnitelné a obtížně interpretovatelné, pokud není dodržena správná metodika vyšetřování tohoto druhu trestné činnosti.

³³ Usnesení Nejvyššího soudu ČR sp. zn. 7 Tz 9/2000 ze dne 15. 12. 2000.

³⁴ JELÍNEK, J. a kol. *Trestní zákoník a trestní řád s poznámkami a judikaturou*. 6. aktualizované vyd. Praha: Leges, 2016.

³⁵ VÁVRA, L. Tak copak máme v tom mailu? *Právní prostor*, 8. 9. 2016. Dostupné na <http://www.pravniprostor.cz/clanky/trestni-pravo/tak-copak-mame-v-tom-mailu>.

³⁶ K tomu viz SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015, s. 496 a násled.

Každé technologické zařízení, které získává, zpracovává, předává nebo uchovává data, zanechává záznamy (odrazy) o své činnosti. Tyto záznamy z kriminalistického hlediska jsou stopami. Lze také říci, že digitální stopa je fyzikální interpretací (záznamem) nehmotné informace, zakódované do digitálního formátu.³⁷ Fyzické a datové objekty se stávají důkazy teprve tehdy, jsou-li akceptovatelné orgány činnými v trestním řízení. Klíčovou je právě otázka prokazatelnosti, že se stopa nacházela na určitém místě a že v procesu od jejího zajištění do ukončení znaleckého zkoumání nebyla žádným způsobem modifikována.

Z hlediska kriminalistické počítačové analýzy je pro nás klíčové, abychom mohli konformně správným a přísně legálním způsobem najít, zadokumentovat a provést důkazy zjištěné z digitálních stop.³⁸ V prostředí ICT lze nalézt řadu aspektů, které nám dokazování mimořádně znesnadňují, právě pro nehmotný charakter, vzdálený přístup, možnosti anonymity a vysokou dynamiku prostředí.³⁹

Závěr

Řada otázek souvisejících s nasazením ITP v kyberprostoru a v zařízeních ICT zůstává i nadále nejasných, případně lze poukázat na aspekty, které činí některé uvažované či prováděné postupy za rizikové pro všechny zúčastněné strany. Patří sem zejména:

1. Používání ITP v prostředí tzv. skrytého Internetu, tj. v síti, která má svůj vlastní doménový systém (.onion) a přistupuje se do ní v rámci šifrované anonymní sítě Tor.⁴⁰

2. Možnosti nasazení ITP obecně pro odposlech telekomunikačního provozu, který je šifrován. Platí sice ust. § 75 odst. 1 EKZ, *„Je-li to technicky proveditelné, je podnikatel poskytující veřejně dostupnou telefonní službu prostřednictvím veřejné mobilní telefonní sítě povinen na základě písemné žádosti Policie České republiky a na její náklady pro účely trestního řízení znemožnit na požadovanou dobu, nejdéle však na dobu povoleného odposlechu, provozování koncového mobilního telekomunikačního zařízení (mobilní telefonní přístroj) ve veřejné mobilní telefonní síti, který umožňuje šifrování, kódování nebo jiný způsob utajení přenášené zprávy účastníkem“*, nicméně jeho skutečná aplikovatelnost a vynutitelnost je značně problematická. Nemluvě o tom, že aplikací tohoto postupu (na rozdíl od ust. § 97 odst. 6 EKZ) se potenciální odposlouchávaný o zájmu orgánů o obsah jeho hovorů spolehlivě doví.

Toto ustanovení v podstatě může postihnout nejen vlastníky šifrovacích telefonů (např. Cryptocult), ale v podstatě každého majitele tzv. chytrého telefonu, vybaveného operačním systémem (např. Android, iOS, PalmOS, Symbian OS, Windows Phone apod.) a s možností instalovat nejrůznější aplikace, mezi kterými se mohou vyskytovat i aplikace chránící obsah komunikace jako vedlejší efekt (Skype, WhatsApp, Viber apod.) nebo jako hlavní cíl jejich nasazení (např. Tiger XS, pořízený bezpečnostní a zpravodajskou komunitou ČR, nebo běžně dostupné produkty jako Secuvoice, Teldeko, Cryptosmart apod.). Pokud zákonodárce umožňuje tento postup vůči přístrojům, které „umožňují“ šifrování, a to bez ohledu na to, zda tak uživatel skutečně činí (a otázkou je, zda při použití IP telefonie to může Policie ČR vůbec zjistit), pak se jedná o velice

³⁷ PORADA, V., ŠEDIVÝ, P. Praktická využitelnost kriminalistických a forenzních aplikací v oblasti počítačové/kybernetické kriminality. *Karlovarská právní revue*, 2012, č. 3, s. 94–114.

³⁸ Viz zejména SMEJKAL, V. Metodika vyšetřování kybernetické kriminality. In: Porada Viktor a kol. *KRIMINALISTIKA. Technické, forenzní a kybernetické aspekty*. 1. vydání. Plzeň: Aleš Čeněk, 2016, s. 786–802.

³⁹ Viz např. SMEJKAL, V. Důkazy a dokazování v kyberprostoru. Sborník z konference „PRIENIKY TRESTNÉHO PRÁVA K INÝM PRÁVNÝM ODVETVIAM A VEDNÝM DISCIPLÍNAM“, Košice: Právnická fakulta UPJŠ v Košiciach, 24. 11. 2016, v tisku.

⁴⁰ K tomu viz SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015, s. 71 a násl.

silnou presumpci viny a nelze než doufat, že povolující soud bude zkoumat velice bedlivě a ve smyslu poměrně rozsáhlé judikatury Ústavního soudu přiměřenost takového požadavku.

3. S touto tematikou úzce souvisí i snahy vlád prakticky celého světa o zpřístupnění dat, tedy prolomení šifrování používaného v zařízeních ICT. Moderní šifrování využívající výhody digitalizace informací prodělalo v posledních desetiletích významný vývoj. K dešifrování utajených dat již není možné využívat charakteristických znaků řeči, ani nedokonalosti „neprolomitelných“ šifrovacích algoritmů. Tím na jednu stranu roste bariéra proti útočníkům na obsah nosičů informací, na druhou stranu dochází k nevyhnutelnému střetu mezi zájmy státu na boj proti různým kriminálním, teroristickým a jiným nelegálním aktivitám, na druhou stranu oprávněný zájem fyzických i právnických osob na ochranu soukromí a důvěrných informací.

Pod hlavičkou boje proti terorismu sílí tlak vládních organizací na zamezení možnosti ochrany identity a obsahu (komunikace a dat na nosičích informací), neboť tvrdí, že se kybernetické nástroje a kyberprostor staly velice efektivními pomůckami pro organizovaný zločin a terorismus (např. možnosti dané šifrováním). V České republice se jako stejná záminka používá dnes všudypřítomný „boj s korupcí“, který hraje stejnou úlohu v zdůvodňování nepřiměřených postupů orgánů činných v trestním řízení v oblasti odposlechů (monitorování služeb elektronických komunikací a lokalizačních údajů), přičemž nelze vyloučit i aktivní zasahování do (zákonem chráněné elektronické komunikace) tak, aby došlo k jejímu ovlivnění nebo odposlechu, při snaze získat nástroj na prolamování šifer viz níže bod 4.⁴¹

4. Jako velmi nebezpečný nástroj se jeví pořízení softwaru s názvem „Remote Control System Galileo“ firmy Hacking Team využívaného údajně od roku 2011 Policií ČR pro úkony podle § 158d tr. řádu. Podle veřejných zdrojů zmiňovaný software je schopen infiltrovat elektronická zařízení, využít je ke sledování jejich obsahu, odposlouchávání a pozměňování jejich softwarového vybavení a obsahu datových souborů, aktivovat kameru zařízení a ukládat pořízené obrázky nebo video, zaznamenávání všech stisků kláves a hesel uložených v zařízení.⁴² Podobnou úlohu údajně plní i software FinFisher společnosti Gamma.

Lze očekávat, že se začnou objevovat argumenty obhajoby o tom, že usvědčující materiály – např. dětskou pornografii u osoby, podezřelé ze spáchání hospodářských trestných činů – mohla do jeho počítače nahrát sama policie s využitím takového programu, a obtížně, jako každý důkaz věrnosti, se budou vyvracet.

5. Současné možnosti nasazování ITP, odposlechů, zjišťování provozních a lokalizačních údajů, propojování databází atd. vedou k tomu, že lze stále více pozorovat, jak policejní složky, alespoň v ČR, prakticky rezignovaly na klasickou policejní práci a místo toho spoléhají na stále plošnější monitorování obyvatelstva. Jak uvedl Ústavní soud ČR ve věci návrhu na zrušení § 97 odst. 3 a 4 EKZ, „*Plošné shromažďování a využívání provozních a lokalizačních údajů o telekomunikačním provozu, zejména bez jasného omezení veřejné moci v daném směru a poskytnutí příslušných záruk jednotlivci, představuje porušení požadavků plynoucích z principu právního státu a je v kolizi s požadavky na omezení základního práva na soukromí v podobě práva na informační sebeurčení ve smyslu čl. 10 odst. 3 a čl. 13 Listiny, které plynou z principu proporcionality.*“⁴³

⁴¹ SMEJKAL, V., KODL, J. Význam autentizace a šifrování pro zajištění bezpečnosti informačních systémů. In: Lisník, Anton a Katarína Greňová (eds.). *Posolstvo Jána Pavla II. 2016 „Súčasný výzvy a trendy v...“*. Zborník z medzinárodnej vedeckej konferencie konanej v dňoch 21. – 22. apríla 2016 v Poprade. VERBUM – vydavateľstvo Katolíckej univerzity v Ružomberku, Ružomberok 2016, s. 324–333.

⁴² ŠPAČEK, S. *Analýza Remote Control Systemu společnosti Hacking Team*. Diplomová práce. Brno: Fakulta informatiky Masarykovy univerzity, 2016.

⁴³ Nález Ústavního soudu ČR sp. zn. Pl. ÚS 24/10-1 ze dne 22. 3. 2011.

Na Slovensku po zrušení směrnice č. 2006/24/ES⁴⁴ Velkým senátem Soudního dvora EU a v souladu s dalšími rozhodnutími SDEU⁴⁵ je uplatňován princip Data Freeze (tedy adresní sledování), zatímco v ČR stále přetrvává princip Data Retention (plošné sledování). Slovenská právní úprava, která v porovnání s právní úpravou Data Retention sleduje totožný veřejný zájem, podle dostupných informací funguje se srovnatelnou efektivitou, avšak při nesrovnatelně méně intenzivním zásahu do práva na ochranu soukromí.⁴⁶

6. V současné době je ve 2. čtení v Poslanecké sněmovně Parlamentu ČR velmi diskutovaná, až kontroverzní novela zákona č. 289/2005 Sb., o Vojenském zpravodajství,⁴⁷ která pověřuje Vojenské zpravodajství plněním úkolů obrany České republiky v kybernetickém prostoru (dále jen „kybernetická obrana“). Text této novely je značně vágní, přičemž nedochází k takové specifikaci nástrojů a postupů, které mají být používány, aby to nebudilo obavy z možného zneužití. Podle novely může Vojenské zpravodajství při zajišťování kybernetické obrany využívat technické prostředky kybernetické obrany, kterými jsou věcné technické prostředky a související postupy a opatření vedoucí k předcházení, zastavení nebo odvrácení kybernetického útoku ohrožujícího zajišťování obrany České republiky. Využívat technické prostředky kybernetické obrany na území České republiky, pokud lze očekávat, že naruší důvěrnost zpráv podle zákona o elektronických komunikacích a s nimi spojených provozních a lokalizačních údajů konkrétní osoby, lze výlučně za podmínek stanovených pro použití zpravodajské techniky tímto zákonem. Umístění technických prostředků kybernetické obrany podle § 16a může být provedeno výlučně na základě jeho schválení vládou, která rovněž schválí podmínky jejich používání k zajištění kybernetické obrany. Přitom Vojenské zpravodajství může za podmínek schválených vládou podle § 16b a v rozsahu potřebném pro zajišťování kybernetické obrany požadovat od právnické nebo podnikající fyzické osoby zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací zřízení a zabezpečení rozhraní pro připojení technických prostředků kybernetické obrany. Je zřejmé, že z dikce zákona nelze vydedukovat nic jiného, nežli že vláda bude mít plnou kontrolu i odpovědnost za to, jaké (neznámé) prostředky, ve sdělovacích prostředcích označované jako „černé krabičky“, budou u poskytovatelů zajišťujících síť a služby elektronických komunikací připojovány.

7. Stále nové technické možnosti – např. využití dronů jako ITP – bude přinášet stále více legislativních, procesních i metodických otázek, které bude třeba řešit ústavně konformním způsobem.⁴⁸

⁴⁴ Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES, Úř. věst. EU, L 105, 13. 4. 2006, s. 54–63.

⁴⁵ Rozsudkem Velkého senátu Soudního dvora EU ze dne 8. dubna 2014, spojené věci C-293/12 a C-594/12 byla směrnice Evropského parlamentu a Rady 2006/24/ES prohlášena za neplatnou. V rozsudku z 21. prosince 2016 ve spojených věcech C-203/15 a C-698/15 Soudní dvůr EU rozhodl, že vnitrostátní právní úprava založená na plošném uchovávání veškerých provozních a lokalizačních údajů všech účastníků a uživatelů je v rozporu s Listinou základních práv EU, a to i v případě, když by takováto národní právní úprava byla přijata za účelem boje proti trestné činnosti.

⁴⁶ UŘIČAŘ, M. Data Retention – povinnost uchovávat provozní a lokalizační údaje účastníků a uživatelů služeb a sítí elektronických komunikací ve světle judikatury. Sborník z konference „PRIENIKY TREŠTNÉHO PRÁVA K INÝM PRÁVNÝM ODVETVIAM A VEDNÝM DISCIPLÍNAM“, Košice: Právnická fakulta UPJŠ v Košiciach, 24. 11. 2016, v tisku.

⁴⁷ Sněmovní tisk 931/0, Poslanecká sněmovna, 7. volební období, od 2013.

⁴⁸ „Policie ČR zavádí do výzbroje bezpilotní prostředek z produkce Vojenského technického ústavu. ... Unikátní řídicí systém tohoto bezpilotního prostředku nám do budoucna umožní autonomní lety s konkrétním zadáním,“ konstatuje zástupce vedoucího územního odboru Příbram Krajského ředitelství policie Středočeského kraje plk. Ing. Ondřej Smotlacha. – viz <http://www.policiejinoviny.cz/drony-brus-v-rukach-policie.html>.

Literatura

- BASTL, M., GRUBEROVÁ, Z. Kyberprostor jako „pátá doména“? *Vojenské rozhledy*, 2013, roč. 22 (54), č. 4, s. 10–21.
- BERTALANFFY, L. von. *General System Theory: Foundations, Development, Applications*. New York: George Braziller, 1968.
- CENTRE FOR INTERNATIONAL GOVERNANCE INNOVATION AND THE ROYAL INSTITUTE OF INTERNATIONAL AFFAIRS. *Research Volume Two – Global Commission on Internet Governance. Who Runs the Internet? The Global Multi-stakeholder Model of Internet Governance*. Waterloo, ON, Canada, 2016. Dostupné na <https://www.cigionline.org/sites/default/files/documents/GCIG%20Volume%202.pdf>.
- JELÍNEK, J. a kol. *Trestní zákoník a trestní řád s poznámkami a judikaturou*. 6. aktualizované vyd. Praha: Leges, 2016.
- MAYER, M., MARTINO, L., MAZURIER, P., TZVETKOVA, G. *How would you define Cyberspace?* First Draft Pisa, 19. 5. 2014. Dostupné na https://www.academia.edu/7096442/How_would_you_define_Cyberspace.
- NOVÁK, J. ml. K uchování provozních a lokalizačních údajů v České republice ve světle rozhodnutí Soudního dvora Evropské unie. *Bulletin advokacie*, 2015, č. 5, s. 36–41.
- PORADA, V., ŠEDIVÝ, P. Praktická využitelnost kriminalistických a forenzních aplikací v oblasti počítačové/kybernetické kriminality. *Karlovarská právní revue*, 2012, č. 3, s. 94–114.
- SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015.
- SMEJKAL, V. Metodika vyšetřování kybernetické kriminality. In: Porada Viktor a kol. *KRIMINALISTIKA. Technické, forenzní a kybernetické aspekty*. 1. vydání. Plzeň: Aleš Čeněk, 2016, s. 786–802.
- SMEJKAL, V. Důkazy a dokazování v kyberprostoru. Sborník z konference „PRIENIKY TRESTNÉHO PRÁVA K INÝM PRÁVNÝM ODVETVIAM A VEDNÝM DISCIPLÍNAM“, Košice: Právnická fakulta UPJŠ v Košiciach, 24. 11. 2016, v tisku.
- SMEJKAL, V. Analýza rizik jako nástroj prevence kybernetické kriminality. In: Bradáč, A., Křižák, M. (eds.). *Sborník příspěvků XXVI. mezinárodní vědecké konference Expert Forensic Science 2017*. ÚSI VUT v Brně, Brno 2017, s. 504–515.
- SMEJKAL, V., KODL, J. Význam autentizace a šifrování pro zajištění bezpečnosti informačních systémů. In: Lisník, Anton a Katarína Greňová (eds.). *Posolstvo Jána Pavla II. 2016 „Súčasný výzvy a trendy v...“*. Zborník z medzinárodnej vedeckej konferencie konanej v dňoch 21. – 22. apríla 2016 v Poprade. VERBUM – vydavateľstvo Katolíckej univerzity v Ružomberku, Ružomberok 2016, s. 324–333.
- ŠÁMAL, P., NOVOTNÝ, F., RŮŽIČKA, M., VONDRUŠKA, F., NOVOTNÁ, J. *Přípravné řízení trestní*. 2. podstatně přepracované vydání, Praha: C. H. Beck, 2003, s. 247.
- ŠPAČEK, S. *Analýza Remote Control Systemu společnosti Hacking Team*. Diplomová práce. Brno: Fakulta informatiky Masarykovy univerzity, 2016.
- UŘIČAŘ, M. Data Retention – povinnost uchovávat provozní a lokalizační údaje účastníků a uživatelů služeb a sítí elektronických komunikací ve světle judikatury. Sborník z konference „PRIENIKY TRESTNÉHO PRÁVA K INÝM PRÁVNÝM ODVETVIAM A VEDNÝM DISCIPLÍNAM“, Košice: Právnická fakulta UPJŠ v Košiciach, 24. 11. 2016, v tisku.
- VÁVRA, L. Tak copak máme v tom mailu? *Právní prostor*, 8. 9. 2016. Dostupné na <http://www.pravniprostor.cz/clanky/trestni-pravo/tak-copak-mame-v-tom-mailu>.
- VESELÝ, J. *Systémové nástroje řízení*. Praha: Institut řízení, 1982.

Použitie inštitútu agenta pri odhaľovaní a objasňovaní kriminality v kybernetickom prostredí

The Use of Agent's Institute in Crime Detection and Investigation in Cyber Environment

Lucia Kurilovská¹

Stanislav Šišulák²

Abstrakt: Cieľom odborného článku je zadefinovať pojem agenta z trestnoprávneho aspektu v kybernetickom prostredí a to v intenciách právneho poriadku Slovenskej republiky a poukázať na niektoré aplikačné problémy v exekutive oprávnení kompetentných orgánov v súvislosti s týmto druhom kriminality. Súčasne akcentuje na základné úkony v procese dokazovania a prezentuje nielen najčastejšie problémy v súvislosti s vyhodnocovaním a objasňovaním kriminality v kybernetickom prostredí, ale taktiež navrhuje určité metodické postupy kompetentných orgánov v prípadoch protiprávneho konania zo strany páchatelov voči používateľom internetových služieb.

Abstract: The objective of this article is to define the concept of an agent in the criminal aspect in the cyber environment within the intentions of the Slovak legal system and to point out to some application problems in the executive branch authorized by the competent authorities with regard to this type of criminality. At the same time it emphasizes the basic steps in the process of detection and represents not only the most common problems in relation to scoring and detection of crime in the cyber environment, but it also proposes specific methodological procedures of competent authorities in cases of illicit action from the part of the perpetrators towards the users of Internet services.

Kľúčové slová: kyberpriestor, informačná bezpečnosť, trestný čin, agent, páchatel, trestné konanie, dokazovanie, technické prostriedky.

Keywords: cyberspace, information security, criminal act, agent, perpetrator, criminal prosecution, proof, technical resources.

Úvod

Problematika kybernetickej kriminality každým dňom nadobúda na svojom význame. Rozsiahle útoky v kybernetickom priestore permanentne nútia štáty k aktívnejšiemu postupu v oblasti prevencie a bezpečnosti. Máme tým na mysli najmä bezpečnostné incidenty ktoré môžu významne dezorganizovať a dezorientovať celú spoločnosť. Medzi hlavné bezpečnostné hrozby, ktorým musia jednotlivé štáty čeliť patrí kybernetická kriminalita. Súčasná doba je charakteristická pomerne vysokou závislosťou samotných organizácií na používaní informačných a komunikačných technológií a elektronickom spracúvaní údajov. A práve pri zneužití informačných a komunikačných technológií môže dôjsť k strate kontinuity v činnosti organizácie, maximalizácii obchodných strát a minimalizácii návratnosti investícií. Ak chceme bližšie prezentovať možnosti a spôsoby použitia inštitútu agenta v tomto prostredí musíme poukázať na rozdielnosť

¹ Lucia Kurilovská, Doc., JUDr., PhD., Právnická fakulta, Katedra trestného práva, kriminológie a kriminalistiky, Univerzita Komenského v Bratislave, Šafárikovo nám. č. 6, 810 00 Bratislava, Slovenská republika, lucia.kurilovska@flaw.uniba.sk.

² Stanislav Šišulák, Ing., PhD., Katedra kriminalistiky a forenzných vied, Akadémia Policajného zboru v Bratislave, Sklabinská č. 1, 831 06 Bratislava, Slovenská republika, stanislav.sisulak@minv.sk.

niektorých pojmov, s ktorými sa v praxi veľmi často stretávame. Konkrétne sa jedná o pojmy kybernetická bezpečnosť a informačná bezpečnosť. Aký je však medzi nimi rozdiel? Kybernetická bezpečnosť zahŕňa schopnosť obrany proti kybernetickým útokom. Kybernetická bezpečnosť je súhrn právnych, organizačných, technických a vzdelávacích prostriedkov smerujúcich k zabezpečeniu ochrany kybernetického priestoru.³ Ide o ochranu počítačov, sietí a internej a externej komunikácie spojenej prostredníctvom kybernetickej bezpečnosti. A ak niekto pracuje na informačnej bezpečnosti tak vlastne hodnotí riziká a zraniteľnosť ktoré potom implementuje do plánu riadenia z dôvodu minimalizácie problémov. Napríklad pojem „informačná bezpečnosť“ bol prvýkrát použitý americkou vládou, ale od tej doby sa v bežnom prostredí vyvinul ako definícia „technických a riadiacich opatrení, ktoré majú zabezpečiť dôvernosť, kontrolu, integritu, autentickosť, dostupnosť a užitočnosť informácií a informačných systémov.“⁴

Cieľom informačnej bezpečnosti je chrániť informácie a informačné systémy zabezpečením ich dostupnosti, integrity, dôvernosti, autentifikácie a nepopierateľnosti. Patrí sem aj obnova informačných systémov zabudovaním kapacít v oblasti detekcie a reakcie na bezpečnostné incidenty. Pozor, ale stále musíme myslieť na to, že informačná bezpečnosť sa vzťahuje aj na informácie, ktoré nemajú elektronickú podobu, to znamená, že opatrenia smerujú aj k zaisteniu bezpečnosti tlačенých dokumentov.⁵ Pojem kybernetická bezpečnosť je v skutočnosti o niečo menej široký v jeho definícii a je považovaný za podmnožinu k definícii informačnej bezpečnosti. Kybernetickú bezpečnosť chápeme ako ochranu dát a systémov v sieťach, ktoré sú pripojené k internetu.⁶ Základom kybernetickej bezpečnosti je zaistenie ochrany kybernetického priestoru na národnej úrovni. V našich podmienkach však budeme vychádzať z premisy že kybernetická bezpečnosť je podmnožinou informačnej bezpečnosti. Nakoľko cieľom informačnej bezpečnosti je ochrana informácií v akejkoľvek forme, oproti tomu, že cieľom kybernetickej bezpečnosti je ochrana informácií len v digitálnej forme. Skutočnosť že pojem „kybernetická bezpečnosť“ nie je doteraz v Slovenskej republike definovaný, dokumentuje v súvislosti s prijatím Konceptie kybernetickej bezpečnosti Slovenska na roky 2015 – 2020⁷ aj nasledovný text: „O fakte, že kybernetickej bezpečnosti nebola doteraz venovaná náležitá pozornosť, svedčí podľa koncepcie i to, že nemá formálne ustálenú terminológiu v tejto oblasti. Slovo kybernetický sa momentálne nevyskytuje v žiadnom všeobecne záväznom právnom predpise ani terminologických slovníkoch.“⁸ V uvedenej téme rezonujú aj pojmy ako kybernetický priestor, kybernetické riziká, kybernetické hrozby, kritická infraštruktúra, kritická informatická infraštruktúra, národná infraštruktúra ktorých interpretáciou by sme ale prekročili náš edukačný zámer.

³ Národné centrum kybernetickej bezpečnosti. Výkladový slovník kybernetickej bezpečnosti – tretí vydání [cit. 2015-12-11] Dostupné na internete: <<http://www.govcert.cz/cs/informacni-servis/vykladovy-slovník/>>.

⁴ PC Magazine [cit. 2017-02-11] Dostupné na internete: <<http://www.pcmag.com/encyclopedia/term/44936/information-assurance>>.

⁵ HUDEC, L.: Bezpečnostné požiadavky na zariadenia pre elektronický podpis. s. 7 [cit. 2017-02-16] Dostupné na internete: <www.lnd.sk/hudec2003-1.rtf>.

⁶ PC Magazine [cit. 2017-03-03] Dostupné na internete: <<http://www.pcmag.com/encyclopedia/term/40643/cyber-security>>.

⁷ Konceptia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020, Rokovania vlády Slovenskej republiky [cit. 2017-03-09] Dostupné na internete: <<http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=24702>>.

⁸ Web noviny, Hlavné správy, Vláda prijala Konceptiu Kybernetickej bezpečnosti Slovenska na roky 2015 – 2020 [cit. 2017-03-10] Dostupné na internete: <<http://www.hlavnespravy.sk/vlada-prijala-koncepciu-kybernetickej-bezpecnosti-slovenska-na-roky-2015-2020/633726>>.

Agent v trestno-procesnej rovine

Prostredie virtuálnej reality, čiže komplexne vnímaný kyberpriestor, je rozsiahlym systémom, poskytujúci bezpočetné množstvo možností v sociálnej, pracovnej, informačnej i technickej rovine. Je však aj priestorom, v ktorom sa preukázateľne pácha protiprávna činnosť a preto je dôležité reflektovať na nastupujúce trendy kriminality a používať všetky možnosti predchádzania, odhaľovania a objasňovania týchto trestných činov.

V kybernetickom prostredí je dôležité prihliadať na všetky aspekty jeho fungovania, pričom jedným z najdôležitejších je práve právne definovanie určitých procesov a správania sa jeho používateľov. V trestno-právnej, respektíve trestno-procesnej rovine pôjde najmä o jasné definovanie protiprávnosti určitých konaní a kreovanie nových druhov trestných činov, v rovine procesnej najmä o delegovanie a určenie kompetencií orgánom činným v trestnom konaní pri vyšetrovaní či operatívno-pátracej činnosti a možnostiach dokazovania a samozrejme zákonosti jednotlivých postupov.

V rámci uvedených skutočností je potrebné vyvodiť záver, že každý procesný úkon či použitý procesný prostriedok musí byť jednak v súlade s právnymi princípmi trestných kódexov, ale musí však rovnako odzrkadľovať aktuálny stav trestnej činnosti v tom – ktorom prostredí a prispôbovať dokazovanie súčasným trendom. Nakoľko kybernetické prostredie svojou štruktúrou, obrovským množstvom údajov a používateľov je bezprecedentne špecifickým, je nevyhnutné používať také prostriedky, ktoré dokážu efektívne a rýchlo zhromaždiť relevantné informácie ako podklad či už k samotnému trestnému konaniu alebo k meritórnemu rozhodnutiu v zmysle platného Trestného poriadku.⁹ Vzhľadom na to, že v rámci trestných činov, páchaných v prostredí internetu (kyberpriestore) prostredníctvom informačných a komunikačných technológií môžeme hovoriť o veľmi sofistikovaných a latentných skutkoch, je nanajvýš potrebné uvažovať o používaní takých procesných prostriedkov, ktoré dokážu účinne odhaľovať, zisťovať a usvedčovať páchatelov týchto skutkov. Jedným z tých nástrojov, ktorý by mohol byť veľmi efektívny a účinný, je inštitút agenta.

Pri definícii pojmu agent v trestnom konaní je potrebné hľadiť na relevantné právne definície. Agent je subsumovaný ako jeden z prostriedkov operatívno-pátracej činnosti, ktoré sú definované v § 10 ods. 22 Trestného poriadku. Podľa § 10 ods. 20 je legálnym pojmom agent označený *„príslušník Policajného zboru alebo príslušník polície iného štátu, ktorý na základe príkazu prokurátora alebo súdu prispieva k odhaľovaniu, zisťovaniu a usvedčovaniu páchatelov zločinu, trestných činov uvedených v treťom diele ôsmej hlavy osobitnej časti Trestného zákona, trestného činu zneužívania právomoci verejného činiteľa a trestného činu legalizácie príjmu z trestnej činnosti. Pri odhaľovaní, zisťovaní a usvedčovaní páchatelov korupcie alebo trestných činov terorizmu môže byť agentom aj iná osoba ako príslušník Policajného zboru ustanovená prokurátorom na návrh policajta alebo príslušníka Policajného zboru povereného ministrom vnútra Slovenskej republiky“*.¹⁰

Z právnej kvalifikácie tohto pojmu môžeme taxatívne určiť konkrétne trestné činy, pri ktorých je možné inštitút agenta použiť, pričom ide najmä o korupčné trestné činy a trestné činy verejných činiteľov a zločiny, teda trestné činy, pri ktorých je možné uložiť trest odňatia slobody s hornou hranicou trestnej sadzby prevyšujúcu päť rokov. Táto skutočnosť vychádza najmä z potreby a zložitosti jednotlivých trestných vecí v korelácii s použitím agenta ako procesného prostriedku, respektíve operatívno-pátracieho prostriedku v rámci trestného poriadku. Agent

⁹ Zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov.

¹⁰ § 10 ods. 20 Zákona č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov.

predstavuje veľmi zložitý prostriedok, ktorý si vyžaduje nie len pevný legislatívny a teoretický základ, ale najmä praktické skúsenosti a takisto aj profesionálne personálne a materiálno-technické zabezpečenie.¹¹

Možnosti použitia inštitútu agenta, ako aj úpravu jednotlivých náležitostí pri jeho použití, definuje § 117 Trestného poriadku. Podľa tohto ustanovenia predmetného zákona „na odhaľovanie, zisťovanie a usvedčovanie páchatelov zločinov, korupcie, trestných činov extrémizmu, trestného činu zneužívania právomoci verejného činiteľa alebo trestného činu legalizácie príjmu z trestnej činnosti možno použiť agenta. Jeho použitie je prípustné len vtedy, ak odhaľovanie, zisťovanie a usvedčovanie páchatelov uvedených trestných činov by bolo iným spôsobom podstatne sťažené a získané poznatky odôvodňujú podozrenie, že bol spáchaný trestný čin alebo má byť spáchaný taký trestný čin.“¹² Trestný poriadok predpokladá, že použitie agenta je len možnosťou, nie zákonným predpokladom či obligatórnou súčasťou dokazovania taxatívne vymenovaných trestných činov, čo zabezpečuje využitie celkového potenciálu tohto inštitútu, nakoľko nie je potrebné používať agenta pri každom prípade uvedených trestných činov.

Rovnako je dôležité pripomenúť, že agent ako už „reálna osoba“ je limitovaný právnymi normami a to tak, že „konanie agenta musí byť v súlade s účelom tohto zákona a musí byť úmerné protiprávnosti konania, na odhaľovaní, zisťovaní alebo usvedčovaní ktorého sa zúčastňuje. Agent nesmie iniciatívne navádzať na spáchanie trestného činu; to neplatí, ak ide o korupciu verejného činiteľa alebo zahraničného verejného činiteľa a zistené skutočnosti nasvedčujú, že páchatel by spáchal taký trestný čin aj vtedy, ak by príkaz na použitie agenta nebol vydaný.“¹³ Pôsobenie agenta a jeho samotné konanie musí byť jednoznačne kontrolovateľné a kontrolované, pričom ak agent nekoná v súlade so zákonom, je potrebné voči nemu vyvodiť príslušné konzekvencie. Ak odhliadneme od inštitútu agenta provokatéra, agent ako osoba pôsobí v záujmovom prostredí za účelom priameho získavania informácií, respektíve dôkazných prostriedkov, potrebných na odhaľovanie a objasňovanie konkrétneho trestného činu. Takáto osoba, ktorá je príslušníkom Policajného zboru, však vo väčšine prípadov nemôže vystupovať pod svojim vlastným menom, preto je zákonne možné vytvoriť takejto osobe dočasnú alebo trvalú legendu (identitu), aby bolo znemožnené odhalenie jeho totožnosti a najmä príslušnosti k Policajnému zboru.

Zákonné predpoklady použitia agenta, ako aj legálne definície jeho činnosti a možností musia podliehať logickým zmenám v rámci reflektovania nových trendov v páchaní kriminality, najmä tej obzvlášť závažnej. Takisto je na mieste pripomenúť, že ako sa menia spôsoby páchania trestnej činnosti, tak sa mení aj prostredie, v ktorom je páchaná a rovnako vznikajú nové, protiprávne konania, na ktoré je treba reagovať nielen zahrnutím do Trestného zákona ako takého, ale aj vytváraním a používaním takých dôkazných a procesných prostriedkov, ktoré pomôžu efektívne odhaliť a vyšetriť nové formy kriminality v akomkoľvek prostredí.

Špecifiká inštitútu agenta v kybernetickom prostredí

Aj napriek tomu, že inštitút agenta je teoreticky aj právne jasne definovaný a zákonné právomoci a limity nastavené a relatívne ustálené,¹⁴ je potrebné poukázať na určité špecifiká, ktoré vznikajú v súvislosti s použitím agenta v kybernetickom prostredí.

¹¹ REMETA, R. *Výsluch agenta*, In: Policajná teória a prax, 2013, číslo 4, s. 109.

¹² § 117 ods. 1 zák. č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov.

¹³ § 117 ods. 2 zák. č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov.

¹⁴ Pozri viac odseky § 117 Zákona č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov.

Odhaľovanie, objasňovanie a predchádzanie kriminalite v kybernetickom prostredí je veľmi náročný proces, ktorý si vyžaduje osobitný prístup vzhľadom na atypické procesy a špecifickú fungovania kyberpriestoru. Tie kladú na orgány činné v trestnom konaní nie len vysoko náročné kritériá v legislatívno-právnej rovine, ale aj v rovine technických zručností a vedomostí.¹⁵ Znamená to, že ak orgány, oprávnené v zmysle zákona vyšetrovať trestné činy v kyberpriestore, sú dostatočne technologicky a personálne vybavené a majú aj náležitú podporu v zákone, ich práca je efektívnejšia a opodstatnenejšia. Nakoľko mnohé z kybernetických trestných činov sú sofistikované a najmä latentné, zo strany kompetentných orgánov nemožno požadovať len ich odhalenie a náležité vyšetrovanie, ale aj popísanie spôsobu ich vykonania a zabezpečiť následnú prevenciu pred ich opätovným spáchaním.

Z uvedenej premisy je zrejme možné vyvodiť jednoznačný záver, že nekompetentný orgán nemôže adekvátne riešiť nastolený sofistikovaný problém a rovnako nemôže používať prostriedky, ktoré sú neefektívne, respektíve bez podpory zákona majú pomôcť k odhaleniu a následne aj zabrániť páchaniu kriminality. Získavanie relevantných dôkazov, používanie procesných prostriedkov a komplexne proces vyšetrovania je v kybernetickom prostredí o to zložitejší, že priestor, v ktorom sa trestné činy páchajú, presahuje hranice štátov a štátnych zriadení s odlišnými právnymi systémami a platnými zákonmi. To však nie je jediným problémom právnej regulácie „kybernetických trestných činov“, pretože svoj podiel ťažkopádnosti a vágnosti nesú aj samotní prevádzkovatelia služieb vo virtuálnom prostredí.¹⁶

Je na mieste uvedomiť si, že moderné technológie slúžia nie len na uľahčenie života ich používateľom, ale poskytujú aj nové možnosti pre kompetentné orgány v zabezpečovaní dôkazných prostriedkov a vytváranie dobre zorganizovaných a premyslených postupov v boji proti kriminalite. Takýto druh sebareflexie je nanajvýš dôležitý najmä pri nových druhoch trestnej činnosti, kde „bežné“ postupy a procesné úkony nestačia na adekvátne získavanie informácií.

V súvislosti s vyšetrovaním kyberkriminality je dôležité poznamenať, že aj napriek pokročilým možnostiam virtuálneho sveta aj v tejto oblasti, existuje súbor postupov a činností, ktoré presahujú rámec niekoľkých vedných odborov a technických disciplín a priamo zahŕňajú aj procesne používané logické prostriedky orgánov činných v trestnom konaní. V procese odhaľovania a vyšetrovania jednotlivých trestných činov v kyberpriestore je dôležité postupovať, nie len podľa platných právnych noriem, ale aj podľa určitých stanovených predpokladov, ktoré sú kladené na jednotlivé zložky v procese vyšetrovania. Môžeme ich rozdeliť na:¹⁷

Súbor organizačných prostriedkov

- komunikácia – prostriedok založený na styku s verejnosťou, komunikácii s kompetentnými orgánmi, s akademickou obcou, odborníkmi a podobne.
- racionálne postupy – zahŕňa rýchlu a efektívnu reakciu na vzniknutý problém s následnou potrebou správneho vyhodnotenia a prijatia adekvátnych postupov.
- spolupráca – vytvára predpoklady pre interdisciplinárne vzťahy a ich udržanie.
- intuícia – prezentuje zmysel pre rozlišovanie rizikových udalostí.
- súvislosti – tento prostriedok prezentuje získané informácie, ktoré aplikuje pre široké spektrum prijímateľov.
- flexibilita – určuje priority kompetentných orgánov a vytvára pracovné postupy jednotlivých zložiek.

¹⁵ GRAYCAR, A.: *New crimes or new responses*, 2001, Australian institute of criminology, s. 7.

¹⁶ ŠALMÍK, M.: *Kriminalita na sociálnych sieťach*, Diplomová práca, 2014, Akadémia PZ v Bratislave, s. 20.

¹⁷ BROWN, C.: *Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice*, In: *International Journal of Cyber Criminology*, 2015, číslo 9, s. 65.

- presnosť – je dôležitou súčasťou procesných postupov, nakoľko vytvára podmienky pre striktné dodržiavanie termínov a následné výstupy podľa vopred určenej špecifikácie.
- výber – zakladá pozornosť k relevantným informáciám a detailom, ktoré sú dôležité pre riadne objasnenie problému.
- zákonnosť – ide o dôležitý prostriedok dodržiavania platných právnych noriem a interných predpisov.
- stratégia – v rámci riešenia problému je potrebné vytvárať také postupy, ktoré individuálne reflektujú na danú špecifickú situáciu a zároveň predpokladajú efektívne plnenie vopred stanovených úloh.

Súbor technických prostriedkov

- výskum – zahŕňa získavanie dôkazných prostriedkov a informácií pomocou dostupných nástrojov kybernetického prostredia.
- vzdelávanie – vytvára predpoklady na neustály edukatívny rozvoj personálnej bázy kompetentných orgánov.
- kontinuita dôkazov – je potrebná pri ukladaní a následnom vyhľadávaní informácií. Dôkazy musia byť uložené v evidencii takým spôsobom, aby k nim bol jednoduchý a rýchly prístup a zároveň musia byť chránené pred neautorizovaným vstupom.
- zobrazovanie údajov – súvisí s ukladaním údajov do evidencií a ich následným zobrazovaním tak, aby boli zachované v určitej procesnej podobe.
- sieťová architektúra – databázové systémy, kam sa ukladajú nie len dôkazy, ale aj iné dôležité informácie musia mať jasnú a bezpečnú štruktúru založenú na oprávneniach a kompetenciách jednotlivých zložiek procesu vyšetrovania. To isté platí aj o celej sieti zariadení, ktoré zabezpečujú optimálny chod celého systému. Táto podmienka platí aj reverzne, to znamená že kompetentné orgány musia mať znalosti o stavbe a štruktúre systémov, z ktorých možno získavať dôkazy a informácie, slúžiace v rámci odhaľovania či objasňovania trestných činov.
- hardware – technická základňa každého systému je založená na kvalitných a spoľahlivých informačno-komunikačných technológiách.
- súborové systémy – tento prostriedok aplikuje do praxe znalosti rôznorodých súborových systémov a ich vzájomnú koreláciu pre dosiahnutie efektívneho narábania a aj získavania dôkazných prostriedkov.
- analýza – ide o komplexnú analýzu štruktúrovaných či neštruktúrovaných dát, ktorej výsledkom je ucelený obraz, informácia či dôkaz použiteľný v trestnom konaní.
- pochopenie nelegálnych postupov – prostriedok slúžiaci na pochopenie štruktúry, významu a postupov, ktoré sú využívané v nelegálnych nástrojoch kyberkriminality a to takým spôsobom, že kompetentný orgán simuluje používanie takýchto nástrojov pre ich lepšie pochopenie.
- programovanie – ide o pochopenie náležitostí v procese programovania programov, aplikácií či webových rozhraní v rôznych programovacích jazykoch za účelom lepšieho a konzistentnejšieho získavania relevantných dôkazných prostriedkov.
- virtualizácia – zahŕňa dôsledné pochopenie stavby, štruktúry, konfigurácie a fungovania virtuálnych nástrojov.
- technické hlásenia – predpokladá znalosti z oblasti informačných a komunikačných technológií za účelom pochopenia technologickej bázy získaných informácií a následného zostavenia reťazca dôkazných prostriedkov.

Pri pohľade na vymenované prostriedky je veľmi dôležité pripomenúť, že sa nejedná o prostriedky, ktoré sú priamo zahrnuté v trestno-procesných normách. Ide o základnú bázu predpokladov a znalostí v súvislosti s riadnym a efektívnym vyšetrovaním trestných činov v kybernetickom prostredí, pričom tieto prostriedky sú používané viacerými subjektmi v rámci procesu odhaľovania, objasňovania a vyšetrovania tohto druhu kriminality. Majú predovšetkým odporúčací charakter v podobe presnej špecifikácie podmienok, kladených najmä na personálne ale aj materiálne zabezpečenie kompetentných orgánov. To isté platí aj pre jednotlivé prvky štruktúry procesných prostriedkov v oboch rovinách a sú aplikovateľné aj pre inštitút agenta v rámci nevyhnutnosti teoretických a praktických vedomostí a zručností v kybernetickom prostredí.

Pôsobenie agenta vo virtuálnom priestore vyžaduje koreláciu so špecifikami tohto prostredia, ako aj definovanie základných rozdielov medzi agentom pôsobiacim v reálnom kriminálnom prostredí a agentom vykonávajúcim svoju činnosť v kybernetickom prostredí. Môžeme hovoriť o niekoľkých špecifických diferenciáciách:

- anonymita – kybernetické prostredie a jeho platformy poskytujú jeho používateľom najmä v on-line prostredí (web stránky, sociálne siete, diskusné fóra) vysokú mieru anonymity, nakoľko v tomto prostredí subjekt nie je fyzicky prítomný a žiadny z nástrojov virtuálneho priestoru nemôže reálne donútiť používateľa vystupovať pod svojimi osobnými údajmi, ktoré sú priamou cestou k identifikácii osoby, využívajúcej nástroje tohto prostredia.¹⁸ V tejto súvislosti možno z pohľadu použitia agenta hovoriť ako o výhode, nakoľko nie je potrebné vytvárať zložité „krytie subjektu“ v tomto prostredí, nakoľko virtuálne prostredie samo o sebe zabezpečuje viacero možností vytvorenia hodnoverného krytia bez nutnosti fyzických predispozícií agenta.
- virtuálny kontakt – pri „klasickom“ použití agenta ide o infiltráciu osoby do kriminálneho prostredia s reálnym kontaktom s kriminálne podozrivými osobami za účelom získavania a zhromažďovania informácií, pričom ide o zložitý proces výberu vhodného subjektu agenta, vytvárania jeho legendy a krytia. V kybernetickom prostredí ide o výsostne nefyzický kontakt, pričom agent prichádza do styku s kriminálne podozrivými osobami a s kybernetickým prostredím len v rovine virtuálnej bez nevyhnutnosti odhalenia svojej fyziognómie, mimiky, gestikulácie a podobne. Je tu preto minimálna šanca odhalenia agenta, nakoľko na agenta nemusia byť kladené také vysoké nároky a podobne. Virtuálny kontakt takisto neprenáša emócie pri komunikácii, respektíve pri získavaní relevantných informácií, agent nemusí v prostredí pôsobiť sám a svoje výsledky môže tak prezentovať v reálnom čase kompetentnej osobe. Virtuálny kontakt takisto zabezpečuje rozmanitosť vytvárania legendy, kde pri jednotlivých znakoch môžu byť použité rôznorodé informácie, ktoré zabezpečia jeho efektívne krytie.
- možnosť použitia viacerých legiend – aj napriek tomu, že agent v kybernetickom prostredí vystupuje v prevažnej miere anonymne, nie je možné nespomenúť nutnosť vytvorenia legendy, pričom čím sofistikovanejšiu trestnú činnosť odhaľuje, tým kvalitnejšia musí byť aj jeho legenda. Vychádzajúc z uvedených skutočností, vo virtuálnej realite agent nemusí disponovať len s jednou legendou, ale môže mať vytvorených viacero legiend, ktoré môže účinne používať podľa potreby bez rizika odhalenia. V praktickej rovine však agent musí disponovať dostatočnými vedomosťami a technickými zručnosťami v ovládaní nástrojov používaných v kybernetickom priestore, aby implementácia viacerých legiend nebola kontraproduktívna a zmaťová. Výhodou použitia viacerých legiend je aj možnosť nasadiť

¹⁸ LI, X.: *Phenomenal exploration into impact of anonymity on law and order in cyberspace*, In.: *Kriminologija i socijalna integracija*, 2014, číslo 22, s. 106.

inú než zaužívanú legendu namiesto takej, ktorá bola odhalená, respektíve hrozí riziko jej odhalenia.

- pôsobenie bez obmedzenia priestoru a času – „virtuálny agent“ pôsobí v prostredí, ktoré nemá reálne hranice a trestná činnosť mnohokrát presahuje hranice aj niekoľkých štátov. Rovnako prebieha neobmedzene v čase, preto je potrebné vytvoriť také podmienky pre pôsobenie agentov v tomto kybernetickom prostredí, ktoré budú na tieto reálie reflektovať v teoretickej, legislatívnej ako aj technickej rovine.
- špecifické predispozície – od samotnej osoby agenta v kybernetickom prostredí je potrebné vyžadovať určité teoretické ako aj praktické technické vedomosti z oblasti informačných a komunikačných technológií, nakoľko v kybernetickom priestore musí vystupovať profesionálne, musí vedieť, akým spôsobom, kedy a kde vyhľadávať a získavať potrebné informácie, akým spôsobom sa infiltrovať do kriminálneho prostredia a podobne.
- využitie prostredia – virtuálna realita ponúka nespočetné množstvo nástrojov, možností, aplikácií a prostriedkov, pomocou ktorých je možné získavať informácie, alebo sa dostať do určitých komunít a skupín, kde sa takéto informácie nachádzajú. Agent v takomto prostredí by mal bezpodmienečne ovládať tieto nástroje a používať ich vo svoj prospech.

Pri pohľade na špecifiká pôsobenia agenta v kybernetickom prostredí možno povedať, že pôsobenie takéhoto subjektu nevykazuje legislatívne znaky definície agenta, nakoľko použitie tohto inštitútu v kybernetickom prostredí si nevyžaduje tak náročné zázemie a legislatívnu ochranu, ako je to v prípade nasadenia agenta v reálnom prostredí. Je však dôležité pripomenúť, že postavenie a úlohy agenta upravuje priamo zákon, ktorý však nemôže upraviť použitie tohto procesného prostriedku v tom ktorom konkrétnom prostredí. Znamená to, že použitie agenta v kybernetickom prostredí nie je explicitne upravené určitou právnou normou, pričom špecifickým nie je jeho samotné použitie, ale skôr pôsobenie v tomto kybernetickom prostredí.

Teoretické východiská použitia agenta pri konkrétnej trestnej činnosti

Použitie inštitútu agenta v trestnom konaní nie je len teoretickým použitím prostriedku operatívno-pátracej činnosti, ale praktickým nasadením takých síl a prostriedkov, ktoré účinne a efektívne bojujú proti samotnej trestnej činnosti. Ak zoberieme do úvahy použitie agenta v kybernetickom prostredí, je rovnako dôležité poukázať na konkrétne druhy kriminality, alebo trestnej činnosti, v ktorých môže byť takýto postup efektívny:

- kriminalita na sociálnych sieťach – prostredie sociálnych sietí poskytuje široké spektrum možností páchania trestnej činnosti, najmä nebezpečného prenasledovania, rôznych druhov kyberšikany či cybergroomingu.¹⁹ Inštitút agenta v tomto prípade môže účinne napomôcť odhaliť latentné prejavy kriminality, nakoľko táto sa vo väčšine prípadov realizuje v uzavretom kruhu používateľov.
- výroba a distribúcia detskej pornografie – je to jeden z najhorších druhov kriminality, ktorej objasňovanie a vyšetrovanie musí neustále reagovať na nové spôsoby jej páchania a utajovania.²⁰ Použitie agenta je v tomto prípade na mieste, aj keď je náročné, nakoľko komunity, ktoré distribuujú alebo vyrábajú detskú pornografiu, sú prísne uzavreté a možná infiltrácia zahŕňa v sebe rôzne spôsoby overovania dôveryhodnosti a podobne. Samotný

¹⁹ Cybergrooming (tiež grooming alebo child grooming) je metódou tzv. predátorov alebo groomerov, ktorí pod falošnou alebo pozmenenou identitou za použitia určitých psychologických metód vylákajú na fiktívne, zväčša tajné stretnutie dieťa a následne zneužívajú, unesú alebo inak nelegálne vplývajú na dieťa.

²⁰ VENDIUS, T.: *Proactive Undercover Policing and Sexual Crimes against Children on the Internet*, In: The European Review of Organised Crime, 2015, číslo 2, s. 8.

zber relevantných informácií je potom jednoduchší, nakoľko na portáloch či webstránkach s týmto obsahom je dostatok dôkazového materiálu, avšak páchatelia tejto trestnej činnosti mnohokrát vystupujú pod skrytou identitou, ktorá je ťažko vystopovateľná.

- organizovaná kriminalita – pri tomto druhu trestnej činnosti pôjde najmä o stopovanie a zhromažďovanie údajov a informácií z transakcií finančných tokov za nelegálne zbrane a drogy. Nesmieme však zabudnúť, že do tejto kategórie patrí aj obchod s bielym mäsom, pričom použitie agenta v tomto smere predpokladá odhaľovanie podvodných pracovných agentúr, zhromažďovanie informácií o komunikácii obetí s páchatelmi a ďalšie nevyhnutné úkony. Veľká časť aktivít organizovaných skupín prechádza postupne do prostredia virtuálnej reality, nakoľko anonymita a vysoká miera latencie robia takúto kriminalitu sofistikovanejšou a efektívnejšou.
- Hacking – pojmom hacking sa označuje akákoľvek činnosť osoby smerujúca k nelegálnemu prístupu k cudziemu počítačovému systému.²¹ Vývoj informačných a komunikačných technológií však priniesol pre osoby hackerov viacero možností zneužitia počítačových systémov, pričom vzniklo aj viacero pojmov v oblasti hackingu ako takého. Hackerov môžeme rozdeliť do viacerých skupín, z ktorých najvýznamnejšie sú „whitehat hackeri“, ktorí vykonávajú svoju činnosť za účelom odhalenia bezpečnostných chýb napadnutého systému a „blackhat hackeri“ ktorí svoju činnosť zameriavajú na priame získavanie citlivých informácií z informačných systémov. Inštitút agenta v tomto prípade predpokladá infiltráciu do skupín hackerov, ktorí napádajú informačné systémy za účelom osobného a finančného prospechu. Opäť však treba zdôrazniť a dať na prvé miesto podmienku, že takýto agent musí disponovať náležitými vedomosťami a zručnosťami v oblasti hackovania informačných systémov aby sa nie len v určitej komunite osvedčil, ale aj aby vedel efektívne získavať relevantné informácie.

Kazuistika²²

Zlom v celosvetovom fenoméne krádeží identity a foriem vydierania, ktoré spôsobili škodu za viac ako 50 miliónov amerických dolárov, prišiel v roku 2013, keď sa bývalý agent tajnej služby USA Michael Adams rozhodol, že sa pokúsi odhaliť interné fungovanie organizácie Carder.su, ktorá bolo federálnou vládou označená ako Rusmi vedený zločinecký syndikát v kyberpriestore s viac ako 7 800 členmi.

Michael Adams začal vo virtuálnom priestore používať nickname (prezývku) človeka, ktorý použil v marci roku 2007 falošnú kreditnú kartu vo Whole Foods v meste Henderson. Išlo o prezývku „Celtic“ a pod touto identitou začal štyri a pol ročné vyšetrovanie, ktorého súčasťou boli konverzácie, online chatovanie, e-maily a pohyby finančných prostriedkov medzi používateľmi stránky Carder.su. Táto webstránka bola v princípe trhoviskom, kde zainteresovaní používatelia predávali a kupovali napríklad falošné vodičské preukazy, údaje z cudzích kreditných kariet či informácie o osobných údajoch iných ľudí a ich prístupových právach do určitých elektronických systémov, pričom samotní používatelia si tu dávali cenné rady o tom, ako sa vyhnúť trestno-právnym dôsledkom svojich činov.

Samotná webová stránka mala zabezpečené prihlasovanie, čo je priam ironické pre organizáciu, ktorej jednou z činností bola krádež osobných identifikačných údajov a týmto zabezpeče-

²¹ KOLOUCH, J.: Cybercrime, 2016, Praha, s. 269.

²² Undercover agent outlines \$50 million cybercrime scheme [cit. 2017-02-22] Dostupné na internete: <<http://www.reviewjournal.com/news/undercover-agent-outlines-50-million-cybercrime-scheme>>.

ním chceli správcovia tejto webovej stránky udržať celý projekt v tajnosti a zároveň podporovať obchod s odcudzeným „virtuálnym tovarom“ len medzi dôveryhodnými a overenými používateľmi. Organizácia vyvinula overovací proces pre predajcov, ktorý v sebe zahŕňal určitú formu záruky za predajcu inými používateľmi. Ak nebol predajca overený, tak správcovia systému prišli s určitou formou trestu, respektíve jeho vylúčenia z komunity v podobe negatívnych recenzií na profile používateľa, zmazanie účtu alebo zverejnenie identity kupujúceho alebo predávajúceho v on-line režime a priestore a to aj mimo spoločnosti Carder.su.

Michael Adams sa nakoniec stal predajcom a začal pracovať v utajení, pričom ostatným používateľom dodával falošné vodičské preukazy z Nevady, Virgínie, Gruzínska, Illinois, New Yorku alebo Tennessee. Adams následne prezentoval dôkazy v podobe komunikácie prostredníctvom e-mailu medzi ním ako „Celticom“ a Davidom Camezom z Phoenixu, ktorý si kúpil falošný vodičský preukaz z Nevady v roku 2009. Camezov právnik z Las Vegas Chris Rasmussen a aj federálny prokurátor súhlasil s dôkazmi, že Camez používa on-line prezývky „Bad Man“ alebo „Doctorsex“, ktoré boli zahrnuté v komunikácii s Michaelom Adamsom, pričom však išlo len o malého hráča vo veľkom prípade. Camezov spoluobžalovaný, 29-ročný Alexander Kostyukov z Miami sa v novembri 2013 priznal k účasti na organizácii vydierania, ako aj k výrobe a obchodovaniu s falošnými identifikačnými dokladmi.

V obžalobe sú identifikovaní aj dvaja muži, označení ako lídri portálu spoločnosti Carder.su a to Konstantin Lopatin s prezývkou „Graf“ a Roman Zolotarev ako „admin“, pričom obžaloba predpokladá aj existenciu tretieho správcu uvedenej webstránky, ktorého však pozná iba pod prezývkou „Maxxtro“. Tieto osoby sú v súčasnosti stále na slobode, pričom na Lopatina je vypísaná odmena jeden milión amerických dolárov a na Zolotareva dva milióny amerických dolárov.

Prípád Michaela Adamsa ako agenta v kybernetickom prostredí je jedným z prvých, no určite nie posledným prípadom, keď osoba v utajení odhalila kriminálnu sieť a zhromaždila veľké množstvo cenných dôkazov, ktoré slúžili vo vyšetrovaní závažnej trestnej činnosti.

Záver

Kybernetické útoky sú čoraz bežnejšie, nebezpečnejšie a prepracovanejšie. Naša spoločnosť je terčom páchatelov, ktorých útoky smerujú do komplexnej kritickej infraštruktúry, vrátane súkromného i verejného sektora. Narastajú útoky na obchodné spoločnosti zamerané na obchodné tajomstvo a iné citlivé firemné údaje. Na občanov sa špecializujú podvodníci a zloději identity a na deti dopadajú protiprávne aktivity prostredníctvom on-line komunikácie. To znamená, že je potrebné zvýšiť možnosti použitia agenta v kybernetickom prostredí v súvislosti s elimináciou protiprávných zásahov do štátnych a súkromných počítačových sietí. Na zreteli však treba mať skutočnosť, že agent sa neustále pri svojej činnosti pohybuje na hranici zákona a zločinu a mohol by ľahko nadobudnúť presvedčenie, že mu je všetko dovolené. Jeho konanie preto musí byť limitované určitými zásadami, ktoré musia byť pri jeho použití rešpektované. Musí sa riadiť zásadou zákonnosti čo znamená že jeho konanie musí byť v súlade s účelom Trestného poriadku a musí byť úmerná protiprávnosť na odhaľovanie, zisťovanie alebo usvedčovanie, ktorého sa zúčastňuje.

Musíme si uvedomiť aj ten fakt, že boj s kriminalitou v kybernetickom prostredí musí byť prioritou. Vzhľadom na skutočnosť že informačno-komunikačné technológie budú mať dopad na všetky činnosti ktoré vykonávame. Pri pohľade na tento druh kriminality si všetci musíme priznať, že je tu kyberpriestor, sociálny a digitálny prvok, ktorý je obsiahnutý v každom skutku

v rámci trestnej činnosti v tomto priestore. Rovnako je potrebné zlepšiť komunikáciu so súkromným sektorom a poskytovateľmi internetových služieb nakoľko tento vzťah je kľúčom v boji proti tejto kriminalite. Súkromný sektor sa skladá z 80 % používateľov internetových služieb a bez tejto spolupráce nemôže byť odhaľovanie a objasňovanie týchto trestných činov úspešné.

Je zrejme že orgány činné v trestnom konaní sú stále v počiatočných fázach vo vývoji komplexných stratégií v boji proti tomuto fenoménu ale reagujú a snažia sa predchádzať kriminalite v kybernetickom prostredí. Cieľom je však urobiť také opatrenia, aby každý príslušník Policajného zboru vedel ako má reagovať na výzvu v tomto boji.

Literatúra

- BROWN, C.: *Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice*, In: International Journal of Cyber Criminology, 2015, číslo 9, 119 s.
- GRAYCAR, A.: *New crimes or new responses*, 2001, Australian institute of criminology, 13 s.
- HUDEČ, L.: Bezpečnostné požiadavky na zariadenia pre elektronický podpis. s. 7 [cit. 2017-02-16] Dostupné na internete: <www.lnd.sk/hudec2003-1.rtf>.
- KOLOUCH, J.: *Cybercrime*, 2016, Praha, 528 s.
- LI, X.: *Phenomenal exploration into impact of anonymity on law and order in cyberspace*, In.: Kriminologija i socijalna integracija, 2014, číslo 22, s. 102–123.
- REMETA, R.: *Výsluch agenta*, In: Policajná teória a prax, 2013, číslo 4, s. 108–120.
- ŠALMÍK, M.: *Kriminalita na sociálnych sieťach*, Diplomová práca, 2014, Akadémia PZ v Bratislave, 90 s.
- VENDIUS, T.: *Proactive Undercover Policing and Sexual Crimes against Children on the Internet*, In: The European Review of Organised Crime, 2015, číslo 2, s. 6–24.
- Undercover agent outlines \$50 million cybercrime scheme [cit. 2017-02-22] Dostupné na internete: <<http://www.reviewjournal.com/news/undercover-agent-outlines-50-million-cybercrime-scheme>>.
- Národní centrum kybernetické bezpečnosti. Výkladový slovník kybernetické bezpečnosti – třetí vydání [cit. 2015-12-11] Dostupné na internete: <<http://www.govcert.cz/cs/informacni-servis/vykladovy-slovník/>>.
- PC Magazine [cit. 2017-02-11] Dostupné na internete: <<http://www.pcmag.com/encyclopedia/term/44936/information-assurance>>.
- PC Magazine [cit. 2017-03-03] Dostupné na internete: <<http://www.pcmag.com/encyclopedia/term/40643/cybersecurity>>.
- Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020, Rokovania vlády Slovenskej republiky [cit. 2017-03-09] Dostupné na internete: <<http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=24702>>.
- Web noviny, Hlavné správy, Vláda prijala Koncepciu Kybernetickej bezpečnosti Slovenska na roky 2015 – 2020 [cit. 2017-03-10] Dostupné na internete: <<http://www.hlavnespravy.sk/vlada-prijala-koncepciu-kybernetickej-bezpecnosti-slovenska-na-roky-2015-2020/633726>>.
- Zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov.

Prípustnosť využitia dôkazov získaných použitím informačno-technických prostriedkov pre účely trestného konania¹

Admissibility of Evidence Obtained by the Use of Information Technology for the Purposes of Criminal Proceeding

Peter Polák²

Marek Talapka³

Abstrakt: Problematika uplatňovania informačno-technických prostriedkov v trestnom konaní je vzhľadom na ich účel, náročné právne podmienky ich použitia a využitia, ako aj vzhľadom na pozitívne výsledky pre dokazovanie v trestnom konaní, stále v centre záujmu odbornej a laickej verejnosti. Použitie informačno-technických prostriedkov v trestnom konaní je spojené so zásahom do garantovaných ľudských práv a slobôd. Z tohto dôvodu ide o neštandardné procesné postupy získavania informácií pre účely trestného konania. Preto v súvislosti s použitím informačno-technických prostriedkov objektívne existujú otázky o prípustnosti a zákonnosti získavania dôkazov. V poslednom čase sú to aj otázky spojené s prípustnosťou využitia dôkazov získaných zo súkromných záznamov. Príspevok na tieto problémy reaguje a v niektorých prípadoch ponúka aj ich riešenia.

Abstract: Due to the purpose, challenging legal conditions of use, moreover with respect to positive results for evidence in criminal proceedings, topic of information technical means in criminal proceedings stands in center of interest of expert and laic public. Use of information technical means in criminal proceedings is associated with interference to guaranteed human rights and freedoms. As such, it is non-standard procedure of obtaining information for purposes of criminal proceedings. Therefore in connection with the objective use of information technical means, questions about their legality and admissibility arise. Recently also questions related to the use of admissibility of evidence obtained from private records arise. This article reacts on these issues and in some cases also offers their solutions.

Kľúčové slová: dokazovanie, zákonnosť a prípustnosť dôkazov, informačno-technické prostriedky, informácie získané informačno-technickými prostriedkami ako dôkaz, informácie získané zo súkromných záznamov ako dôkaz

Keywords: evidence, the legality and admissibility of evidences, information and technical resources, information obtained by information and technical resources as evidence, information obtained from private records as evidence.

Úvod

Dokazovanie v trestnom konaní je popri rozhodovaní najdôležitejšou procesnou činnosťou orgánov činných v trestnom konaní a súdov, nakoľko umožňuje zistiť skutkový základ pre ich rozhodovanie ako aj pre ďalší potup v trestnom konaní tak, aby mohol byť naplnený účel trestného konania, ktorým je aby trestné činy boli náležite zistené a ich páchatelia podľa zákona spravodli-

¹ Tento príspevok je podporovaný Agentúrou na podporu výskumu a vývoja na základe Zmluvy č. APVV-15-0644.

² Doc. JUDr. Peter Polák, PhD., Ústav verejného práva, Fakulta práva Paneurópskej vysokej školy, Tomášikova 20, 821 02 Bratislava, peter.polak@paneurouni.com.

³ JUDr. Marek Talapka, Interný doktorand Ústavu verejného práva, Fakulta práva Paneurópskej vysokej školy, Tomášikova 20, 821 02 Bratislava, marek.talapka@paneurouni.com.

vo potrestaní. Nezastupiteľnosť dokazovania predovšetkým spočíva v tom, že ide o jedinú cestu, ktorou si orgány činné v trestnom konaní a súdy môžu a musia obstarat' skutkový podklad pre svoje rozhodnutie, prípadne pre iný postup v trestnom konaní. Trestné konanie sa vedie o skutku, ktorý sa stal v minulosti, a ktorý orgán činný v trestnom konaní ako aj súd osobne nepozoroval. Preto sa s ňou môže oboznámiť len nepriamo tým, že si jej priebeh zrekonštruuje pomocou vykonaných dôkazov. Trestný poriadok v ustanovení § 119 ods. 2 demonštratívne uvádza dôkazné prostriedky, medzi ktorými sú okrem iných aj práve informácie získané použitím informačno-technických prostriedkov.

1. Všeobecne o prípustnosti a zákonnosti dôkazov

S problematikou dokazovania, ako aj s informáciami získaných použitím informačno-technických prostriedkov úzko, súvisí prípustnosť a zákonnosť dôkazov. Možno uviesť, že v literatúre často dochádza k zamieňaniu týchto pojmov. Dôvodom môže byť, že vyššie uvedené pojmy sú späté, previazané, vládne medzi nimi organická väzba a rozlíšenie medzi týmito pojmi nenasáva vždy, alebo iba v závislosti od konkrétnych procesných situácií.

Mather⁴ používa oba termíny, avšak ich nestotožňuje, aj keď súhlasí, že nezákonný dôkaz je neprípustný. K podobnému záveru dochádza aj Nett,⁵ ktorý zdôrazňuje, že „nezákonný dôkaz je vždy neprípustný.“ Burda⁶ zdôrazňuje, že „nezákonne získaný dôkaz nemôže byť v zásade prípustný v trestnom konaní, pokiaľ jeho nezákonnosť nie je odstrániteľná a následne i odstránená (tzv. relatívne neúčinné dôkazy)“. Možno ešte uviesť, že Syrový pripúšťa za určitých okolností aj použitie nezákonne získaného dôkazu, pričom uvádza, že ustanovenie § 119 ods. 4 Trestného poriadku „vyklúčuje prípustnosť dôkazu získaného nezákonným spôsobom, ale nie každého. Nezákonnosť dôkazu musí byť daná súčasne s donútením alebo s hrozbou donútenia. Samotná nezákonnosť preto a priori nevylučuje prípustnosť dôkazu.“⁷

Šimovček⁸ uvádza, že prípustnosť dôkazu znamená, že určitý element dokazovania je spôsobibilý na základe práva podporiť resp. vyvrátiť určité tvrdenia alebo nároky a sudca ho nemôže a priori odmietnuť. Prípustnosť dôkazu vychádza z práva na spravodlivý proces, ktoré je garantované v čl. 6 Európskeho dohovoru o ochrane základných práv a slobôd. Prípustnosť dôkazu je potrebné hodnotiť vzhľadom na jeho povahu, ako aj vzhľadom na spôsob jeho zaobstarania. Šimovček zároveň zdôrazňuje, že dôležitým kritériom prípustnosti dôkazu je zákonnosť jeho získania.

Na základe vyššie uvedeného možno konštatovať, že prípustnosť dôkazu je pojem, ktorý je významovo širší ako zákonnosť dôkazu, nakoľko každý nezákonne získaný dôkaz je neprípustný, ale nie každý neprípustný dôkaz je nezákonný. Podľa Šimovčeka⁹ neprípustnosť je považovaná za širší pojem, ktorý v sebe zahŕňa nie len neprípustnosť vyplývajúcu z nezákonného dôkazu, ale aj neprípustnosť danú prameňom dôkazu a neprípustnosť z formálneho dôvodu časovej preklúzie predloženia dôkazov procesnými stranami na súd.

⁴ MATHERN, V.: Dokazovanie v československom trestnom procese. Bratislava: Obzor, 1984, s. 107.

⁵ NETT, A.: Plody z otráveného stromu. 1. vydání. Brno: Masarykova univerzita, 1997, s. 9, 45.

⁶ BURDA, E.: Teoretické a praktické problémy dokazovania. Zborník príspevkov z celoštátnej konferencie s medzinárodnou účasťou konanej dňa 15. decembra 2008. Bratislava: BVŠP, 2008, s. 23.

⁷ SYROVÝ, I.: Použitie nezákonne získaného dôkazu v trestnom konaní; Bulletin slovenskej advokácie, č. 3/2007, s. 7–14.

⁸ ŠIMOVIČEK, I.: Teoretické a praktické problémy dokazovania. Zborník príspevkov z celoštátnej konferencie s medzinárodnou účasťou konanej dňa 15. decembra 2008. Bratislava: BVŠP, 200, s. 255.

⁹ ŠIMOVIČEK, I.: Teoretické a praktické problémy dokazovania. Zborník príspevkov z celoštátnej konferencie s medzinárodnou účasťou konanej dňa 15. decembra 2008. Bratislava: BVŠP, 200, s. 255.

Podľa teórie prípustnosť dôkazu je nevyhnutná vlastnosť dôkazu, ktorá je charakterizovaná predovšetkým:

- súladom medzi ustanoveniami Trestného poriadku, základnými zásadami trestného konania a prameňmi resp. nositeľmi dôkazov,
- súladom medzi ustanoveniami Trestného poriadku, základnými zásadami trestného konania a metódami, prostriedkami a postupmi použitými na získanie informácií tvoriacich obsah dôkazu.¹⁰

Pokiaľ ide o súlad s ustanoveniami Trestného poriadku, základnými zásadami trestného konania a prameňmi dôkazov, rozumie sa tým predovšetkým dodržanie zásady stíhania len zo zákonných dôvodov v zmysle ustanovenia § 2 ods. 1 Trestného poriadku. V prípade súladu s ustanoveniami Trestného poriadku, základnými zásadami trestného konania a metódami, prostriedkami a postupmi slúžiacimi na získavanie informácií tvoriacich obsah dôkazov sa vychádza opäť zo zásady stíhania len zo zákonných dôvodov v zmysle § 2 ods. 1 Trestného poriadku, v zmysle ktorej na získanie dôkazu je možné použiť len také metódy, prostriedky alebo postupy, ktoré sú v medziach a v súlade s ustanoveniami Trestného poriadku. Prípadne zvolená metóda, prostriedok alebo postup teda nesmie odporovať ustanoveniam Trestného poriadku a zároveň ani ho nijako obchádzať.

Aby niektorý dôkaz bol prípustný, pri jeho vyhľadávaní a vykonávaní je potrebné dodržať nasledovné pravidlá:

- znalosť pôvodu prameňa dôkazov, resp. dôkazných informácií a možnosť ich preverenia,
- zistenie totožnosti osôb, od ktorých dôkazné informácie pochádzajú,
- kompetencie subjektov trestného konania na zaobstarávanie dôkazov,
- dodržanie všeobecných procesných pravidiel pre vyhľadávanie a vykonanie dôkazov,
- dodržanie pravidiel pre úplnosť a presnosť zafixovania zaobstarávaných dôkazných informácií.¹¹

Z vyššie uvedených skutočností vyplýva, že v prípade ak by pri vykonávaní dôkazov došlo k porušeniu zákona, nemožno tento dôkaz hodnotiť ako zákonný a tým pádom ani ako prípustný v dôsledku porušenia procesných predpisov, a nemožno ho použiť ani ako dôkaz pre ďalšie štádiá trestného konania, a to ani v tom prípade keby v ňom dosiahnuté tvrdenia boli jednoznačne pravdivé.

Prípustnosť dôkazov zahŕňa v sebe aj znaky vzťahujúce sa na obsah dôkazu a na procesnú formu dôkazu. Ak má byť dôkaz prípustný, tak musí spĺňať zákonom predpísanú formu, ako aj zákonom stanovené obsahové náležitosti, pričom obe tieto požiadavky spolu úzko súvisia a vzájomne sa ovplyvňujú. Forma dôkazu vplýva na úplnosť a presnosť obsahu dôkazu, a obsah na dodržanie určitej procesnej formy.

Možno konštatovať, že súčasný Trestný poriadok používa termín zákonnosť. Podľa § 2 ods. 12 Trestného poriadku *orgány činné v trestnom konaní a súd hodnotia dôkazy získané zákonným spôsobom*. Podľa ustanovenia § 119 ods. 2 Trestného poriadku *za dôkaz môže slúžiť všetko, čo môže prispieť na náležité objasnenie veci a čo sa získalo z dôkazných prostriedkov podľa tohto zákona alebo podľa osobitného zákona*. Osobitným zákonom sa myslí zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov, zákon č. 122/2013 Z. z. o ochrane osobných údajov, zákon č. 171/1993 Z. z. o policajnom zbore, zákon č. 473/2005 Z. z. o poskytovaní služieb v oblasti súkromnej bezpečnosti a o zmene a doplnení niektorých zákonov. Charakter osobitného zákona v zmysle ustanovenia § 119 ods. 2 má

¹⁰ IVOR, J. a kol.: Trestné právo procesné. Druhé, doplnené a prepracované vydanie. Bratislava: Iura Edition, 2010, s. 443.

¹¹ ZÁHORA, J. a kol.: Dokazovanie v trestnom konaní. 1. vydanie. Praha: Leges, 2013, s. 116.

aj zákon č. 1/2014 o organizovaní verejných športových podujatí. Podľa § 243 ods. 4 Trestného poriadku *pri predbežnom prejednaní obžaloby súd preskúma obžalobu a zákonnosť dôkazného materiálu.*

Zákonnosť dôkazu znamená, že dôkaz bol získaný z dôkazného prostriedku, ktorý je prípustný podľa zákona a zároveň že dôkaz bol získaný postupom orgánu činného v trestnom konaní a súdu, ktorý je v súlade s právnymi predpismi. V prípade, ak pri získavaní a použití dôkazov neboli dodržané právne predpisy, resp. neboli v súlade s právnymi predpismi, nasledujú dôsledky porušenia predpisov dokazovania v trestnom konaní, t. zn. dôkaz, ktorý bol získaný protiprávne je nezákonný. „Za dôkaz, ktorý bol získaný nezákonným spôsobom, sa považuje nielen dôkaz, pri ktorom bola nezákonnosť spôsobená, ale aj každý dôkaz získaný na základe takéhoto dôkazu.“¹² To znamená, že nezákonnosťou sú postihované aj všetky ďalšie dôkazy, ktoré boli získané na základe nezákonného postupu. Vzhľadom na to nemožno preto použiť ani ďalšie dôkazy, ktoré boli získané či už priamo alebo nepriamo, ako výsledok nezákonného postupu. Dôkazy, ktoré sú získané nezákonným zásahom do ústavných práv fyzických osôb sú v trestnom konaní nepoužiteľné, nakoľko nespĺňajú podmienky ustanovené v § 119 ods. 2 Trestného poriadku.

Zákonnosť dôkazu predstavuje vlastnosť dôkazu, ako aj otázku hodnotenia dôkazu. V prípade hodnotenia dôkazov z hľadiska ich zákonnosti vychádza teória z koncepcie konfliktu záujmu a hodnoty dôkazu. V prípade otázky účinnosti sa rieši pomocou skúmania hodnoty dôkazov, za ktorú sa považuje aj zákonnosť.

Repík¹³ zdôrazňuje päť kritérií zákonnosti dôkazu, ktorými sú:

- či bol dôkaz získaný z prameňa, ktorý stanoví prípadne pripúšťa zákon,
- či bol dôkaz získaný a vykonaný procesným subjektom k tomu zákonom oprávneným,
- či bol dôkaz získaný a vykonaný v tom procesnom štádiu, v ktorom je príslušný procesný subjekt podľa zákona oprávnený vyhľadávať a vykonávať dôkazy v procesnom zmysle, t. zn. také dôkazy, ktoré môžu byť podkladom pre rozhodnutie v trestnom stíhaní najmä pre rozhodnutie súdu,
- či sa získaný a vykonaný dôkaz týka predmetu dokazovania v danom procese, t. zn. či sa týka skutku, o ktorom sa vedie konanie prípadne otázok, o ktorých je potrebné podľa zákona v súvislosti s týmto skutkom rozhodovať,
- či bol dôkaz získaný a vykonaný spôsobom, ktorý stanovuje, prípadne pripúšťa zákon.

Na základe vyššie uvedených kritérií je zákonnosť dôkazu potom určená prameňom dokazovania, subjektom dokazovania, štádiom konania, v ktorom sa dokazovanie vykonáva, predmetom dokazovania a spôsobom dokazovania. Zákonnosť dôkazu sa však v zásade redukuje len na zákonnosť spôsobu jeho získania a vykonania.¹⁴

Ako už bolo vyššie uvedené, pojem prípustnosť dôkazu znamená, že určitý element dokazovania je spôsobilý na základe práva podporiť resp. vyvrátiť určité tvrdenia alebo nároky a sudca ho nemôže a priori odmietnuť. Možno spomenúť, že Trestný poriadok všeobecne nevymedzuje pravidlá pre prípustnosť dôkazov. Ustanovenie § 119 ods. 2 Trestného poriadku stanovuje pravidlo, že za dôkaz môže slúžiť všetko, čo môže prispieť na náležité objasnenie veci a čo sa získalo z dôkazných prostriedkov podľa tohto zákona alebo podľa osobitného zákona. Na druhej strane možno konštatovať, že niektoré právne normy, medzinárodné zmluvy alebo rozhodovacia činnosť stanovuje určité limity pre prípustnosť dôkazov.

¹² ZÁHORA, J. a kol.: Dokazovanie v trestnom konaní. 1. vydanie. Praha: Leges 2013, s. 114.

¹³ REPÍK, B.: Procesní důsledky porušení předpisů o dokazování v trestním řízení; Bulletin advokacie, 1982, červenec – srpen, s. 122.

¹⁴ NETT, A.: Plody z otráveného stromu. 1. vydání. Brno: Masarykova univerzita, 1997, s. 44.

Niektoré medzinárodné zmluvy priamo vylučujú použitie dôkazov, ktoré boli získané mučením. Dohovor proti mučeniu a inému krutému, neľudskému alebo ponižujúcemu zaobchádzaniu alebo trestaniu výslovne zakazuje použitie dôkazu, ktorý bol získaný mučením. Článok 15 Dohovoru uvádza, že každý štát, ktorý je zmluvnou stranou tohto Dohovoru zabezpečí, aby sa žiadne vyhlásenie, ktoré sa podľa zistenia urobilo v dôsledku mučenia, nepoužilo ako dôkaz v žiadnom súdnom konaní, s výnimkou prípadov, keď sa použije proti osobe obvinenej z mučenia, ako dôkaz o tom, že sa toto vyhlásenie urobilo.

V Rímskom štatúte Medzinárodného trestného súdu v čl. 69 ods. 7 sa výslovne uvádza, že dôkazy, ktoré boli získané porušením tohto štatútu alebo porušením medzinárodne uznávaných ľudských práv, sú neprípustné v prípade, ak porušenie vrhá vážne pochybnosti na spoľahlivosť dôkazov alebo pripustenie dôkazu by bolo v rozpore s bezúhonnosťou konania a mohlo by ju vážne ohroziť.

Z pohľadu judikatúry Európskeho súdu pre ľudské práva možno spomenúť, že Dohovor o ochrane ľudských práv a základných slobôd dokazovanie ako také neupravuje, avšak sa dotýka priamo len niektorých jeho aspektov. V súvislosti s prípustnosťou dôkazov Európsky súd pre ľudské práva viackrát zdôraznil, že Európsky dohovor neupravuje prípustnosť dôkazu ako takú a uvedená otázka spadá do pôsobnosti vnútroštátneho práva. Európsky súd pre ľudské práva ďalej konštatoval, že znenie čl. 6 ods. 1 Dohovoru nestanovuje žiadne pravidlá prípustnosti dôkazu a úlohou súdu je len stanoviť, či konanie ako celok bolo spravodlivé. Avšak možno dodať, že aj napriek tomu, že Európsky súd pre ľudské práva sa odmieta zaoberať otázkou prípustnosti dôkazov, vo viacerých prípadoch priamo vyslovil, že použitie určitého dôkazu voči obvinenému porušilo jeho právo na spravodlivý proces.¹⁵

Na záver možno ešte uviesť, že Trestný poriadok v ustanovení § 119 ods. 2 Trestného poriadku nedovoľuje vylúčiť uplatnenie žiadneho dôkazného prostriedku získaného v súlade so zákonom, avšak na druhej strane v niektorých prípadoch výslovne zakazuje použitie niektorých dôkazov. Možno spomenúť prípady, ktorými sú:

- získanie dôkazu nezákonným donútením alebo hrozbou donútenia podľa § 119 ods. 4, § 121 ods. 1 a 2, § 123 ods. 2 Trestného poriadku,
- získanie dôkazu o kontrolovanej dodávke, sledovanie ktorej bolo vykonané bez príkazu príslušného orgánu, ak nebol príkaz v stanovenej lehote vydaný podľa § 111 ods. 4 Trestného poriadku,
- získanie dôkazu pri predstieranom prevode bez príkazu príslušného orgánu, ak nebol príkaz v stanovenej lehote vydaný podľa § 112 ods. 5 Trestného poriadku,
- komunikácia medzi obhajcom a obvineným pri sledovaní osôb a vecí, pri vyhotovovaní obrazových, zvukových alebo obrazovo-zvukových záznamov, pri odpočúvaní a zaznamenávaní telekomunikačnej prevádzky podľa § 113 ods. 3, § 114 ods. 4, § 115 ods. 1 Trestného poriadku,
- získanie dôkazu pri sledovaní osôb a vecí bez príkazu príslušného orgánu, ak takýto príkaz nebol v stanovenej lehote vydaný podľa § 113 ods. 7 Trestného poriadku,
- využitie dôkazu získaného sledovaním osôb a vecí v inej trestnej veci, ako je tá, v ktorej bolo sledovanie vykonané, možno záznam ako dôkaz použiť len vtedy, ak sa súčasne aj v tejto veci vedie trestné konanie pre úmyselný trestný čin podľa § 113 ods. 9 Trestného poriadku,

¹⁵ MOLE, N., HARBY, C.: Právo na spravodlivý proces. Sprievodca na aplikáciu článku 6 Európskeho dohovoru o ľudských právach. Rada Európy 2009, s. 49.

- informácie získané pri vyhotovovaní obrazových, zvukových alebo obrazovo-zvukových záznamov v obydli bez príkazu sudcu pre prípravné konanie podľa § 114 ods. 2 Trestného poriadku,
- využitie dôkazu získaného vyhotovením obrazových, zvukových alebo obrazovo-zvukových záznamov v inej trestnej veci podľa § 114 ods. 7 Trestného poriadku, ako je tá, v ktorej boli vyhotovené obrazové, zvukové alebo obrazovo-zvukové záznamy, možno záznam ako dôkaz použiť len vtedy, ak sa súčasne aj v tejto veci vedie trestné konanie pre úmyselný trestný čin, na ktorý zákon ustanovuje trest odňatia slobody s hornou hranicou trestnej sadzby prevyšujúcou tri roky, korupciu, trestný čin zneužívania právomoci verejného činiteľa, trestný čin legalizácie príjmu z trestnej činnosti alebo pre iný úmyselný trestný čin, o ktorom na konanie zaväzuje medzinárodná zmluva,
- informácie získané pri odpočúvaní a zázname telekomunikačnej prevádzky bez príkazu sudcu pre prípravné konanie podľa § 115 ods. 2 Trestného poriadku,
- využitie dôkazu získaného pri odpočúvaní a zaznamenávaní telekomunikačnej prevádzky v inej trestnej veci podľa § 115 ods. 7 Trestného poriadku,
- využitie dôkazu získaného pri použití agenta v inej trestnej veci podľa § 117 ods. 12 Trestného poriadku,
- využitie informácií pri porovnávaní údajov v informačných systémoch podľa § 118 ods. 4 Trestného poriadku,
- využitie informácií pri porovnávaní údajov v informačných systémoch v inej trestnej veci v zmysle § 118 ods. 7 Trestného poriadku,
- odmietnutie výpovede obvineným podľa § 201 ods. 4 Trestného poriadku,
- využitie vyhlásenia obvineného v konaní o zmieri v ďalšom súdnom konaní podľa § 226 Trestného poriadku,
- využitie priznania obvineného v konaní o vine a treste na hlavnom pojednávaní podľa § 333 ods. 4 Trestného poriadku.

2. Všeobecne o informáciách získaných použitím informačno-technických prostriedkov

Platnú právnu úpravu použitia informačno-technických prostriedkov v podmienkach Slovenskej republiky upravujú viaceré všeobecne záväzné právne predpisy, ktorými sú predovšetkým zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov a zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) v znení neskorších predpisov. Ďalším osobitným zákonom, ktorého prostriedky a postupy môžu priniesť informácie využiteľné aj ako dôkazy pre účely trestného konania, je zákon č. 122/2013 Z. z. o ochrane osobných údajov. Ustanovenie § 15 odsek 7 tohto zákona obsahuje úpravu, podľa ktorej môže byť záznam z monitorovania priestorov prístupných verejnosti použitý aj pre účely trestného konania. Platí to vtedy, ak bol obrazový, zvukový alebo obrazovo-zvukový záznam použitý na monitorovanie priestorov prístupných verejnosti, získaný v súlade s podmienkami tohto ustanovenia. Charakter osobitného zákona v zmysle ustanovenia § 119 ods. 2 má aj zákon č. 1/2014 o organizovaní verejných športových podujatí. Podľa ustanovenia § 21 možno v priestoroch športových zariadení vykonávať kamerovými systémami monitorovanie priebehu športového podujatia, vrátane účastníkov športového podujatia. Výsledky monitorovania možno zaznamenať na digitálne záznamy. Tieto možno použiť aj pre účely trestného konania,

za podmienky, že boli získané v súlade s ustanoveniami § 21 zákona o organizovaní verejných športových podujatí.

Definícia informačno-technických prostriedkov pre účely trestného konania je upravená v ustanovení § 10 ods. 21 Trestného poriadku, v zmysle ktorého informačno-technickými prostriedkami na účely tohto zákona sa rozumejú elektrotechnické, rádiotechnické, fototechnické, optické, mechanické, chemické a iné technické prostriedky a zariadenia alebo ich súbory použité utajovaným spôsobom pri odpočúvaní a zázname prevádzky v elektronických komunikačných sieťach, obrazových, zvukových alebo obrazovo-zvukových záznamov alebo pri vyhľadávaní, otváraní a skúmaní zásielok, ak sa ich použitím zasahuje do základných ľudských práv a slobôd.

V prípade osobitného zákona o ochrane pred odpočúvaním, pojem informačno-technický prostriedok je upravený v § 2 ods. 1 písm. a), b), c) takto: Na účely tohto zákona sa rozumejú elektrotechnické, rádiotechnické, fototechnické, optické, mechanické, chemické a iné technické prostriedky a zariadenia alebo ich súbory používané utajovaným spôsobom pri vyhľadávaní, otváraní, skúmaní a vyhodnocovaní poštových zásielok a iných dopravovaných zásielok, odpočúvaní a zaznamenávaní v rámci telekomunikačných činností a vyhotovení a využívaní obrazových, zvukových alebo iných záznamov.

Európsky Dohovor o ochrane ľudských práv a základných slobôd v čl. 8 deklaruje právo na súkromie a stanovuje podmienky, za ktorých štát môže do súkromia zasiahnuť. V zmysle čl. 8 spomínaného Dohovoru každý má právo na rešpektovanie svojho súkromného a rodinného života, obydlia a korešpondencie a štátny orgán nemôže do výkonu tohto práva zasahovať okrem prípadov, keď je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom a zločinnosti, ochrany zdravia alebo morálky, alebo ochrany práv a slobôd iných.

Možno uviesť, že zásahy orgánov do práva na súkromie štrasburské orgány ochrany práva posudzujú z troch hľadísk, a to z hľadiska legality, legitímnosti a proporcionality.

Legalita zásahu štátnych orgánov do práva na súkromie znamená, že štátne orgány môžu toto právo obmedziť len na základe zákona pričom táto požiadavka vyplýva priamo z čl. 8 ods. 2 Dohovoru o ochrane ľudských práv a základných slobôd. Pri posudzovaní splnenia podmienky legality štrasburské orgány vychádzajú z toho, či bola rešpektovaná dostupnosť a predvídateľnosť zákona.¹⁶ Legalita zásahu do práva na súkromie taktiež znamená, že príkaz alebo súhlas na použitie informačno-technických prostriedkov, predstavujúci zásah do práva na súkromie, musí byť náležitým spôsobom odôvodnený s poukazom na konkrétne skutočnosti odôvodňujúce zásah, pričom nepostačuje iba odkaz na príslušnú právnu úpravu.

V článku 8 ods. 2 Dohovoru o ochrane ľudských práv a základných slobôd, podobne ako legalita, je priamo stanovená legitímnosť zásahu štátnych orgánov. Legitimita zásahu znamená, že do práva na súkromie možno zasiahnuť len vtedy, keď je to v záujme štátnych orgánov z dôvodov ochrany národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom a zločinnosti, ochrany zdravia alebo morálky, alebo ochrany práv a slobôd iných. Pri posudzovaní legitímnosti zásahu štrasburské orgány skúmajú, či opatrenie umožňujúce zásah štátnych orgánov zodpovedá cieľu odôvodňujúcemu jeho legitimitu.

Proporcionality zásahu štátnych orgánov znamená, že musí byť dodržaná vo vzťahu medzi právom na súkromie a výberom prostriedkov, ktorými štátne orgány disponujú pri plnení legitímneho cieľa. Štátne orgány majú v zásade pri výbere prostriedkov, ktorými chcú dosiah-

¹⁶ SVÁK, J.: Ochrana ľudských práv (z pohľadu judikatúry a doktríny štrasburských orgánov ochrany práv). II. rozšírené vydanie. Bratislava: EUROKÓDEX 2006, s. 584–585.

nuť legitímny cieľ, možnosť uplatniť voľnú úvahu, pričom sú limitované tým, že zásah do práva na súkromie vykonávajú len vtedy, keď to je nevyhnutné, teda v duchu požiadaviek kladených na demokratickú spoločnosť. Inými slovami, štátne orgány môžu k zásahu prikróčiť len vtedy, keď je to nevyhnutné a sledovaný cieľ nemožno dosiahnuť miernejšími prostriedkami.¹⁷

Z vyššie uvedeného vyplýva, že do práva na súkromie možno zasiahnuť výlučne len vtedy, ak je takýto zásah legálny, legitímny a proporcionálny pričom ide o kumulatívne splnenie uvedených podmienok.

Možno konštatovať, že problematika získavania informácií pre účely trestného konania použitím informačno-technických prostriedkov je a aj bude vždy vysoko aktuálna a spoločensky závažná vzhľadom na to, že sa ich použitím výrazným spôsobom zasahuje do základných ľudských práv dotknutých osôb, a to do práva na súkromie.

3. K prípustnosti súkromného zvukového, obrazového alebo obrazovo-zvukového záznamu pre účely trestného konania

Veľmi diskutovanú tému v odborných kruhoch predstavuje prípustnosť súkromného zvukového, obrazového alebo obrazovo-zvukového záznamu. Pod pojmom súkromný zvukový záznam môžeme zjednodušene rozumieť audionahrávku, t. zn. záznam hlasového prejavu inej osoby nahraný súkromnou osobou pomocou diktafónu, mobilného telefónu či iného technického zariadenia, uložený na CD nosiči alebo inom médiu. Môže ísť aj o súkromnú videonahrávku, t. j. video nasnímané pomocou telefónu (obrazový, obrazovo-zvukový záznam) alebo fotografie, ktoré možno prehrať alebo vytlačiť, prípadne zdieľať v rámci sociálnych sietí.

Možno konštatovať, že predloženie obrazového, zvukového alebo obrazovo-zvukového záznamu súkromnou osobou v trestnom konaní vyvoláva viaceré protichodné názory týkajúce sa práve vzťahu zákonnosti a prípustnosti takéhoto dôkazu, pričom sa generálne uplatňuje názor, že pokiaľ záznam zachytáva skutok, ktorý napĺňa skutkovú podstatu niektorého z trestných činov, nemožno v trestnom konaní takýto záznam použiť, ak na vyhotovenie a použitie tohto záznamu nedala súhlas osoba v zmysle ustanovenia § 12 ods. 1 zákona č. 40/1964 Zb. Občiansky zákonník (ďalej len „OZ“), ktorý zakotvuje právnu ochranu prejavov osobnej povahy. V praxi asi len s ťažkosťou nájdeme páchatela, ktorý by potvrdil skutočnosť, že na vyhotovenie záznamu, ktoré ho de facto usvedčuje zo spáchania trestného činu, dal prívolenie.

Považujeme za dôležité spomenúť, že od nariadeného odpočúvania v zmysle § 115 Trestného poriadku a vyhotovovania obrazových, zvukových alebo obrazovo-zvukových záznamov v zmysle § 114 Trestného poriadku treba odlišovať situácie, keď obsah komunikácie resp. skutku nezaznamenáva orgán verejnej moci, ale súkromná osoba resp. poškodený vo forme zvukového záznamu alebo obrazového záznamu, alebo obrazovo-zvukového záznamu, a to bez súhlasu zaznamenávanej osoby. V takomto prípade nepôjde o postup orgánov verejnej moci v zmysle ich tzv. zákonnej licencie, pre ktorý je v trestnom konaní záväzné ustanovenie § 114 Trestného poriadku alebo § 115 Trestného poriadku.¹⁸ Uvedené ustanovenia nemožno aplikovať pre súkromné osoby, a to ani analogicky, nakoľko sa na súkromné osoby nevzťahuje ani článok 8 ods. 2 Dohovoru o ochrane ľudských práv a základných slobôd, ktorý stanovuje, kedy a za akých podmienok, a na ako dlho môže byť zo strany orgánu verejnej moci právo na súkromie obmedzené. Na druhej strane sa však zaznamenávané osoby môžu domáhať ochrany súkromia podľa čl. 8

¹⁷ PERHÁCS, Z. – PERHÁCSOVÁ, A.: Právna úprava používania informačno-technických prostriedkov (1. časť); Justičná revue, 65, 2013, č. 4, s. 543–545.

¹⁸ ČENTĚŠ, J.: Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. Bratislava: C. H. Beck, 2013, s. 132.

ods. 1 Dohovoru o ochrane ľudských práv a základných slobôd, čl. 17 ods. 1 Medzinárodného paktu o občianskych a politických právach, čl. 13 ods. 4, čl. 16 ods. 1 a čl. 19 ods. 2 a 3 Ústavy Slovenskej republiky, ako aj § 11 a § 12 OZ.

V súvislosti s vyššie uvedeným by sa pri posudzovaní zákonnosti a prípustnosti súkromného záznamu, ktorý bude v trestnom konaní predložený súkromnou osobou resp. poškodeným, mala posudzovať zásada proporcionality, nakoľko tu dochádza ku kolízií základných práv. Dochádza tu teda k stretu medzi záujmom na ochranu osobnosti toho, koho prejav je bez jeho súhlasu zaznamenaný, a medzi záujmom na ochranu osobnosti toho, kto tento prejav zaznamenáva a následne použije. Do akej miery je ten-ktorý záujem v konkrétnej situácii prevažujúci, to je potrebné v každom jednotlivom prípade ponechať na posúdenie všeobecnému súdu a tento neriešiť vo všeobecnej rovine. Rovnako je vecou všeobecných súdov samotné pripustenie dôkazov, nakoľko tieto nezávisle rozhodujú o tom, ktorý dôkaz je pre trestné konanie významný, a ktorý možno ako nevýznamný vylúčiť.¹⁹

Posúdenie, či určitý konkrétny záznam bude prípustný ako dôkaz v trestnom konaní, je vecou konkrétneho trestného konania a situácie, za ktorej má byť takýto dôkaz použitý. Záznam vyhotovený súkromnou osobou resp. poškodeným môže byť prípustný za podmienky, že zásah do súkromia je odôvodniteľný prevažujúcim záujmom na strane toho, kto záznam zabezpečil a následne použil. Základným kritériom, ktoré by malo v konečnom dôsledku viesť k rozhodnutiu o prípustnosti či neprípustnosti takto zabezpečeného záznamu ako dôkazu v trestnom konaní, bude pomer chránených práv a záujmov, ktoré sa v tejto súkromnej sfére stretávajú a kde sa štát stáva arbitrom prostredníctvom súdu rozhodujúcim o tom, ktorý z týchto záujmov bude v danom konkrétnom strete prevažujúcim, pričom hodnotenie použiteľnosti či nepoužiteľnosti záznamu sa bude vykonávať podľa procesných noriem.

V súvislosti s problematikou zákonnosti a použiteľnosti dôkazu (súkromného záznamu) možno spomenúť rozhodnutia Krajského súdu v Žiline a Okresného súdu v Pezinku, ktoré dospeli k rôznym záverom. Podľa uznesenia Krajského súdu v Žiline zo dňa 22. 4. 2010, sp. zn. 1To/42/2010 je dôležitým pre posudzovanie zákonnosti dôkazu zistenie, či záujem na ochrane súkromia obžalovaného je väčší než záujem na ochrane poškodeného a záujem spoločnosti na spravodlivom postihnutí možného protiprávneho konania obžalovaného. Na strane druhej je tu odôvodnenie rozhodnutia Okresného súdu Pezinok zo dňa 8. 10. 2012 (spisová značka neuvedená), ktoré sa s uvedenými závermi nestotožňuje, nakoľko ich považuje za účelovú interpretáciu zákona a neprípustne rozširujúci výklad odkazom na uprednostňovanie záujmu na zistení materiálnej pravdy za každú cenu pred záujmom na ochrane iných práv, pritom poukazuje na to, že Krajský súd v Žiline vo svojej argumentácii nepochybne vychádza z ustálenej judikatúry českých súdov, ktorú však vzhľadom na odlišnosť slovenskej právnej úpravy nemožno použiť.²⁰

Možno konštatovať, že v trestnom konaní nie je a priori vylúčené, aby bol záznam, vyhotovený súkromnou osobou resp. poškodeným, bez ingerencie orgánov verejnej moci, použitý v tomto konaní ako prípustný dôkaz aj bez súhlasu zaznamenávanej osoby, pričom samotná prípustnosť takéhoto dôkazu by sa mala prirodzene posudzovať so zreteľom na rešpektovanie práva na súkromie, a to predovšetkým z pohľadu čl. 8 ods. 1 Dohovoru o ochrane ľudských práv a základných slobôd, čl. 17 ods. 1 Medzinárodného paktu o občianskych a politických právach, čl. 16 ods. 1 a čl. 19 ods. 2 a 3 Ústavy SR, § 11 a § 12 OZ, ako aj práva na spravodlivý proces podľa čl. 6 Dohovoru o ochrane ľudských práv a základných slobôd.

¹⁹ GAJDIČIAR, V. – STRIGÁČOVÁ, D.: Prípustnosť súkromnej nahrávky pri trestno-procesnom dokazovaní v slovenskej právnej úprave; *Justičná revue*, 66, 2014, č. 6–7, s. 825.

²⁰ Rozsudok OS Pezinok je uverejnený na stránke www.pravnelisty.sk.

V tejto súvislosti je nevyhnutné spomenúť ustanovenia § 6 a § 417 ods. 1 OZ. V zmysle § 6 OZ, ak hrozí neoprávnený zásah do práva bezprostredne, môže ten, kto je takto ohrozený, primeraným spôsobom zásah sám odvrátiť. Podľa § 417 ods. 1 OZ komu škoda hrozí, je povinný na jej odvrátenie zakročiť spôsobom primeraným okolnostiam ohrozenia.

Na základe analýzy vyššie uvedených ustanovení OZ je následne možné uvažovať o myšlienke, že trestný čin, ktorý je v prvom rade sociálny konflikt a má súkromnoprávny, ako aj verejnoprávny aspekt, predstavuje vo svojej podstate spôsobenie ujmy inej osobe, ale aj spoločnosti. Keďže poškodenému, ako aj spoločnosti hrozí týmto protiprávnym konaním škoda, je na mieste zvážiť tú skutočnosť, že získanie dôkazu poškodenou stranou, hoci spôsobom odporujúcim zákonu, by v zmysle § 6 a § 417 ods. 1 OZ mohlo predstavovať odpadnutie istej vady nezákonnosti takéhoto dôkazu.

Vyššie uvedenú úvahu podporuje aj stanovisko Ústavného súdu Českej republiky, ktorý z hľadiska kolízie dvoch právnym poriadkom chránených záujmov akceptuje takú formu konania poškodenej osoby, ktorá nesie črty svojpomoci obeti trestného činu na úkor práv páchatela.²¹

Je všeobecne známe, že účelom trestného konania je, aby trestné činy boli náležite objasnené a páchatelia spravodlivo potrestaní. Preto možno konštatovať, že ak niekto vyhotoví záznam počas protiprávneho konania inej osoby, ktoré napĺňa znaky konkrétnej skutkovej podstaty trestného činu, hoci bez jej súhlasu, odvracia tým de facto škodu, ktorej spôsobenie hrozí, ak by bol trestný čin dokonaný.

Pri posúdení prípustnosti zvukového záznamu sa treba zamerať predovšetkým na to, či a akým spôsobom sa týmto záznamom zasiahlo do osobnostných práv dotknutej osoby, do jej práva na ochranu súkromia a takisto, či jeho použitie je v súlade so zásadou primeranosti, zásadou prezumpcie neviny ako aj so zásadou proporcionality. Základným kritériom tohto hodnotenia bude zváženie pomeru chránených práv a záujmov, ktoré sa v tejto súkromnej sfére stretávajú, a kde sa má štát predovšetkým prostredníctvom súdu stať arbitrom rozhodujúcim o tom, ktorý z týchto záujmov bude v danom konkrétnom strete prevažujúcim.²²

Možno uviesť, že dôležitý je aj obsah záznamu ako aj okolností, za ktorých bol súkromný záznam vyhotovený, pričom zohľadniť treba tiež fakt, či nedošlo k porušeniu zákona napr. provokáciou protiprávneho konania, alebo či nedošlo k úprave zvukového záznamu. V takýchto prípadoch upozorňuje Čentěš, že vyššie spomínané konania by mali potom za následok, že záznam by predstavoval neprípustný dôkaz v trestnom konaní.²³

Za významnú okolnosť je rovnako nevyhnutné potom považovať aj to, či informácie získané takýmto záznamom predstavujú jediný usvedčujúci dôkaz, a teda či dôkaz v podobe takto získaného záznamu stojí v konkrétnej veci v rámci hodnotenia otázky viny páchatela osamotený, alebo či tieto informácie len „dokresľujú situáciu“ ako podporný dôkaz a súd má k dispozícii aj iné dôkazy, ktoré významným spôsobom nasvedčujú dôvodnosti obvinenia, a s ktorými je tento záznam v obsahovej zhode. V prípade, ak takáto informácia bola podporená aj ďalšími dôkazmi, s obsahom ktorých korešponduje, môže predstavovať dôkaz v trestnom konaní.²⁴

Možno konštatovať, že vo vzťahu k určitým trestným činom je dokazovanie obzvlášť problematické, nakoľko orgán činný v trestnom konaní neraz vychádza výhradne z výpovede poškodeného, pričom absentujú iné relevantné dôkazy, predovšetkým priame svedecké výpovede. Ide predovšetkým o trestné činy súvisiace s domácim násilím, sexuálne trestné činy, nebezpečné

²¹ Uznesenie Ústavného súdu ČR z 19. 8. 2010, sp. zn. III. ÚS 1800/10.

²² Uznesenie Ústavného súdu ČR z 20. 10. 2011 sp. zn. II. ÚS 143/06.

²³ ČENTĚŠ, J.: *Odpočúvanie – procesnoprávne a hmotnoprávne aspekty*. Bratislava: C. H. Beck, 2013, s. 135.

²⁴ POTMĚŠIL, J.: *Přípustnost audio a video nahrávek jako důkazu; Jiné právo*, 16. 12. 2009, dostupné na: <http://jinepravo.blogspot.sk/2009/12/jan-potmesil-pripustnost-audio-video.html>.

vyhrážanie, nebezpečné prenasledovanie, vydieranie či hrubý nátlak a pod. Domáce násilie sa prevažne uskutočňuje bez priamych svedkov, v domácom prostredí bez toho, aby si to najbližšie okolie všimlo, a teda možno uviesť, že pri takomto konaní jednoznačne prevažuje záujem na ochranu osoby a osobnosti poškodeného nad právom na ochranu osobnosti páchatela.

V prípadoch, ak poškodený v rámci stretnutia s páchatelom, keď dôjde ku konaniu, ktoré by naplnilo znaky trestného činu napr. vydierania, hrubého nátlaku alebo k tyranizujúcemu správaniu voči jeho osobe, vyhotoví záznam, mohlo by ísť z hľadiska trestného konania o zákonne získaný usvedčujúci dôkaz. S uvedeným sa stotožňuje aj Čentíš, podľa ktorého v prípadoch domáceho násillia by konanie poškodeného mohlo niesť črty svojpomoci obete trestného činu na úkor práva páchatela v takej forme, ktorú možno akceptovať z hľadiska kolízie dvoch, právnym poriadkom chráneným záujmov.²⁵

Avšak v tejto súvislosti je nutné uviesť, že v mnohých prípadoch súdna prax zastáva názor, že uvedený dôkaz je nezákonný a neprípustný, nakoľko nebol vyhotovený so súhlasom osoby v zmysle § 12 ods. 1 OZ. Je nepochybne zrejmé, že v zmysle § 119 ods. 2 Trestného poriadku môže za dôkaz slúžiť všetko, čo môže prispieť k náležitému objasneniu veci a čo sa získalo z dôkazných prostriedkov podľa Trestného poriadku alebo podľa osobitného zákona, teda len to, čo bolo získané zákonným spôsobom, to znamená v súlade s ustanoveniami Trestného poriadku, prípadne podľa osobitného zákona. Osobitným zákonom sa myslí zákon č. 171/1993 Z. Z. o policajnom zbore, zákon č. 163/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov, Občiansky zákonník a iné v texte predchádzajúcej časti uvedené zákony.

V prípade, ak bol dôkaz získaný v rozpore s Trestným poriadkom resp. v rozpore s osobitným zákonom, nemôže slúžiť ako dôkaz v trestnom konaní a nemôže ani prispieť k náležitému objasneniu veci. Súd vo všeobecnosti pokiaľ ide o posudzovanie neúčinnosti získaného dôkazu uvádza, že dôkaz získaný nezákonným spôsobom je podľa povahy a závažnosti porušenia zákona buď absolútne neúčinný alebo relatívne neúčinný, pričom pri absolútnej neúčinnosti dôkazu nemožno spôsobenú nezákonnosť odstrániť ani napraviť.

Vzhľadom na takto formulovaný problém potom vyvstáva otázka, či je možné v tomto smere zaujať aj taký právny názor, podľa ktorého uvedeným konaním poškodenej osoby ide v podstate o jej prevenčnú zakročovaciu povinnosť v kontexte § 6 a § 417 ods. 1 OZ, a vyhotovenie takéhoto záznamu ako aj jeho následné predloženie v trestnom konaní má za účel nielen objasniť protiprávne konanie páchatela, ale predovšetkým zamedziť jeho opakovaniu, resp. zastaviť ho pro futuro.²⁶

Podľa už vyššie spomenutého uznesenia Okresného súdu Pezinok zo dňa 8. 10. 2012, Okresný súd Pezinok argumentoval, že ani verejný záujem na nájdení materiálnej pravdy nemôže konvalidovať protiprávnosť konania, ktorým je od počiatku nezákonne získaný dôkaz poznačený. Avšak možno ponúknuť iný právny názor s tým, že verejný záujem na nájdení materiálnej pravdy môže konvalidovať protiprávnosť súkromnej nahrávky za určitých podmienok, ktoré by mohli bezprostredne súvisieť s konkrétnymi okolnosťami prípadu, akými sú závažnosť vyšetrovaného trestného činu, miesto kde bol spáchaný trestný čin, miera zásahu do práva na súkromie osoby, ako aj skutočnosti, že osoba, ktorá záznam vyhotovila, tak konala na svoju obranu, aby odvrátila nebezpečenstvo, ktoré z protiprávneho konania páchatela hrozilo, a to predovšetkým pro futuro. Vyššie uvedenú úvahu možno aplikovať pri tom druhu trestnej činnosti, ktorým páchatel priamo zasahuje alebo ohrozuje život či integritu poškodenej osoby.

²⁵ ČENTÍŠ, J.: *Odpočúvanie – procesnoprávne a hmotnoprávne aspekty*. Bratislava: C. H. Beck, 2013, s. 132.

²⁶ GAJDIČIAR, V. – STRIGÁČOVÁ, D.: *Prípustnosť súkromnej nahrávky pri trestno-procesnom dokazovaní v slovenskej právnej úprave*; *Justičná revue*, 66, 2014, č. 6–7, s. 834.

Opodstatnenosť tejto úvahy možno per analogiam oprieť aj o Nález Ústavného súdu Českej republiky zo dňa 9. 12. 2014, sp. zn.: II. ÚS 1774/14, ktorý sa týka prípustnosti (zákonnosti) dôkazu získaného zo zvukového záznamu súkromne vyhotoveného sťažovateľom, obsahom ktorého je rozhovor sťažovateľa s predstaviteľom bývalého zamestnávateľa – firmy Krohne CZ s. r. o. Brno, pričom sťažovateľ zvukový záznam vyhotovil bez vedomia spomínaného druhého účastníka rozhovoru. Ústavný súd ČR začal v tejto veci konanie na základe ústavnej sťažnosti sťažovateľa proti Rozsudku krajského súdu v Brne, ktorým bola zamietnutá sťažovateľova žaloba o neplatnosti výpovede z pracovného pomeru a proti rozsudku Najvyššieho súdu ČR, ktorým bolo zamietnuté sťažovateľove dovolanie. Z odôvodnenia ústavnej sťažnosti vyplýva, že sťažovateľ dostal výpoveď z pracovného pomeru od zamestnávateľa – firmy Krohne CZ s. r. o. Brno, a to z dôvodu nadbytočnosti a pripravovaných organizačných zmien. Sťažovateľ podal žalobu na Mestský súd v Brne, aby rozhodol o neplatnosti výpovede z tohto dôvodu. Mestský súd v Brne po vykonanom dokazovaní svojim rozsudkom určil, že výpoveď na základe uvedeného dôvodu je neplatná. Svoje rozhodnutie oprel aj o dôkaz získaný zo zvukového záznamu, ktorý súkromne vyhotovil sťažovateľ, obsahom ktorého je rozhovor sťažovateľa s predstaviteľom bývalého zamestnávateľa – firmy Krohne CZ s. r. o. Brno, pričom sťažovateľ zvukový záznam vyhotovil bez vedomia spomínaného druhého účastníka rozhovoru. Z obsahu nahrátého rozhovoru vyplýva, že zamestnávateľ organizačné zmeny, ktorými odôvodnil výpoveď, len účelovo predstieral. Zástupca zamestnávateľa podal proti rozsudku Mestského súdu v Brne odvolanie na Krajský súd v Brne. Krajský súd v Brne po vykonanom dokazovaní rozsudok Mestského súdu v Brne o neplatnosti výpovede zrušil. Krajský súd v Brne okrem iného vychádzal z toho, audionahrávka medzi sťažovateľom a predstaviteľom zamestnávateľa je ako dôkaz neprípustná, lebo bola urobená bez vedomia nahrávanej osoby. Sťažovateľ podal proti druhoінстанčnému rozhodnutiu Krajského súdu v Brne dovolanie. Najvyšší súd ČR dovolanie sťažovateľa zamietol. Sťažovateľ v odôvodnení svojej ústavnej sťažnosti uviedol, že nesúhlasí so závermi Krajského súdu v Brne a Najvyššieho súdu ČR o neprípustnosti audionahrávky ako dôkazu. Sťažovateľ mal za to, že táto nahrávka sa týka pracovných záležitostí a nejde tak o prejavy osobnej povahy, čo by odôvodňovalo jej neprípustnosť ako dôkazu v prípade, že nebol daný súhlas nahrávanej osoby.

Ústavný súd ČR vo svojom „Náleze“ rozhodol, že „rozsudkom Krajského súdu v Brne a rozsudkom Najvyššieho súdu ČR bolo porušené právo sťažovateľa na prístup k súdu a na súdnu ochranu zaručenú v článku 36 ods. 1 Listiny základných práv a slobôd.²⁷ Ústavný súd zaujal názor, že vzhľadom na okolnosti prípadu je súkromný audiozáznam ako dôkaz prípustný. V odôvodnení Nálezu Ústavného súdu ČR sa okrem iného uvádza: „Aj pokiaľ by však uvedená audionahrávka obsahovala prejavy osobnej povahy predstaviteľa zamestnávateľa, ktorý si nebol vedomý, že bol nahrávaný, prevažuje v súčasne prejednávanom prípade ochrana práva sťažovateľa na spravodlivý proces, zaručený čl. 36 ods. 1 Listiny základných práv a slobôd. Za bežných okolností je svojvoľné nahrávanie súkromných rozhovorov bez vedomia ich účastníkov hrubým zásahom do ich súkromia. Takýto postup s črtami záľudnosti je vo veľkej väčšine prípadov morálne aj právne neprijateľný, najmä ak je vedený zámerom nahrávanú osobu poškodiť. Ústavný súd sa rozhodne stavia proti nekalým praktikám vzájomného elektronického sledovania a skrytého nahrávania pri súkromných a profesionálnych stretnutiach, ktoré sú spravidla nielen v rozpore s právom, ale po stránke sociálno-etickej šíria v spoločnosti atmosféru podozrievavosti, strachu, neistoty a nedôvery. Celkom odlišne však treba posudzovať prípady, kedy je tajné vyho-

²⁷ Listina základných práv a slobôd bola uvedená do právneho poriadku bývalej Českej a slovenskej federatívnej republiky ústavným zákonom č. 23/1991 Zb. Po vzniku Slovenskej republiky sa Listina základných práv a slobôd stala na základe recepcného ustanovenia Ústavy SR súčasťou jej právneho poriadku. To isté platí aj pre právny poriadok Českej republiky – pozn. autora.

tovenie audiozáznamu rozhovoru súčasťou obrany obeti trestného činu proti páchatelovi alebo ide o spôsob dosiahnutia právnej ochrany výrazne slabšej strany významného občiansko-právneho a najmä pracovno-právneho sporu. Zásah do práva na súkromie osoby, ktorej ústny prejav je zaznamenaný, je tu plne ospravedlniteľný záujmom na ochrane slabšej strany právneho vzťahu, ktorej hrozí vážna ujma (vrátane napr. straty zamestnania). Zadováženie jediného alebo kľúčového dôkazu touto cestou je analogické s konaním za podmienok v krajnej núdzi, či dovoľenej svojpomoci.“

Záver

Pri bližšom pohľade na jednotlivé prístupy, závery, ako aj právnu argumentáciu súdov pri využití súkromnej nahrávky ako prípustného a zákonného dôkazu v trestnom konaní môžeme postrehnúť značnú nejednotnosť ba až rozdielnosť, čo z pohľadu právnej istoty účastníkov trestného konania predstavuje nežiaduci stav, ktorý je z dlhodobého hľadiska právne neudržateľný.

Záznam vyhotovený súkromnou osobou by mohol byť prípustný za podmienky, ak zásah do súkromia je odôvodniteľný prevažujúcim záujmom na strane toho, kto záznam zabezpečil a následne použil. Základným kritériom, ktoré by malo v konečnom dôsledku viesť k rozhodnutiu o prípustnosti alebo neprípustnosti takto zabezpečeného záznamu, ako dôkazu v trestnom konaní, by bolo pomer chránených práv a záujmov, ktoré sa v tejto súkromnej sfére stretávajú, a pri ktorých štát prostredníctvom nezávislého súdu sa stáva arbitrom, rozhodujúcim o tom, ktorý z týchto záujmov by bol v danom konkrétnom strete prevažujúcim, s tým, že hodnotenie použiteľnosti resp. nepoužiteľnosti takéhoto dôkazu sa bude vykonávať podľa zákonných procesných noriem.

Úplným záverom vyslovujeme právny názor, že súkromnú nahrávku, ktorá by preukazovala, že osoba, ktorej prejav je zaznamenaný, sa dopúšťa trestného činu, by bolo možné za určitých podmienok považovať za prípustný dôkaz v trestnom konaní, hoci nebol získaný alebo použitý s privolením osoby páchajúcej trestnú činnosť. Takýmito podmienkami by boli, ak by účastník zaznamenávajúci prejav páchatela trestnej činnosti konal ako obeť trestného činu v rámci krajnej núdze alebo svojpomoci, čím by odvracal nebezpečenstvo bezprostredne hroziace, alebo útok bezprostredne hroziaci alebo trvajúci na záujme, ktorý je chránený Trestným zákonom. Ďalšou podmienkou by bolo, že súkromná nahrávka nepredstavuje jediný usvedčujúci dôkaz, ale je jedným z radu iných dôkazov, ktoré tvoria podklad pre meritórne rozhodnutie.

Použitá literatúra

- BURDA, E.: Teoretické a praktické problémy dokazovania. Zborník príspevkov z celoštátnej konferencie s medzinárodnou účasťou konanej dňa 15. decembra 2008. Bratislava: BVŠP, 2008, s. 23–32.
- ČENTĚŠ, J.: Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. Bratislava: C. H. Beck, 2013. 250 s. ISBN 978-80-89603-09-1
- GAJDIČIAR, V. – STRIGÁČOVÁ, D.: Prípustnosť súkromnej nahrávky pri trestno-procesnom dokazovaní v slovenskej právnej úprave. Justičná revue, 66, 2014, č. 6–7, s. 822–838.
- IVOR, J. a kol.: Trestné právo procesné. Druhé, doplnené a prepracované vydanie. Bratislava: Iura Edition, 2010. 1049 s. ISBN 978-80-8078-309-9
- MATHERN, V.: Dokazovanie v československom trestnom procese. Bratislava: Obzor, 1984. 229 s.
- MOLE, N., HARBY, C.: Právo na spravodlivý proces. Sprievodca na aplikáciu článku 6 Európskeho dohovoru o ľudských právach. Rada Európy, 2009.

- NETT, A.: Plody z otráveného stromu. 1. vydání. Brno: Masarykova univerzita, 1997. 115 s. ISBN 80-8078-085-4
- PERHÁCS, Z. – PERHÁCSOVÁ, A.: Právna úprava používania informačno-technických prostriedkov (1. časť). Justičná revue, 65, 2013, č. 4, s. 542–555.
- POTMĚŠIL, J.: Přípustnost audio a video nahrávek jako důkazu. Jiné právo, 16. 12. 2009, dostupné na: <http://jinepravo.blogspot.sk/2009/12/jan-potmesil-pripustnost-audio-video.html>
- REPÍK, B.: Procesní důsledky porušení předpisů o dokazování v trestním řízení. Bulletin advokacie, 1982, červenec – srpen, s. 122–139.
- SVÁK, J.: Ochrana ľudských práv (z pohľadu judikatúry a doktríny štrasburských orgánov ochrany práva). II. rozšírené vydanie. Bratislava: EUKÓDEX, 2006. 1116 s. ISBN 80-88931-51-7
- SYROVÝ, I.: Použitie nezákonne získaného dôkazu v trestnom konaní. Bulletin slovenskej advokácie, č. 3/2007, s. 7–14.
- ŠIMOVČEK, I.: Teoretické a praktické problémy dokazovania. Zborník príspevkov z celoštátnej konferencie s medzinárodnou účasťou konanej dňa 15. decembra 2008. Bratislava: BVŠP, 2008, s. 255–262.
- ZÁHORA, J. a kol.: Dokazovanie v trestnom konaní. 1. vydanie. Praha: Leges, 2013. 320 s. ISBN 978-80-87576-76-2

Judikatúra

- Uznesenie Krajského súdu v Žiline z 22. 4. 2010, sp. zn. 1 To 42/2010.
- Uznesenie Ústavného súdu ČR z 19. 8. 2010, sp. zn. III. ÚS 1800/10.
- Nález Ústavného súdu ČR z 20. 10. 2011, sp. zn. II. ÚS ČR 143/06.
- Nález Ústavného súdu ČR z 9. 12. 2014, sp. zn. II. ÚS 1774/14,

Informačno-technické prostriedky využívané v účelovo realizovaných procesoch OPČ

Information and Technical Means Used in Purpose Oriented Processes of Operative and Search Activity

Jaroslav Rapčan¹

Adrián Vaško²

Abstrakt: Autori vo svojom príspevku prezentujú výsledky, ktoré dosiahli v procese aplikovaného výskumu a realizáciou prieskumu. Objektom ich skúmania a hodnotenia je akceptácia využívania ITP pri plnení úloh v účelovo realizovaných procesoch OPČ. Z ich poznania vyplýva, že v praxi sú registrované rezervy v tejto činnosti, ktorých odstránením je možné zvýšiť účinnosť a efektívnosť pri plnení policajných úloh na úseku odhaľovania, objasňovania a dokazovania trestnej činnosti.

Abstract: In this article, the authors present the results achieved in the process of applied research and implementation of the survey. The object of their study and assessment is the acceptance of the use of information and technical means in performance of tasks in purpose-oriented processes of operative and search activity. The gathered knowledge has revealed some imperfections in this activity in practice, the removal of which can increase efficiency and effectiveness in carrying out the police tasks in the area of detection, investigation and the process of proving criminal activity.

Kľúčové slová: informačno-technické prostriedky, procesy operatívno-pátracej činnosti, kriminálno-policajné konanie.

Keywords: information and technical means, processes of operative and search activity, criminal police proceedings.

Úvod

Ak určitý subjekt spáchal trestný čin (páchateľ trestného činu), dostáva sa nutne do protikladu s požiadavkami spoločnosti a tým objektívne vytvára konfliktné situácie. Zo strany páchatelov sa takáto situácia vyznačuje najrôznejšími úskokmi, machináciami, utajovaním informácií, snahou o ovplyvnenie svedkov, mnohokrát aj príslušníkov bezpečnostných zložiek, o dezinformácie a využívaním ďalších spôsobov zakrývania protispoločenskej činnosti, ktorých sú aktérmi, s cieľom vyhnúť sa trestnej zodpovednosti. Páchatelia si mnohokrát za týmto účelom vytvárajú podmienky, napríklad dôkladnou prípravou k trestnému činu a k jeho utajovaniu, organizovaním konšpiratívnych skupín, získavaním kriminálnej kvalifikácie apod. Predovšetkým týmto prístupom páchatelia z jednotlivého trestného skutku vytvárajú zložitý, mnohostranný proces, ktorého poznanie si vyžaduje nasadenie adekvátnych metód, prostriedkov a foriem zo strany príslušníkov policajno-bezpečnostných zložiek. K uvedenému konštatovaniu je potrebné dodať, že spoločenská nebezpečnosť konania páchatela trestného činu si vyžaduje rýchly, rozhodný a ofenzívny zásah príslušníkov policajno-bezpečnostných zložiek tak, aby bola vylúčená možnosť pokračovať v konaní, aby nenastal ešte výraznejší spoločensky nežiadúci následok.

¹ JUDr. Jaroslav Rapčan, PhD., Akadémia Policajného zboru v Bratislave, katedra kriminálnej polície, Sklabinská 1, 835 17 Bratislava.

² JUDr. Adrián Vaško, Akadémia Policajného zboru v Bratislave, katedra kriminálnej polície, Sklabinská 1, 835 17 Bratislava, externý doktorand, Fakulta práva PEVŠ v Bratislave, Tomášikova 20, 821 02 Bratislava.

Z výsledkov analýzy bezpečnostnej situácie Slovenskej republiky o. i. vyplýva, že sa po roku 1989 zvýšila spoločenská závažnosť trestných činov. V jednotlivých znakoch, ktoré tvoria kriminálny obsah spôsobu páchania trestných činov, sú frekventovane registrované organizovanosť, agresivita, brutalita a čoraz častejšie sú zaznamenávané prvky medzinárodného charakteru.

Táto situácia si vyžaduje hľadanie a realizáciu nových riešení. Pri riešení trestnej činnosti predovšetkým policajná teória a prax (a to nielen u nás) jednoznačne poukazuje na potrebu aktívne využívať spravodajskú a operatívno-pátraciu činnosť.

Vo všetkých organizáciách manažéri pre svoju riadiacu činnosť potrebujú presné informácie všetkých druhov, ktoré sú základom pre ich rozhodovanie. Predovšetkým ide o dispozíciu poznania, ktorej obsahom je čo sa robí, alebo urobí v pracovnom prostredí manažéra. Ak úroveň poznania manažéra v danom pracovnom prostredí rastie, je vyššia pravdepodobnosť, že z jeho strany budú prijaté správne rozhodnutia.

Z charakteristiky samotného objektu poznávania (kriminalita a jej eliminácia) vyplýva, že ide o pomerne široký rozsah informácií, ktorý určuje samotná povaha trestnej činnosti, predovšetkým jej zložitosť, organizovanosť, latencia, potreba neustále prekonávať najrôznejšie úskoky a prekážky kladené páchatelmi v snahe zakryť tieto údaje pred príslušníkmi policajno-bezpečnostných zložiek, ako aj nutnosť plniť úlohy na úseku kontroly kriminality v maximálne možnej miere jej účinnosti a efektivity (predmet poznávania – operatívno-pátracia činnosť).

Vzhľadom k účelu a konkrétnemu obsahu je operatívno-pátracia činnosť dôležitým článkom v sústave opatrení, ktoré prijíma štát k ochrane právneho poriadku a zákonnosti.

Otázkou je: „Je táto realita v policajnej praxi akceptovaná?“. Na základe výsledkov aplikovaného výskumu, ktorý realizovali pracovníci katedry kriminálnej polície Akadémie PZ v Bratislave, si dovoľujeme uviesť, že pri plnení stanovených úloh využitím dispozície tejto kompetencie sú registrované rezervy znižujúce účinnosť a efektivitu policajnej práce.³

1 Účelovo realizované procesy operatívno-pátracej činnosti

Spravodajská činnosť, operatívno-pátracia činnosť (*ďalej len OPČ*) a vyšetrovanie sú súčasťou štruktúry policajného konania. V policajnej praxi, pri poznávaní konkrétnych trestných činov, procesy týchto špeciálnych činností tvoria systém. Pre potreby policajnej praxe a teórie je vhodné, ak je tento systém skúmaný a vysvetľovaný ako jednotný celok, ktorý je vhodné označiť termínom kriminálno-policajné poznanie.

Správnosť týchto prístupov potvrdzujú výsledky a efekty, ktoré sú v policajnej praxi dosahované pri plnení stanovených úloh. Ich analýzou je možné dospieť k záveru, že ak sú tieto procesy systémovo realizované (*využívaním kompetencií – právna regulácia, zodpovednosť*) výrazne ovplyvňujú úroveň objektivity, účinnosti a efektivity pri poznávaní trestných činov. V teoretickej oblasti je možné poukázať na adresnú, cieľavedomú a systematickú vedecko-výskumnú prácu, ktorej objektom je kriminalita (*jej fragmenty – trestné činy*) a predmetom – procesy týchto špecifických činností pri jej poznávaní a pod.

V súčasnom období je operatívno-pátracia činnosť charakterizovaná ako pracovná náplň príslušníkov operatívnych služieb Policajného zboru (*ďalej len PZ*), orgánov činných v trestnom konaní a ďalších určených príslušníkov policajno-bezpečnostných zložiek (*Finančná správa, Zbor väzenskej a justičnej stráže*), pretože ju môžu využívať pri *účelovom* policajnom poznávaní, a to v medziach (*rozsah a súlad*) právneho poriadku Slovenskej republiky.

³ LISOŇ, M. a kol. *Možnosti rozvoja operatívnej činnosti polície: Správa z aplikovaného výskumu*, 1. vyd. Bratislava: Akadémia PZ v Bratislave, 2012, 131 s. Výsk. 183.

OPČ je systém spravidla utajených, spravodajských opatrení vykonávaných PZ na účely predchádzania, zamedzovania, odhaľovania a dokumentovania trestnej činnosti a zisťovania jej páchatelov, zabezpečovania ochrany určených osôb a strážených objektov, technicky chránených objektov, zabezpečovania a poskytovania ochrany a pomoci ohrozenému svedkovi a chránenému svedkovi, ochrany štátnej hranice a vypátrania osôb a vecí. (Zákon č. 171/1993 Z. z. § 38a)

Charakteristiku OPČ dominantne vymedzujú vlastnosti, ktoré určujú obsah jej procesov. Tie sú účelovo realizované v systéme kriminálno-policiajného poznania. Z tohto pohľadu, je za druhoradá možné označiť inštitucionálne predpoklady pre realizáciu týchto procesov. Je tomu tak preto, lebo procesy OPČ pri plnení úloh realizujú okrem príslušníkov PZ aj iné štátne orgány. Hore uvedené nechce v žiadnom prípade znižovať praktický význam akceptácie inštitucionálnych opatrení, ktoré v určitom slova zmysle vytvárajú predpoklady pre realizáciu procesov OPČ.

OPČ má vo vzťahu ku kriminálno-policiajnému poznaniu špecifický charakter. Ten nie je určený jednoduchým súhrnom rozličných opatrení, vykonávaných čas od času, len v určitých prípadoch a za priaznivých podmienok, ale je zložitý, vnútorne diferencovaný, ucelený systém, ktorý zahrňuje hierarchiu podsystémov rôznych stupňov zložitosti ich štruktúry, organizácie a funkčného poslania. Vzhľadom na účel a konkrétny obsah, je OPČ dôležitým článkom v sústave opatrení, ktoré prijíma štát na ochranu právneho poriadku a zákonnosti a pri zabezpečovaní potrieb občanov.

Základnú osnovu pojmu OPČ tvoria dva osobitné súbory znakov:

1. súbor, ktorý definuje právnu reguláciu OPČ. Tá korešponduje s plnením funkcií štátu:

nielen rešpektuje, ale predovšetkým chráni pluralitný systém, demokratické hodnoty a inštitúcie. Na druhej strane zmyslom a cieľom tejto špecifickej policajnej činnosti je faktické a legálne naplnenie práva občana na bezpečnosť, ako i zabezpečenie ďalších základných a demokratických ľudských a občianskych práv. Procesy OPČ sú realizované len prostredníctvom a v medziach ústavného a právneho poriadku, ich realizačný štrukturálny obsah musí byť teoreticky odvodený z princípov právneho štátu.

2. súbor, ktorý definuje ucelený systém opatrení OPČ, avšak ktorý nie je uzatvorený:

nie je všeobecným súhrnom rozličných opatrení, ktoré sú realizované nekoordinovane len v určitých prípadoch a za vhodných podmienok, ale zložitým vnútorne diferencovaným uceleným systémom, ktorý je vytvorený cieľavedome, má svoju štruktúru, organizáciu a funkčné poslanie. V tomto smere je cieľavedomosť potrebné chápať ako konkrétnosť, ktorá je odrážaná v účelovo realizovaných procesoch.⁴

Analogickým výkladom právnej charakteristiky OPČ je možné dospieť k záveru, že jej základná systémová štruktúra je určená procesmi, ktorých relatívnu samostatnosť určujú realizované opatrenia (*akcie, zákroky*) a úkony. Určené orgány štátnej správy ich realizáciou vytvárajú predpoklady pre plnenie konkrétnych úloh. V právnom štáte pri plnení týchto úloh rešpektujú delegované kompetencie, prostredníctvom ktorých je možné naplniť zákonom stanovený účel. Ten sa predovšetkým týka, aj napriek tomu, že je v právnej norme vymedzený širokospektrálne, špecifického poznania trestných činov (*potrebné pre plnenie preventívnych a represívnych funkcií*). Vzhľadom na charakter a účel tejto činnosti, určuje zákonodarca dominantné postavenie medzi nimi *utajeným a spravodajským opatreniam*. Realizáciu ďalších opatrení zákonodarca pripúšťa. Napríklad ide o legislatívne, organizačno-riadiace, taktické a iné opatrenia. Tými je možné vytvárať vhodné podmienky pre systémové aplikovanie metód a využívanie prostriedkov

⁴ METEŇKO, J. – STIERANKA, J. *Riadenie operatívnych činností I*. Bratislava: Akadémia PZ v Bratislave, 2003, s. 23, ISBN 80-8054-283-X.

OPČ (*napríklad opatrenia, ktorými sa znižuje anonymita prostredia, v ktorom sa pohybuje potenciálny páchatel trestného činu, pátranie a iné*).⁵

Z policajnej praxe je zjavné, že proces, ktorý realizujú príslušníci polície pri poznávaní trestných činov a zisťovaní ich páchatelov, sa vo väčšine prípadov odvíja retrospektívne, od zistenia následkov k príčinám, ktoré ich vyvolali. Avšak, čo sa týka OPČ, v nej realizované procesy tvoria určitú výnimku. V rámci ich realizácie môže byť trestný čin a s ním súvisiace okolnosti odrážané aj v prítomnosti. Napríklad, k uvedeným situáciám dochádza pri neutralizácii zamýšľanej a pripravovanej trestnej činnosti (*identifikácia indikátorov a pod.*), pri rozkladaní kriminálnych skupín (*organizovaných, zločineckých, teroristických, extrémistických*), v rámci operatívnej kontroly nad vyčlenenými objektmi (*dohľadu, miestami odbytu hodnôt pochádzajúcich z trestnej činnosti*) a pod.

Pri využívaní OPČ ide o novú dimenziu na úseku poznávania trestných činov. OPČ príslušníkom PZ umožňuje odhaľovať a objasňovať nielen individuálne trestné činy, ale ich pozornosť môže byť zameraná aj na jednotlivé podozrivé osoby, dokonca i na potenciálnych páchatelov trestných činov, u ktorých sú dlhodobo sledované, predovšetkým kriminálne aspekty v ich konaní a pod. Rešpektujúc právny stav v Slovenskej republike je možné konštatovať, že výsledným produktom OPČ sú spracované informácie, ktoré je možné využiť za stanovených podmienok aj ako dôkaz v trestnom konaní (*Zákon č. 301/2005 Z. z.*).

Touto právnou realitou zvyrazňujeme, že právna regulácia realizácie OPČ nie je vymedzená výlučne v zákone o PZ (ZVJS, FS), ale aj v iných právnych normách. Napríklad konkrétna kompetencia vykonávať dôkazy realizáciou OPČ je implementovaná do Trestného poriadku.⁶

Tieto skutočnosti vyvolávajú potrebu vymedziť pojem OPČ, v štruktúre ktorého je precizovaný nielen vonkajší prejav (*operatívnosť, utajenosť*) tejto činnosti, ale aj jej vnútorný obsah, ktorý je určený účelovo realizovanými opatreniami a úkonmi. Rešpektujúc uvedené, pre potreby predkladaného teoretického poznania, termínom OPČ označujeme systém procesov, ktorých štrukturálny obsah tvoria spravidla utajené opatrenia a úkony, ktoré kompetentné orgány štátnej správy reagujú na vzniknutú alebo vznikajúcu situáciu realizujú pre zákonom vymedzené účely.⁷

Analogickým výkladom tejto charakteristiky vyplýva, že OPČ nie je jednoduchým súhrnom rozličných opatrení a úkonov, vykonávaných náhodne, len v určitých prípadoch a za priaznivých podmienok, ale zložitý, vnútorne diferencovaný ucelený systém, ktorý zahrňuje hierarchiu podsystémov rôzneho stupňa zložitosti jeho štruktúry, organizácie a funkčného poslania. Tak napríklad opatrenia na úseku organizácie práce a riadenia vytvárajú systém zahrňujúci podsystémy špeciálnych orgánov štátnej správy (*kriminálna polícia, finančná polícia, ...*), ktoré plnia stanovené úlohy v súlade so svojou miestnou a vecnou kompetenciou (*na pozíciách – prezídium, kraj, okres*). Z iného uhla pohľadu je možné uviesť, že opatrenia a úkony sú realizované za účelom predchádzania, zamedzovania, odhaľovania trestných činov, zisťovania ich páchatelov, pátrania, dokazovania a pod. Samozrejme je možné využiť túto právnu kompetenciu len v súlade a rozsahu zákona. Nami uvádzanú túto skutočnosť nie je možné považovať za redundantnú, pre-

⁵ K rozboru právnej charakteristiky OPČ je možné uviesť, že jej formulácia nie je presná, v právnom poriadku Slovenskej republiky mnohých prípadoch pôsobí kontraproduktívne. Zákonodarcu „neobvykle“ v jednom ustanovení sformuloval právnu charakteristiku tak širokospektrálnej činnosti. Osobitne je možné kriticky posudzovať ním použitú formuláciu, ktorá umožňuje v obsahu tejto činnosti realizovať spravodajské opatrenia a iné.

⁶ Zákon č. 301/2005 Z. z. Trestný poriadok, § 10 ods. 22, § 119 ods. 2.

⁷ LIŠOŇ, M. *Operatívno-pátracia činnosť: všeobecná časť*. 1. vyd. Bratislava: Akadémia PZ v Bratislave, 2012, s. 25–27.

tože v súlade so súčasným právnym poriadkom Slovenskej republiky je za podmienok, ktoré sú uvedené v Trestnom poriadku využívaním prostriedkov OPČ a ITP vykonávať dokazovanie.

Na základe výsledkov kauzálnych analýz sme dospeli k záveru, že v právnej praxi nie je to vždy plne akceptované, najmä zo strany obhajoby.

2 Informačno-technické prostriedky – funkcie

Tak ako je to v iných demokratických krajinách, aj v podmienkach Slovenskej republiky je nasadenie informačno-technických prostriedkov pri zabezpečovaní úloh na úseku kontroly kriminality viazané na osobitné, v zákonoch stanovené podmienky.

2.1 Právna úprava informačno-technických prostriedkov

V Slovenskej republike sú právne charakteristiky informačno-technických prostriedkov (*ďalej len ITP*) vymedzené v Trestnom poriadku a v zákone o ochrane súkromia pred neoprávneným použitím ITP a o zmene a doplnení niektorých zákonov (*zákon o ochrane pred odpočúvaním*). Subsidiarita využívania týchto prostriedkov je vymedzená v zákone o Policajnom zbore.⁸ Spoločným rysom charakteristík ITP, ktoré sú vymedzené v týchto právnych normách, je ich všeobecnosť, ktorá pripúšťa zaradiť medzi tieto prostriedky i také, ktoré sú doposiaľ neznáme, alebo nepoužívané (*najmä z technicko-informačného hľadiska*).

Použitie ITP je viazané na povolenie orgánov, ktoré sú mimo rámec polície. Tieto orgány sú povinné kontrolovať zákonnosť a účelnosť vydaného povolenia zasahovať do práv a slobôd občanov. V Slovenskej republike je uvedená povoľovacia kompetencia prenesená na sudcov a v určitých prípadoch na prokurátora.

Zo zákonných formulácií je možné vyvodiť, že použitím ITP je možné zasiahnuť predovšetkým do ústavou chráneného listového tajomstva a tajomstva, ktoré súvisí s poskytovaním a využívaním elektronických komunikácií. Z analogického výkladu zákonov je zrejmé, že týmito prostriedkami je možné taktiež zasiahnuť do domovej slobody. Toto oprávnenie vyplýva z možnosti *vyhotovovať obrazové, zvukové, alebo iné záznamy*, ktoré zákonodarca ničím nelimituje. V danom prípade pripúšťa ich realizáciu aj v spojení s tajným vstupom a prehliadkou obydlia, alebo iného priestoru. Použitím ITP možno obmedziť nedotknuteľnosť obydlia a prepravovanej správy len v nevyhnutne potrebnej miere.

Pri použití ITP sú, prevádzkovatelia verejných telefónnych sietí, poskytovatelia elektronických telekomunikačných sietí, poskytovatelia elektronických telekomunikačných služieb, poštový podnik, dopravcovia a iní zasielateľia a ich zamestnanci, povinní kompetentným orgánom štátnej správy poskytnúť nevyhnutnú súčinnosť; pritom sa nemôžu dovoľávať povinnosti mlčanlivosti podľa osobitných zákonov.

Použitie ITP limituje *katalóg trestných činov* – kriminálne situácie, pri riešení ktorých môžu byť vykonané informačno-technické úkony, ktorými dochádza k intenzívnym zásahom do občianskych práv a slobôd. ITP je možné v Slovenskej republike použiť len v prípadoch, keď odhaľovanie týchto trestných činov, zisťovanie ich páchatelov a zabezpečovanie nevyhnutných dôkazov pre trestné konanie by bolo iným spôsobom neúčinné alebo podstatne sťažené, rešpektujúc pritom princíp subsidiarity.

⁸ Zákon č. 171/1993 Z. z. o Policajnom zbore, § 36.

2.2 Právne charakteristiky ITP v Slovenskej republike

ITP sa na účely Zákona č. 301/2005 Z. z., v znení neskorších predpisov Trestného poriadku, § 10, ods. 21 rozumejú: elektrotechnické, rádiatechnické, fototechnické, optické, mechanické, chemické a iné technické prostriedky a zariadenia alebo ich súbory použité utajovaným spôsobom pri – odpočúvaní a zázname prevádzky v elektronických komunikačných sieťach (ďalej len „odpočúvanie a záznam telekomunikačnej prevádzky“), – obrazových, zvukových alebo obrazovo-zvukových záznamov alebo pri – vyhľadávaní, otváraní a skúmaní zásielok, ak sa ich použitím zasahuje do základných ľudských práv a slobôd.	ITP sú na účely Zákona č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) § 2 ods. 1 najmä elektrotechnické, rádiatechnické, fototechnické, optické, mechanické, chemické a iné technické prostriedky a zariadenia alebo ich súbory používané utajovaným spôsobom pri a) vyhľadávaní, otváraní, skúmaní a vyhodnocovaní poštových zásielok a iných dopravných zásielok, b) odpočúvaní a zaznamenávaní v rámci telekomunikačných činností, c) vyhotovovaní a využívaní obrazových, zvukových alebo iných záznamov.
---	--

Z analýzy uvádzaných charakteristík vyplýva, že z pohľadu realizácie procesov OPC využitím ITP, ide o celý rad možných (*potenciálnych*) zdrojov informácií (*informačných sietí*). Na spracúvanie informácií získaných použitím ITP, ich evidenciu, dokumentáciu, ukladanie a vyradovanie sa vzťahujú osobitné predpisy, ak zákon neustanovuje inak. Informácie získané ITP môžu byť využité výlučne na dosiahnutie účelu uvedeného v zákone.

ITP môže používať Policajný zbor, Slovenská informačná služba, Vojenské spravodajstvo, Zbor väzenskej a justičnej stráže a Finančná správa (*ďalej len „orgán štátu“*) v rozsahu podľa osobitných predpisov.

Používanie ITP, pre Zbor väzenskej a justičnej stráže a Finančnú správu, technicky zabezpečuje Policajný zbor, po predložení písomného súhlasu zákonného sudcu udeleného orgánu, pre ktorý sa použitie ITP zabezpečuje.

Pri odpočúvaní a zaznamenávaní telekomunikačnej prevádzky sa môže použiť len taký ITP, ktorý umožní okamžitú identifikáciu koncového telekomunikačného zariadenia, ktoré bolo použité na odpočúvanie a zaznamenávanie telekomunikačnej služby; ktorý neumožní vymazanie údajov identifikujúcich toto zariadenie, ako aj vymazanie času odpočúvania a zaznamenávania telekomunikačnej služby (*Zákon č. 351/2011 Z. z. o elektronických komunikáciách*).

Príslušník alebo zamestnanec orgánu štátu, ktorý plní úlohy súvisiace s technickým zabezpečením používania ITP sa musí podrobiť psychologicko-fyziologickému overeniu pravdivosti v lehotách určených vedúcim orgánu štátu.

Vzhľadom na náročnosť a riziká, ktoré sú spojené s využitím ITP, je v každom prípade potrebné prehodnotiť platnosť princípu zákonnosti a subsidiarity pri ich nasadzovaní.

Operatívni pracovníci sú, pri plnení svojich úloh, na úseku kontroly kriminality, povinní skúmať nutnosť kooperácie s orgánmi činnými v trestnom konaní (*najmä vyšetrovateľmi PZ*).

Použitie ITP podľa Trestného poriadku slúži na získavanie dôkazov pre trestné konanie.

ITP možno použiť iba vtedy, ak je to v demokratickej spoločnosti nevyhnutné pre zabezpečenie bezpečnosti štátu, obranu štátu, predchádzanie a objasňovanie trestnej činnosti, alebo na ochranu práv a slobôd iných. Použitím ITP sa môže základné právo alebo sloboda obmedziť len v nevyhnutnom rozsahu a nie dlhšie ako je nevyhnutné pre dosiahnutie zákonom uznaného cieľa, na ktorý slúži.

Konkrétne metódy a formy práce, špeciálne technické prostriedky používané pri informačno-technickom úkone a písomná dokumentácia sú utajované skutočnosti.

Orgány územnej samosprávy, súkromné bezpečnostné služby, ani iná fyzická osoba alebo právnická osoba nesmú použiť ITP.

Význam ITP pre realizáciu procesov OPČ

Údaje získané nasadením ITP možno použiť výlučne na dosiahnutie zákonom stanoveného účelu.

Na základe dosiahnutých výsledkov výskumu uvádzame, že ITP predstavujú veľmi významný nástroj, ktorým je možné získať relevantné informácie pre plnenie operatívnych úloh a dokazovanie. Ich využitím je možné vyhotoviť objektívnu dokumentáciu javov, ktoré vykazujú znaky kriminálnej aktivity. Za dôležité je možné označiť limitujúce možnosti, ktoré korešpondujú s využitím techniky pri získavaní, zbere, spracovaní a distribúcii relevantných informácií.

Využitím ITP je možné pomerne presne, objektívne vyhotovovať záznamy – bezprostredne alebo sprostredkované o skúmanom jave. Napríklad, význam takto získaného poznania predovšetkým spočíva v tom, že dochádza k fixácii (*dokumentácii*) genézy kriminálnej aktivity (*aj situácie*), často i takých detailov, ktoré môžu pri iných spôsoboch poznávania uniknúť a nie je možné ich získať opakovaným pozorovaním. Ak sú javy zdokumentované (čo *umožňuje nasadenie ITP*), je možné kedykoľvek reprodukovať jednotlivé etapy sledovaného deja, upresňovať skôr prijaté závery a dôkladnejšie a presnejšie určovať ďalší smer činnosti (*nielen v účelovo realizovaných procesoch OPČ*).

Informácie získané technickými úkonmi nemajú len charakter operatívnych informácií, ktoré slúžia na odhalenie trestných činov, zistenie ich páchatelov, ale aj sú dôležitým inštrumentom pri dokazovaní.

„Ako to vníma a rešpektuje policajná prax?“ Pri hľadaní odpovedí na túto otázku sme oslovili príslušníkov v policajnej praxi technikou riadeného rozhovoru. Respondentov celkom 20, sme vybrali z poslucháčov II. ročníka magisterského externého štúdia Akadémie PZ v Bratislave v školskom roku 2016/2017 (mesiac február 2017). Tí (so svojim osobným komentárom) na nami formulovanú otázku odpovedali, že nasadením ITP plnia tieto úlohy:

- zisťovať, upresňovať a dokumentovať mechanizmus protispoločenského konania, 100 % oslovených respondentov vyjadrilo toto stanovisko,
- stanoviť rozsah protispoločenského konania a podiel jednotlivých osôb na ňom, 100 % oslovených respondentov vyjadrilo toto stanovisko,
- odhaliť spolupáchateľov a iné osoby konania zúčastnených osôb, 100 % oslovených respondentov vyjadrilo toto stanovisko,
- zisťovať a zaisťovať informácie o protispoločenskom konaní, ktoré môžu byť využité ako dôkazy v trestnom konaní, ktoré by mohli byť zničené alebo neodhalené, 80 % oslovených respondentov vyjadrilo toto stanovisko,
- zisťovať informácie o úkrytoch páchatelov, vecí pochádzajúcich z protispoločenského konania, 50 % oslovených respondentov vyjadrilo toto stanovisko,

- zistiť kontakty, ich frekvenciu a tým dešifrovať štruktúru kriminálnych skupín a hierarchické postavenie ich subjektov, 90 % oslovených respondentov vyjadrilo toto stanovisko,
- získať portréty, záznam hlasu, biomechanický portrét podozrivých osôb k kriminalistickým analýzám (fonoskopia, ...), 40 % oslovených respondentov vyjadrilo toto stanovisko,
- dokumentovať realizáciu procesov OPČ, predovšetkým k potrebám dokázania zákonnosti, resp. previerok a pod., 20 % oslovených respondentov vyjadrilo toto stanovisko.

Na základe vyhodnotenia nami realizovaného prieskumu sme dospeli k záveru, že z pohľadu realizácie OPČ, v danom prípade, ide o celý rad možných (potenciálnych) zdrojov informácií. Za osobitne dôležité považujeme zdôrazniť, že policajná prax ITP nevyužíva v celom spektre zákonných oprávnení. Vzhľadom k možnej polemike k tomuto záveru, sme jeho objektivitu sekundárne overili na príslušnom špeciálnom pracovisku PZ, ktorého pracovníci vykonávajú tzv. servisnú službu vo vzťahu k ITP.

Domnievame sa, že v praxi tento stav vykazuje charakter rezervy. Tak, ako nám uviedli respondenti v procese prieskumu jej odstránenie je možné dosiahnuť zvýšením úrovne prípravy kompetentných príslušníkov polície. Túto skutočnosť pracovníci katedry kriminálnej polície akceptujú. V úzkej súčinnosti s vedením P PZ kreujú moduly vzdelávania, ktorých adresátom sú primárne príslušníci PZ. Samozrejme, tak ako sme už uviedli pritom rešpektujeme akceptáciu tejto ponuky aj od iných orgánov, ktoré sú oprávnené využívať ITP.

Ďalej je možné zo slovného vyjadrenia zákonov dedukovať možnosť zasiahnuť týmito prostriedkami taktiež do domovej slobody. Túto možnosť predovšetkým možno dedukovať z možnosti *vyhotovovať obrazové, zvukové alebo iné záznamy*, ktoré zákonodarca ničím nelimituje. V danom prípade pripúšťa ich realizáciu v spojení s tajným vstupom a prehliadkou obydľia, alebo iného priestoru.

Návrhy do diskusie

Príslušníci polície realizáciou OPČ znižujú úroveň anonymity prostredia, v ktorom sa pohybuje potenciálny páchatel' trestnej činnosti. Realizáciou OPČ sú vykonávané výrazné zásahy do práv a slobôd dotknutých subjektov (fyzické, právnické osoby). Použitie ITP pri plnení úloh je jedným z najintenzívnejších zásahov do práv a slobôd osôb. Kompetentné orgány pri ich nasadení musia rešpektovať zásadu subsidiarity, striktné rešpektujú princípy práva, slobody a humanizmu.

V policajnej praxi pri využívaní ITP sú registrované rezervy. Týka sa to tak nereálne definovaných cieľov ich nasadenia ako aj neakceptácie ich realizačných možností (viď výsledky účelovo realizovaného prieskumu).

Tieto rezervy je možné odstrániť špecializovanou prípravou príslušníkov polície a ďalších kompetentných orgánov, na ktorej sú povinní participovať aj pracovníci špeciálnych pracovísk PZ.

Máme zato, že aj našim výstupom na tejto medzinárodnej vedeckej konferencii sme dostatočne poukázali, že využívanie ITP je realita, ktorú je možné skúmať a hodnotiť.

Zoznam použitej literatúry

- LISOŇ, M. a kol. *Možnosti rozvoja operatívnej činnosti polície: Správa z aplikovaného výskumu*, 1. vyd. Bratislava: Akadémia PZ v Bratislave, 2012, 131 s. Výsk. 183.
- LISOŇ, M. *Operatívno-pátracia činnosť: všeobecná časť*. 1. vyd. Bratislava: Akadémia PZ v Bratislave, 2012, 225 s. ISBN 978-80-8054-541-3.

METEŇKO, J. – STIERANKA, J. *Riadenie operatívnych činností I*. Bratislava: Akadémia PZ v Bratislave, 2003, s. 23, ISBN 80-8054-283-X.

Zákon č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov.

Zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov.

Zákon č. 166/2003 Z. z. Zákon o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním).

Historický exkurz odpočúvania a záznamu telekomunikačnej prevádzky¹

Historical Review of the Legislation of the Eavesdrop and Telecommunication Recording

Jozef Medelský²

Abstrakt: Jedným z významných informačno-technických prostriedkov je aj odpočúvanie a záznam telekomunikačnej prevádzky. Štúdia ponúka podrobnú analýzu historického vývoja inštitútu odpočúvania a záznamu telekomunikačnej prevádzky v podmienkach Slovenskej republiky. Záverom sú predstavené základné atribúty tohto inštitútu a ponúknuté je aj zhodnotenie získaných poznatkov, apelujúc na striktné dodržiavanie zákonných podmienok nevyhnutných pre efektívnu a účinnú realizáciu tohto trestnoprávneho inštitútu.

Abstract: One of the important information and technical means is the interception and recording of telecommunications. The study provides a detailed analysis of the historical development of the institute interception and recording of telecommunications traffic in the Slovak Republic. The conclusions are presented the basic attributes of this institute and is also offered to assess lessons learned, Calling on strict compliance with the legal conditions necessary for effective and efficient implementation of the penal institute.

Kľúčové slová: informačno-technické prostriedky, odpočúvanie a záznam telekomunikačnej prevádzky, história, prehľad, analýza, komparácia, charakteristika, hodnotenie.

Keywords: information and technical means, interception and recording of telecommunications, history, review, analysis, comparison, rating, review.

Úvod

Odpočúvanie a záznam telekomunikačnej prevádzky je typickým príkladom informačno-technického prostriedku, ktorý je zadaný v § 10 ods. 21 zákona č. 301/2005 Z. z. Trestného poriadku v znení neskorších predpisov (ďalej len TP). Tento trestnoprávny inštitút je následne bližšie definovaný v § 115 a § 116 TP, kde sú obsiahnuté základné podmienky realizácie odpočúvania a záznamu telekomunikačnej prevádzky, ako aj spôsob oznámenia údajov o telekomunikačnej prevádzke.

Informačno-technické prostriedky je možné definovať ako elektrotechnické, rádiotechnické, fototechnické, optické, mechanické, chemické a iné technické prostriedky a zariadenia alebo ich súbory použité utajovaným spôsobom pri odpočúvaní a zázname telekomunikačnej prevádzky v elektrokomunikačných sieťach, obrazových, zvukových alebo obrazovo-zvukových záznamoch alebo pri otvorení a skúmaní zásielok, ak sa ich použitím zasahuje do základných ľudských práv a slobôd.³

Pokiaľ ide o definíciu odpočúvania a záznamu telekomunikačnej prevádzky, je potrebné uviesť, že ide o: „Trestno-procesný inštitút, pri ktorom sa zaznamenávajú telefonické hovory

¹ Táto štúdia bola podporovaná Agentúrou na podporu výskumu a vývoja na základe Zmluvy č. APVV-15-0272.

² PhDr. JUDr. Mgr. Jozef Medelský, PhD., Akadémia Policajného zboru v Bratislave, Katedra verejnoprávných vied, Sklabinská 1, 835 17 Bratislava.

³ Pozri bližšie: § 10 ods. 21 TP.

a iné informácie, ktoré sa realizujú elektronickou komunikačnou sieťou, ak sú svojím obsahom dôležité pre trestné konanie.⁴

Minárik definuje odpočúvanie a záznam telekomunikačnej prevádzky, ako: „zákonný postup, ktorý umožňuje prenos obsahu komunikácie a prepravovaných údajov prináležiacich k určitej adrese do zariadení oprávnených subjektov. Tento procesný inštitút smeruje k zaisteniu obsahu telekomunikačnej prevádzky prebiehajúcej v konkrétnej forme buď v aktuálnom čase, alebo v budúcnosti.“⁵

Napokon prof. Ivor definuje odpočúvanie a záznam telekomunikačnej prevádzky ako: „trestno-procesný inštitút umožňujúci zaznamenávať telefónne hovory a iné skutočnosti oznamované prostredníctvom elektronickej komunikačnej siete, ak sú svojím obsahom významné pre trestné konanie.“⁶

Pod pojmom telekomunikačná prevádzka je potrebné rozumieť: „technické zariadenie na vysielanie, prenos, smerovanie, príjem, prepojenie alebo spracovanie signálov šírených prostredníctvom vedení, rádiovými, optickými alebo inými elektromagnetickými prostriedkami.“ Predstavená zákonná definícia je obsiahnutá v § 4 ods. 1 zákona č. 351/2011 Z. z. o elektronických komunikáciách.

Bez pochyb realizáciou tohto trestno procesného inštitútu dochádza k značnému zásahu do základných ľudských práv a slobôd. Konkrétne to je zásah do práva na ochranu tajomstva dopravovaných správ. Uvedené právo je garantované Ústavou SR, konkrétne v článku 22 ods. 1 a 2, podľa ktorého:

„Listové tajomstvo, tajomstvo dopravovaných správ a iných písomností a ochrana osobných údajov sa zaručujú.

Nikto nesmie porušiť listové tajomstvo ani tajomstvo iných písomností a záznamov, či už uchovávaných v súkromí, alebo zasielaných poštou, alebo iným spôsobom; výnimkou sú prípady, ktoré ustanoví zákon. Rovnako sa zaručuje tajomstvo správ podávaných telefónom, telegrafom alebo iným podobným zariadením.“

Významným článkom obsiahnutým v Ústave je aj článok 16 ods. 1, ktorý garantuje právo na súkromie a nedotknuteľnosť osoby, pričom toto právo môže byť obmedzené len na základe zákona, resp. v prípadoch ustanovených zákonom.

Rovnako je toto právo garantované aj na medzinárodnej úrovni, a to konkrétne Dohovorom o ochrane ľudských práv a základných slobôd. Je to článok 8 ods. 1 a 2, ktorý bližšie definuje, že:

„Každý má právo na rešpektovanie svojho súkromného a rodinného života, obydlika a korešpondencie.

Štátny orgán nemôže do výkonu tohto práva zasahovať okrem prípadov, keď je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom a zločinnosti, ochrany zdravia alebo morálky alebo ochrany práv a slobôd iných.“

Odpočúvanie a záznam telekomunikačnej prevádzky je bez pochyb významným inštitútom, ktorým je možné získavať jedinečné informácie dôležité pre trestné konanie. Nakoľko sa realizáciou tohto inštitútu výrazne zasahuje do základných práv a slobôd dotknutých osôb je nevyhnutné apelovať na dodržiavanie všetkých zákonných podmienok pri využívaní odpočúvania

⁴ KORGÓ, D. a kolektív. 2013. *Trestné právo procesné*. Plzeň: Aleš Čeněk. 2013, s. 196.

⁵ MINÁRIK, Š. a kolektív. 2010. *Trestný poriadok*. Stručný komentár, Druhé, prepracované a doplnené vydanie. Bratislava: IuraEdition. 2010, s. 370–371.

⁶ IVOR, J. a kol. 2010. *Trestné právo procesné*. Druhé, doplnené a prepracované vydanie. Bratislava: IuraEdition. 2010, s. 403.

a záznamu telekomunikačnej prevádzky. Absenciou niektorej zo zákonných podmienok jednak dochádza k neoprávnenému zásahu do osobnostnej, súkromnej sféry dotknutej osoby, a zároveň môže dôjsť k zmareniu trestného konania, tým, že získané informácie, a dôkazy budú neúčinné a teda nebudú môcť byť v rámci trestného konania využité.

Historický exkurz odpočúvania a záznamu telekomunikačnej prevádzky

Z názvu štúdie vyplýva, že predmetom analýzy bude úprava odpočúvania a telekomunikačnej prevádzky v minulých zákonných úpravách, teda pred rokom 2005, kedy došlo k rekodifikácii trestného práva hmotného a procesného.

Zákon č. 141/1961 Zb. o trestnom konaní súdnom v pôvodnej časovej verzii s účinnosťou od 1. januára 1962 neobsahoval špecifické ustanovenie o odpočúvaní a zázname telekomunikačnej prevádzky. Bolo to zrejme aj vzhľadom na neexistenciu technických zariadení, ktoré by mohli odpočúvanie, resp. záznam realizovať. Za zmienku však stojí ustanovenie § 88, ktoré umožňovalo zaistovanie vecí bezpečnostnými orgánmi. V zmysle tohto ustanovenia boli bezpečnostné orgány oprávnené vykonať zaistovacie úkony, pričom mali povinnosť si vopred zadovážiť súhlas prokurátora, resp. aj bez súhlasu z dôvodu neodkladnosti, pričom ich povinnosťou bolo do 48 hodín prokurátora o úkone upovedomiť. Bezpečnostné orgány boli zároveň povinné postupovať v zmysle predpisov trestného poriadku, pričom zákonnosť a neodkladnosť takýchto úkonov prokurátor vždy preveril.⁷ Predstavené ustanovenie sa už v časovej verzii zákona od 1. augusta 1965 viac nenachádza.

Legislatívna zmena nastala až pri časovej verzii účinnej od 1. júla 1990, a to konkrétne zákonom 178/1990 Zb., kedy bolo do ustanovení zákona o trestnom konaní súdnom opäť zakomponované paragrafové znenie 88. Tentokrát však s názvom: „Odpočúvanie telefonických hovorov“.

Uvedené ustanovenie umožňovalo odpočúvanie telefónnych hovorov a to po začatí trestného stíhania pre obzvlášť závažný úmyselný trestný čin alebo pre iný úmyselný trestný čin, na ktorého stíhanie zaväzuje vyhlásená medzinárodná zmluva. K nariadeniu odpočúvať hovory bol oprávnený predseda senátu v konaní pred súdom a prokurátor v prípravnom konaní, pričom príkaz musel byť daný písomne a musel byť odôvodnený. Podmienkou vydania príkazu bolo aj vymedzenie doby, počas ktorej sa bude odpočúvanie realizovať. Samotná realizácia odpočúvania bola zverená Zboru národnej bezpečnosti. Základnou podmienkou pre nariadenie bola existencia dôvodného predpokladu, že odpočúvaním budú oznámené významné skutočnosti pre trestné konanie, pričom zákon vylúčil odpočúvanie hovorov medzi obhajcom a obvineným.

Ak sa vedie trestné stíhanie pre iný trestný čin, než je úmyselný trestný čin, resp. závažný úmyselný trestný čin, je orgán činný v trestnom konaní oprávnený nariadiť odpočúvanie hovorov len so súhlasom účastníka konkrétnej telefónnej stanice.

Záverečné ustanovenie § 88 vyžaduje, že v prípade ak sa má záznam hovoru použiť ako dôkaz, je potrebné k nemu pripojiť protokol, kde budú základné informácie, ako miesto, čas, spôsob, obsah záznamu, ako aj informácie o osobe, ktorá záznam vyhotovila.

⁷ § 88 ods. 1 a 2 zákona č. 141/1961 Zb. o trestnom konaní súdnom: „(1) Ak je nevyhnutne potrebné ešte pred začiatkom vyšetrovania vykonať zaistovacie úkony, na ktoré sú bezpečnostné orgány podľa ustanovení tretieho, štvrtého a piateho oddielu tejto hlavy oprávnené, zadovážia si bezpečnostné orgány na ich vykonanie vopred súhlas prokurátora. Ak nemožno pre neodkladnosť veci zadovážiť súhlas vopred, musia do 48 hodín prokurátora o vykonanom úkone upovedomiť.“

(2) Pri vykonávaní úkonov sú bezpečnostné orgány povinné i v prípade uvedenom v odseku 1 postupovať podľa predpisov trestného poriadku. Zákonnosť a neodkladnosť takých úkonov prokurátor vždy preverí.“

Čiastočnú modifikáciu ustanovenia § 88 priniesla novela zákona o trestnom konaní súdnom, konkrétne zákonom č. 558/1991 Zb. Modifikácia sa týkala odseku druhého. Zachované ostali úvodné vety pojednávajúce o skutočnosti, že príkaz na odpočúvanie musí byť daný písomne a odôvodnený, ako aj že v príkaze musí byť vymedzená doba odpočúvania. Novinkou bola povinnosť upovedomiť o vykonávaní odpočúvania organizáciu, ktorá prevádzkuje telekomunikačnú sieť, v ktorej obvode sa bude odpočúvanie realizovať. Samotný výkon odpočúvania bol napokon zverený policajnému orgánu.

Ďalšia modifikácia § 88 bola vykonaná zákonom 247/1994 Zb., ktorým sa novelizoval zákon o trestnom konaní súdnom. V tomto prípade to bola časová verzia od 1. októbra 1994.

Prvá zmena nastala hneď v zmene názvu šiesteho oddielu. Pôvodná úprava pracovala s názvom odpočúvanie telefonických hovorov. Novelizované znenie už pracuje s pojmom odpočúvanie a záznam telekomunikačnej prevádzky. Druhá zmena bola obsiahnutá v odseku prvom. V pôvodnom znení bolo možné nariadiť realizáciu odpočúvania hovorov v dvoch prípadoch. Prvým prípadom bol obzvlášť závažný úmyselný trestný čin a v druhom prípade to bolo v prípade spáchania iného úmyselného trestného činu, o ktorom na konanie zaväzovala vyhlásená medzinárodná zmluva. V novom znení pribudla ďalšia možnosť, kedy je možné nariadiť odpočúvanie a záznam telekomunikačnej prevádzky. Bolo to v prípade trestných činov uvedených v osobitnom predpise, pričom takýmto osobitným zákonom bol zákon č. 249/1994 Z. z. o boji proti legalizácii príjmov z najzávažnejších, najmä organizovaných, foriem trestnej činnosti a o zmenách niektorých ďalších zákonov. Konkrétne to bol § 2 spomenutého zákona, ktorý vymedzoval trestné činy: „trestné činy teroru podľa § 93 a 93a, záškodníctva podľa § 95, falšovania a pozmeňovania peňazí a cenných papierov podľa § 140, zneužívania právomoci verejného činiteľa podľa § 158 ods. 2, všeobecného ohrozenia podľa § 179, ohrozenia bezpečnosti vzdušného dopravného prostriedku a civilného plavidla podľa § 180a, nedovoleného ozbrojovania podľa § 185 ods. 2 a 3, nedovolennej výroby a držania omamných a psychotropných látok, jedov a prekurzorov podľa § 187, nedovolennej výroby a držania jadrových materiálov podľa § 187a, obchodovania s deťmi podľa § 216a, vraždy podľa § 219, zavraždenia do cudziny podľa § 233, lúpeže podľa § 234 ods. 2 a 3, brania rukojemníka podľa § 234a, vydierania podľa § 235 ods. 2, obchodovania so ženami podľa § 246, krádeže podľa § 247 ods. 3 písm. a) a ods. 4, neoprávneného používania cudzieho motorového vozidla podľa § 249a ods. 3 a 4, podvodu podľa § 250 ods. 3 písm. a) a ods. 4 a legalizácie príjmov z trestnej činnosti podľa § 252 Trestného zákona.“

Významná zmena bola zrealizovaná v odseku 2. Doterajší návrh nedefinoval konkrétnu dobu realizácie odpočúvania hovorov. Nový návrh už teda vymedzuje, že doba odpočúvania a záznamu nesmie trvať dlhšie ako šesť mesiacov, pričom predseda senátu, resp. prokurátor v rámci právneho konania mohol túto dobu predĺžiť o ďalších šesť mesiacov.

Štvrtý odsek stanovil ďalšie povinnosti v prípade, ak sa má záznam použiť ako dôkaz. Okrem doterajších povinností, pribudla povinnosť záznamy označiť, spoľahlivo uschovať a v zápisnici založenej do spisu uviesť, kde sú uložené. Zároveň dodával, že v inej trestnej veci, ako je tá, v ktorej sa odpočúvanie a záznam telekomunikačnej prevádzky urobili, možno záznam ako dôkaz použiť len vtedy, ak sa súčasne aj v tejto veci vedie trestné konanie pre trestný čin uvedený v odseku 1 alebo ak s tým súhlasí účastník odpočúvanej stanice.

Do ustanovenia § 88 pribudol aj odsek piaty, ktorý stanovil povinnosť orgánom činným v trestnom konaní zničiť záznamy v zmysle predpisov o skartácii, a to v prípade ak sa vykonaným odpočúvaním alebo záznamom nezistili skutočnosti významné pre trestné konanie.

Ďalšia legislatívna zmena prišla v podobe novelizácie, a to zákonom č. 366/2000 Z. z. s účinnosťou od 7. novembra 2011. K zmene došlo v prvom odseku. Podľa nového znenia bolo možné nariadiť odpočúvanie a záznam telekomunikačnej prevádzky v prípade obzvlášť závažného

zločinu, v prípade korupcie, trestného činu podľa § 158 Trestného zákona a následne aj v prípade úmyselného trestného činu o ktorom na konanie zaväzuje vyhlásená medzinárodná zmluva. Novinkou teda bol trestný čin korupcie a trestný čin zneužívania právomoci verejného činiteľa v zmysle § 158⁸ zákona č. 140/1961 Zb. Trestného zákona.

K parciálnej zmene došlo aj v prípade odseku druhom. V zmysle novej úpravy musí byť príkaz vydaný zvlášť pre každú účastnícku stanicu a zároveň musí byť presne určená osoba, ktorej sa odpočúvanie a záznam týka. Novinkou v identickom odseku je, že so získaným záznamom sa nakladá ako s písomnosťou obsahujúcou predmet štátneho tajomstva.

Pozmenený bol aj ods. 4 § 88. Podľa nového znenia, ak sa má záznam telekomunikačnej prevádzky použiť ako dôkaz, treba k nemu pripojiť písomný záznam, ktorý vyhotoví orgán Policajného zboru vykonávajúci odpočúvanie, pričom uvedie údaje o mieste, čase a zákonnosti vykonania odpočúvania. Do spisu sa zároveň založí doslovný prepis záznamu telekomunikačnej prevádzky, ktorý sa neutajuje, podpísaný orgánom, ktorý ho vyhotovil. Záznam telekomunikačnej prevádzky sa môže použiť ako dôkaz až po ukončení samotného odpočúvania telekomunikačnej prevádzky.

K malej „kozmetickej“ úprave došlo zákonom č. 253/2001 Z. z. účinnosťou od 1. novembra 2001. Pozmenená bola veta v druhom odseku § 88. Predošlá úprava považovala získaný záznam ako písomnosť obsahujúcu predmet štátneho tajomstva. Nová úprava túto vetu vypustila a nahradila vetou podľa ktorej sa s príkazom, ktorým sa nariadi odpočúvanie a záznam, nakladá ako s utajovanou skutočnosťou.

K významným zmenám došlo novelizáciou zákona o trestnom konaní súdnom, konkrétne zákonom č. 422/2002 Z. z. Prvou zmenu bolo doplnenie nového odseku do ustanovenia § 12, ktorý ponúka výklad niektorých pojmov. Nový ods. 13⁹ definuje čo sú informačno technické prostriedky a vymedzuje jednotlivé druhy takýchto prostriedkov, vrátane odpočúvania a záznamu telekomunikačnej prevádzky.

V prípade § 88 došlo k viacerým zásadným zmenám. Do prvého odseku bolo zakomponované, že ak sa pri odpočúvaní a zaznamenávaní telekomunikačných činností zistí, že obvinený komunikuje so svojím obhajcom, takto získané informácie nie je možné na účely trestného konania použiť a musia sa predpísaným spôsobom bezodkladne zničiť; to neplatí, ak ide o informácie, ktoré sa vzťahujú na vec, v ktorej obhajca nezastupuje obvineného. Je možné konštatovať, že zostala zachovaná pôvodná myšlienka, ktorá bola obsiahnutá aj v predošliých zneniach, že komunikácia medzi obhajcom a obvineným nemôže byť predmetom odpočúvania, resp. záznamu. Nové znenie bližšie špecifikuje daný zákaz.

⁸ § 158 Trestného zákona (140/1961 Zb.): „Zneužívanie právomoci verejného činiteľa

(1) Verejný činiteľ, ktorý v úmysle spôsobí inému škodu alebo zadovážiť sebe alebo inému neoprávnený prospech

a) vykonáva svoju právomoc spôsobom odporujúcim zákonu,

b) prekročí svoju právomoc, alebo

c) nesplní povinnosť vyplývajúcu z jeho právomoci,

potresce sa odňatím slobody na šesť mesiacov až tri roky alebo peňažným trestom alebo zákazom činnosti.

(2) Odňatím slobody na tri roky až desať rokov sa páchatel potresce,

a) ak zadováží činom uvedeným v odseku 1 sebe alebo inému značný prospech,

b) ak spôsobí takým činom vážnu poruchu v činnosti podniku alebo organizácie, alebo

c) ak spôsobí takým činom značnú škodu alebo iný obzvlášť závažný následok.“

⁹ § 12 ods. 13 zákona o trestnom konaní súdnom: „Informačno-technickými prostriedkami sa na účely tohto zákona rozumejú elektrotechnické, rádiotechnické, fototechnické, optické, mechanické, chemické a iné technické prostriedky a zariadenia alebo ich súbory použité utajovaným spôsobom pri odpočúvaní a zázname telekomunikačných činností (§ 88) alebo vyhotovovaní obrazových, zvukových alebo iných záznamov (§ 88e), ak sa ich použitím zasahuje do základných ľudských práv a slobôd.“

V novej úprave pribudol odsek druhý, ktorý pojednáva o vydaní príkazu. Podľa nového znenia príkaz na odpočúvanie a záznam telekomunikačných činností vydáva písomne pred začatím trestného stíhania a v **prípravnom konaní sudca na návrh prokurátora, v konaní pred súdom aj bez takého návrhu sudca alebo predsedu senátu**. Špecifikoval sa aj postup v prípade ak vec neznesie odklad. V takomto prípade ak ide o vec, ktorá neznesie odklad, a písomný príkaz sudcu nie je možné získať vopred, môže pred začatím trestného stíhania vydať príkaz **prokurátor**, avšak len ak odpočúvanie a záznam telekomunikačných činností nie je spojený so vstupom do bytu iného. Takýto príkaz vydaný prokurátorom musí byť najneskôr do 24 hodín od jeho vydania potvrdený sudcom, inak by stratil platnosť, a všetky získané informácie by nebolo možné použiť na účely trestného konania a musia byť predpísaným spôsobom bezodkladne zničené.

K výraznej zmene došlo v odseku treťom (podľa novej úpravy je to odsek štvrtý). Kým predošlé znenie umožňovalo v trestnom konaní pre iný trestný čin, než je špecifikovaný v prvom odseku, nariadiť odpočúvanie a záznam telekomunikačnej prevádzky, resp. ho vykonať aj samotnému orgánu činnému v trestnom konaní, tak podľa nového znenia môže v takomto prípade príkaz vydať pred začatím trestného stíhania a v prípravnom konaní sudca na návrh prokurátora, v konaní pred súdom aj bez takého návrhu sudca alebo predsedu senátu. Zároveň zostala zachovaná podmienka, že takýto postup je možný len so súhlasom dotknutého účastníka, voči ktorému smeruje odpočúvanie, resp. záznam.

Pôvodný odsek štvrtý bol rozdelený do dvoch odsekov. Text však zostal zachovaný. Pôvodný štvrtý odsek bol teda rozdelený po novom na odsek piaty a odsek siedmy. Z uvedeného vyplýva, že do novej úpravy bol zakomponovaný nový odsek šiesty. V zmysle nového odseku je orgán policajného zboru, ktorý vykonáva odpočúvanie, resp. záznam, povinný sústavne skúmať trvanie dôvodov, pre ktoré bol vydaný príkaz na odpočúvanie, resp. záznam. Zároveň dodáva, že ak pominuli dôvody, odpočúvanie a záznam telekomunikačných činností sa musí skončiť, a to aj pred uplynutím šesť mesačnej lehoty, ktorá je bližšie špecifikovaná v treťom odseku. Policajnému zboru zároveň vzniká zákonná povinnosť pominutia dôvodov, pre ktoré bol príkaz vydaný, bezodkladne písomne oznámiť, tomu orgánu, ktorý takýto príkaz vydal.

Nová úprava v dôsledku pribudnutia, ale aj rozdelenia obsahovala nových osem odsekov.

Ďalšia legislatívna zmena bola zrealizovaná zákonom č. 457/2003 Z. z. s účinnosťou od 1. 12. 2013. Paragrafové znenie 88 zákona bolo doplnené o dva nové odseky. Prvým bol odsek deviaty v zmysle ktorého fyzická alebo právnická osoba vykonávajúca telekomunikačnú činnosť bola povinná poskytnúť dotknutým subjektom (orgánom činným v trestnom konaní alebo súdu), v závislosti od štádia trestného konania, potrebné údaje o uskutočnenej telekomunikačnej činnosti, ktoré sú predmetom telekomunikačného tajomstva. Desiaty odsek dodáva, že príkaz na zaistenie a oznámenie údajov o uskutočnenej telekomunikačnej činnosti sa musí vydať písomne a musí byť odôvodnený.

Táto zmena bola zároveň poslednou legislatívnou zmenou, vzhľadom na prijatie zákona č. 301/2005 Z. z. Trestného poriadku v znení neskorších predpisov.

Nový rekodifikovaný Trestný poriadok priniesol so sebou množstvo zmien. Pokiaľ sa jedná o odpočúvanie a záznam telekomunikačnej prevádzky, tak úvodné vymedzenie informačno technických prostriedkov bolo obsiahnuté v § 10 ods. 20. Ustanovenie vymedzovalo jednotlivé informačno technické prostriedky, vrátane odpočúvania a záznamu telekomunikačnej prevádzky. Bližšie špecifikoval následne spracúvanie záznamov, ktoré sa riadi osobitným záko-

nom. V záverečnej časti apeluje na povinnosť vybraných subjektov¹⁰ poskytnúť súčinnosti pri realizácii jednotlivých informačno technických prostriedkov.

Odpočúvanie a záznam telekomunikačnej prevádzky bol v novom Trestnom poriadku vymedzený v § 115. Ustanovenie bolo rozdelené do deviatich odsekov.

V prvom odseku boli zadefinované základné podmienky využitia záznamu a odpočúvania. Príkaz na odpočúvanie a záznam mohol byť v zmysle novej právnej úpravy vydaný v dvoch prípadoch:

1. „V trestnom konaní

- a. O zločine, o trestných činoch korupcie, o trestnom čine zneužívania právomoci verejného činiteľa, trestnom čine legalizácie príjmu z trestnej činnosti alebo pre iný úmyselný trestný čin, o ktorom na konanie zaväzuje medzinárodná zmluva,
- b. Ak možno dôvodne predpokladať, že budú zistené skutočnosti významné pre trestné konanie.

2. V trestnom konaní

- a. Pre iný úmyselný trestný čin, ako je uvedený v bode 1,
- b. Iba so súhlasom užívateľa odpočúvaného alebo zaznamenávaného telekomunikačného zariadenia.¹¹

Druhá zákonná možnosť použitia odpočúvania, resp. záznamu len na základe súhlasu dotknutej osoby je vymedzená v ods. 5 Trestného poriadku.

V odseku prvom je zdôraznený zákaz realizácie odpočúvania, resp. záznamu medzi obvineným a jeho obhajcom. Jedinou výnimkou je, že sa nejedná o vec, v ktorej advokát obvineného zastupuje.

Príkaz na odpočúvanie a záznam vydáva v konaní pred súdom predseda senátu. V rámci prípravného konania alebo aj pred začatím trestného stíhania to je sudca pre prípravné konanie na návrh prokurátora. Ak vec neznesie odklad je oprávnený vydať príkaz aj prokurátor, avšak len v prípravnom konaní alebo pred začatím trestného stíhania. Podmienkou je aj, že príkaz sudcu pre prípravné konanie nie je možné v danom momente získať vopred a samotné odpočúvanie, resp. záznam prevádzky, nie je spojený so vstupom do obydlija. Príkaz vydaný prokurátorom musí byť do 24 hodín potvrdený sudcom pre prípravné konanie, inak stratí platnosť a všetky získané informácie musia byť bez meškania zničené.

Odsek tretí vymedzuje ďalšie zákonne podmienky. Príkaz na odpočúvanie musí byť písomný a odôvodnený skutkovými okolnosťami, osobitne na každú účastnícku stanicu, resp. zariadenie. Osoba, ktorej sa odpočúvanie, resp. záznam týka musí byť určená, pokiaľ je známa. Realizácia odpočúvania, resp. záznamu môže trvať šesť mesiacov, pričom ustanovenie tretieho odseku umožňuje predĺženie o ďalšie dva mesiace, a to aj opakovanie. Avšak predĺženie je možné len v rámci prípravného konania na návrh prokurátora. Príkaz na odpočúvanie a záznam telekomunikačnej prevádzky má povahu rozhodnutia sui generis, nejde teda o uznesenie. Z tohto dôvodu nie je proti nemu prípustný opravný prostriedok a dotknutá osoba nemá možnosť domáhať sa ochrany pred všeobecným súdom v súvislosti s faktom, že jej telefonický hovor bol odpočúvaný. Podľa názoru Ústavného súdu (nález I. ÚS 274/2005) oprávnenosť vydania právoplatného príkazu nemôže všeobecný súd preskúmať, a to práve preto, lebo príkaz je právoplatným rozhodnutím, ktorým je súd viazaný, resp. z ktorého musí vychádzať. Vzťahuje sa to tak na trest-

¹⁰ Prevádzkovatelia verejných telefónnych sietí, poskytovatelia elektronických telekomunikačných sietí, poskytovatelia elektronických telekomunikačných služieb, poštový podnik, dopravcovia a iní zasielateľia a ich zamestnanci sú povinní poskytnúť nevyhnutnú súčinnosť pri použití informačno-technických prostriedkov; pritom sa nemôžu dovoliavať povinnosti mlčanlivosti podľa osobitných zákonov.

¹¹ IVOR, J. kolektív. 2006. *Trestné práv procesné*. Bratislava: IuraEdition. 2006, s. 402.

né konanie, ako aj na prípadné občianskoprávne konanie na ochranu osobnosti (na ochranu súkromia).¹²

Zákonnou povinnosťou policajta, resp. útvaru Policajného zboru, ktorý je zo zákona oprávnený realizovať odpočúvanie a záznam, je sústavne skúmať dôvody, na základe ktorých bolo odpočúvanie alebo záznam umožnený. Ak by pominula existencia dôvodov, ktoré viedli k vydaniu príkazu je povinný odpočúvanie a záznam ukončiť. Táto skutočnosť musí byť bez meškania písomne oznámená orgánu, ktorý príkaz vydal a v rámci prípravného konania aj prokurátorovi.

Pokiaľ je potrebné použiť záznam ako dôkaz, musí byť v takomto konaní striktné dodržaný postup, ktorý je vymedzený v šiestom odseku. V takomto prípade príslušník Policajného zboru vyhotoví doslovný prepis, pričom uvedie údaje o mieste, čase, zákonnosti odpočúvania, ktoré realizoval. „Do spisu sa zakladá prepis záznamu telekomunikačnej prevádzky, ktorý sa neutajuje, podpísaný príslušníkom Policajného zboru, ktorý ho vyhotovil; ak doslovný prepis telekomunikačného záznamu obsahuje utajovanú skutočnosť, utajuje sa podľa osobitného predpisu.“¹³ Osobitným predpisom je zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností.¹⁴ Základnou podmienkou je, že záznam sa môže použiť ako dôkaz, až po ukončení realizácie odpočúvania a záznamu telekomunikačnej prevádzky.

Prepis nie je potrebný v prípade prebiehajúceho prípravného konania. V prípravnom konaní, ak to odôvodňujú okolnosti prípadu, možno predložiť záznam telekomunikačnej prevádzky súdu aj bez prepisu tohto záznamu, pokiaľ zo sprievodnej správy vyplývajú údaje o mieste, čase a zákonnosti vykonávania odpočúvania, ako aj o osobách, ktorých sa záznam telekomunikačnej prevádzky týka, a záznam telekomunikačnej prevádzky je zrozumiteľný. (§ 88 ods. 6)

Odpočúvanie a záznam telekomunikačnej prevádzky je možné použiť ako dôkaz aj v inej trestnej veci, avšak len ak sa súčasne aj v tejto veci vedie trestné konanie pre trestný čin vymedzený v odseku prvom.

Predposledný odsek stanovuje povinnosť bez meškania zničiť získané záznamy, ak sa nezistili skutočnosti významné pre trestné konanie, čo je jednou zo základných požiadaviek pre vydanie príkazu pre realizáciu odpočúvania a záznamu. O úkone, ktorým sa záznam zničí sa spíše zápisnica, ktorá je súčasťou spisu. „O zničení záznamu dotknutú osobu, ktorá nemá možnosť nazeráť do spisu, upovedomí orgán, ktorého rozhodnutím sa vec právoplatne skončila, a v konaní pred súdom predseda senátu súdu prvého stupňa do troch rokov od právoplatného skončenia trestného stíhania v danej veci; to neplatí ak sa koná o obzvlášť závažnom zločine alebo zločine spáchanom organizovanou skupinou, zločineckou skupinu alebo teroristickou skupinou, alebo ak sa na trestnom čine podieľalo viac osôb a vo vzťahu aspoň k jednému z nich nebolo trestné stíhanie právoplatne skončené, alebo ak by poskytnutím takej informácie mohol byť zmarený účel trestného konania.“¹⁵ Z uvedeného vyplýva, že osoba voči ktorej sa realizovalo odpočúvanie, resp. záznam musí byť do troch rokov oboznámená o tejto skutočnosti. Táto požiadavka vyplýva aj z medzinárodných normatívnych aktov, ako aj z judikatúry Európskeho súdu pre ľudské práva. Samotné zničenie sa robí najmä zmazaním, spálením, resp. iným efektívnym spôsobom. Zničenie sa týka tak záznamov, ako aj urobených prepisov.

¹² MINÁRIK, Š. a kolektív. 2010. *Trestný poriadok*. Stručný komentár, Druhé, prepracované a doplnené vydanie. Bratislava: IuraEdition. 2010, s. 372.

¹³ IVOR, J. kolektív. 2006. *Trestné práv procesné*. Bratislava: IuraEdition. 2006, s. 403.

¹⁴ IVOR, J. kolektív. 2006. *Trestné práv procesné*. Bratislava: IuraEdition. 2006, s. 404.

¹⁵ IVOR, J. kolektív. 2006. *Trestné práv procesné*. Bratislava: IuraEdition. 2006, s. 404.

Záverečný odsek stanovuje, že: „Postup podľa odsekov 1 až 8 možno primerane aplikovať aj na obsahové údaje alebo prevádzkové údaje, ktoré sú v reálnom čase prenášané prostredníctvom počítačového systému.“¹⁶

Pôvodná úprava nového Trestného poriadku z 1. januára 2016 predstavila novú úpravu, ktorá bola obsiahnutá v § 115 a bola rozdelená do deviatich odsekov. Úprava bola rozšírená aj o § 116. Ustanovenie umožňuje vydať príkaz na zaistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke. Naplnené však musia byť zákonné podmienky, a to:

- a) Trestné konanie o úmyselnom trestnom čine,
- b) Uskutočnená telekomunikačná prevádzka,
- c) Objasnenie skutočností dôležitých pre trestné konanie.

Samotný príkaz na zaistenie a oznámenie vydáva písomne predseda senátu v konaní pred súdom alebo sudca pre prípravné konanie v rámci prípravného konania, ako aj v štádiu pred začatím trestného stíhania a to na návrh prokurátora. Ustanovenie vyžaduje, aby bol príkaz odôvodnený, a to aj skutkovými okolnosťami.

Fyzické a právnické osoby, ktoré zabezpečujú telekomunikačnú prevádzku, majú zákonnú povinnosť oznámiť predsedovi senátu, resp. prokurátorovi alebo policajtovi, v závislosti od štádia trestného konania, údaje o uskutočnenej telekomunikačnej prevádzke. Uvedené sa vzťahuje aj na obsahové údaje alebo prevádzkové údaje prenášané prostredníctvom počítačového systému.

„Účelom tohoto inštitútu je najmä nutnosť zistenia, či preverenia skutočností dôležitých pre trestné konanie prostredníctvom oznámenia prevádzkovateľa telekomunikačnej prevádzky, prípadne zistenia údajov prenášaných prostredníctvom počítačového systému. Tieto skutočnosti sú predmetom telekomunikačného tajomstva alebo podliehajú ochrane osobných údajov.“¹⁷

Zmena rekodifikovaného Trestného poriadku prišla zákonom č. 262/2011 Z. z. a zákonom č. 220/2011 Z. z. s účinnosťou od 1. 9. 2011. Zmena nastala v odseku šiestom. „Záznam telekomunikačnej prevádzky sa na vhodných elektronických nosičoch uchováva v celosti v spise, ktorých kópie si môže vyžiadať prokurátor a obvinený alebo obhajca. Po ukončení odpočúvania a záznamu telekomunikačnej prevádzky si obvinený alebo obhajca môžu na svoje náklady vyhotoviť prepis záznamu telekomunikačnej prevádzky v rozsahu, v akom to uznajú za vhodné. Samotnú hodnovernosť prepisu posudzuje súd. Ak bol prepis záznamu vyhotovený v prípravnom konaní, predseda senátu môže nariadiť jeho doplnenie, ktoré vyhotoví príslušník Policajného zboru uvedený v prvej vete.“ (§ 115 ods. 6)

Novelizácia ustanovenia § 115 bola zrealizovaná zákonom č. 204/2013 Z. z. s účinnosťou od 1. augusta 2013. Do odseku prvého pribudla nová skutková podstata trestných činov extrémizmu, pre ktoré mohol byť vydaný príkaz na odpočúvanie a záznam telekomunikačnej prevádzky.

Pomerne významná zmena prišla novelizáciou Trestného poriadku a na základe nálezu Ústavného súdu, ktorý bol uverejnený v Zbierke zákonov pod č. 139/2015 Z. z. Na základe uvedeného nálezu bol vypustený z ustanovení Trestného poriadku celý § 116, ktorý pojednával o možnosti vydať príkaz na zaistenie a oznámenie údajov uskutočnenej telekomunikačnej prevádzky.

Zásadné zmeny nastali novelizáciou s účinnosťou od 1. januára 2016. v prvom prípade došlo k úprave odseku prvého, v jeho druhej časti. V zmysle nového znenia je možné vydať príkaz na odpočúvanie a záznam telekomunikačnej prevádzky, ak nie je možné sledovaný účel (zistiť sku-

¹⁶ MINÁRIK, Š. a kolektív. 2010. *Trestný poriadok*. Stručný komentár, Druhé, prepracované a doplnené vydanie. Bratislava: IuraEdition. 2010, s. 375.

¹⁷ MINÁRIK, Š. a kolektív. 2010. *Trestný poriadok*. Stručný komentár, Druhé, prepracované a doplnené vydanie. Bratislava: IuraEdition. 2010, s. 376.

točnosti významné pre trestné konanie), dosiahnuť inak alebo ak by bolo jeho dosiahnutie iným spôsobom podstatne sťažené. Znamená to, že je potrebné využiť všetky iné dostupné trestnoprosesné prostriedky na zistenie skutočností významných pre trestné konanie.

Ďalšia modifikácia nastala v záverečnej časti § 115. Pôvodný § 8 bol rozdelený do dvoch nových odsekov (ods. 8 a ods. 9), pričom došlo aj k textovej zmene. O zničení záznamu v prípade, kedy sa nezistili skutočnosti významné pre trestné konania, je potrebné informovať dotknutú osobu, ak je známa. O zničení záznamu informuje polícia, prokurátor alebo predseda senátu, ktorých rozhodnutím sa právoplatne vec skončila. Informáciu poskytuje orgán, ktorý vydal rozhodnutie, ktorým sa vec právoplatne skončila (v konaní pred súdom to je predseda senátu súdu prvého stupňa), a to v lehote do troch rokov od právoplatného skončenia trestného stíhania v danej veci. Takáto informácia má v zmysle dikcie ustanovenia obsahovať označenie súdu, ktorý vydal alebo potvrdil príkaz na odpočúvanie a záznam telekomunikačnej prevádzky, dĺžku odpočúvania a dátum jeho ukončenia. Významnou súčasťou informácie je aj poučenie možností podať návrh na preskúmanie zákonnosti príkazu na odpočúvanie a záznam. Návrh môže oprávnená osoba podať v lehote dvoch mesiacov od doručenia informácie. Podať ho možno na najvyšší súd.

V zmysle odseku 10 vyššie uvedené osoby nie sú povinné poskytnúť informáciu, ak ide o osobu, ktorá má možnosť nazeráť do spisu, alebo osobu v konaní o obzvlášť závažnom zločine alebo zločine spáchanom organizovanou skupinou, zločineckou skupinou alebo teroristickou skupinou, alebo ak sa na trestnom čine podieľalo viac osôb a vo vzťahu aspoň k jednému z nich nebolo trestné stíhanie právoplatne skončené, alebo ak by poskytnutím takej informácie mohol byť zmarený účel trestného konania.

Nový odsek 11 zachoval myšlienku pôvodného odseku 9, a teda že všetky odseky (1 až 10) § 115 sa rovnako vzťahujú na údaje, ktoré sú v reálnom čase prenášané prostredníctvom počítačového systému.

Do ustanovení Trestného poriadku bol opäť zakomponovaný § 116 s názvom Oznámenie údajov o telekomunikačnej prevádzke.

Odsek prvý vymedzuje trestné činy (prípady),¹⁸ ktoré umožňujú vydanie príkazu na zaistenie a oznámenie údajov o telekomunikačnej prevádzke, pričom príkaz je možné vydať, len ak nie je možné sledovaný účel dosiahnuť inak, resp. by bolo jeho dosiahnutie podstatne sťažené. Samotný príkaz musí byť písomný a odôvodnený aj skutkovými okolnosťami. Zároveň musí byť súčasťou príkazu aj spôsob, rozsah a lehota oznámenia údajov. Samotné zisťovanie môže trvať najviac šesť mesiacov, pričom odsek druhý umožňuje túto lehotu predĺžiť o ďalšie dva mesiace (to aj opakovanie), avšak len v prípravnom konaní. Príkaz vydáva predseda senátu, resp. sudca pre prípravné konanie v závislosti od štádia trestného konania.

Príkaz na zistenie a oznámenie údajov o telekomunikačnej prevádzke sa doručuje podniku poskytujúcemu verejné siete alebo služby. V prípade, že na základe vydaného príkazu neboli zistené skutočnosti významné pre trestné konanie, ten orgán ktorého rozhodnutím vec právoplatne skončila, takýto údaj bezodkladne zničí. Zápisnica o zničení údajov sa založí do spisu. O zničení údajov je nutné oboznámiť dotknutú osobu. Odsek štvrtý definuje všetky náležitosti takejto informácie, vrátane oprávnenia dotknutej osoby podať návrh na preskúmanie zákonnosti prí-

¹⁸ § 116 ods. 1: V trestnom konaní pre úmyselný trestný čin, za ktorý zákon ustanovuje trest odňatia slobody, ktorého horná hranica je najmenej tri roky, pre trestný čin ochrany súkromia v obydlí podľa § 194a, podvodu podľa § 221, nebezpečného vyhrážania podľa § 360, nebezpečného prenasledovania podľa § 360a, šírenia poplašnej správy podľa § 361, podnecovania podľa § 337, schvaľovania trestného činu podľa § 338, pre trestný čin, ktorým bola spôsobená ťažká ujma na zdraví alebo smrť alebo pre iný úmyselný trestný čin, pri ktorom na konanie zaväzuje medzinárodná zmluva.

kazu na zistenie a oznámenie údajov o telekomunikačnej prevádzke najvyššiemu súdu. Odsek piaty definuje komu nie sú oprávnené osoby takúto informáciu poskytnúť. Priorite ak ide o osobu, ktorá má možnosť nazeráť do spisu podľa tohto zákona alebo v konaní o obzvlášť závažnom zločine alebo zločine spáchanom organizovanou skupinou, zločineckou skupinou alebo teroristickou skupinou, alebo ak sa na trestnom čine podieľalo viac osôb a vo vzťahu aspoň k jednému z nich nebolo trestné stíhanie právoplatne skončené, alebo ak by poskytnutím takej informácie mohol byť zmarený účel trestného konania. Záverečný odsek § 116 len zdôrazňuje, že všetky ustanovenia sa vzťahujú aj na údaje prenášané prostredníctvom počítačového systému.

Uvedenou legislatívnou zmenou je ukončená historická analýza vývoja inštitútu odpočúvania a záznamu telekomunikačnej prevádzky. Táto posledná legislatívna zmena predstavuje zároveň aktuálnu úpravu tohto trestnoprocésneho inštitútu, ktorý je významným informačno-technickým prostriedkom.

Odpočúvanie a záznam telekomunikačnej prevádzky

K základnému rozdielu medzi odpočúvaním a záznamom sa vyjadruje Minárik:

„Odpočúvaním sa rozumie utajené a účelové vnímanie komunikácie medzi účastníkmi telekomunikačnej prevádzky, ktoré je sprostredkované telekomunikačnými zariadeniami tretej osobe.

Záznamom sa rozumie najmä proces zaznamenávania komunikácie prebiehajúcej podľa bodu 5 na príslušný nosič, ktorý umožní archiváciu a reprodukciu zaznamenananej komunikácie v budúcnosti, ako aj toho, čo takýto nosič obsahuje.“¹⁹

Samotná realizácia odpočúvania a záznamu telekomunikačnej prevádzky je zverená Policajnému zboru. „Odpočúvanie a záznam telekomunikačnej prevádzky vykonáva utajeným spôsobom príslušný útvar PZ, a to za použitia technických prostriedkov a zariadení, ktoré umožňujú takéto odpočúvanie a záznam. Hlavný cieľ tohto postupu je získanie informácií, ktoré sú dôležité pre trestné konanie.“²⁰

Odpočúvanie a záznam musí byť realizovaný v zmysle zákonnej úpravy, ktorá bola predstavená. Čentéš zároveň definuje niekoľko zásad, ktorých naplnenie je nevyhnutné, aby bol tento trestnoprocésny prostriedok účinný a bol naplnený jeho, v zákone vymedzený, účel.

Prvou je zásada legality. V zmysle tejto zásady musí byť odpočúvanie zákonné, musia byť naplnené všetky zákonné podmienky a dôvody na realizáciu.

Druhou je zásada legitimacy. Znamená, že orgány, ktoré rozhodujú o odpočúvaní a zaznamenávaní telekomunikačnej prevádzky, sú povinné zohľadňovať legitimitu zásahu do práva na súkromie, ktoré je garantované ústavou a medzinárodnými dokumentmi.

Treťou je zásada proporcionality, ktorá sa taktiež viaže na zásah do práva na súkromie, ktoré je narušané realizáciou odpočúvania a záznamu telekomunikačnej prevádzky. V zmysle tejto zásady je nevyhnutné neustále skúmať, či porušenie práva na súkromie neprekračuje medze spoločenskej nevyhnutnosti, či získanie skutočností dôležitých pre trestné konanie nie je možné dosiahnuť inak.

Zásada primeranosti a zdržanlivosti. Touto zásadou sa obmedzuje zásah do základných práv v prípadoch dovolených zákonom len v miere nevyhnutnej na dosiahnutie účelu trestného ko-

¹⁹ MINÁRIK, Š. a kolektív. 2010. *Trestný poriadok*. Stručný komentár, Druhé, prepracované a doplnené vydanie. Bratislava: IuraEdition. 2010, s. 376.

²⁰ TITĽOVÁ, M. 2015. *Korupcia. Vybrané kriminologické a trestnoprávne aspekty*. Bratislava: Wolters Kluwer. 2015, s. 125.

ania, pričom sa zvyrazňuje potreba rešpektovania dôstojnosti osôb a ich súkromia. Zmyslom tejto zásady je obmedziť na najnutnejšiu mieru akékoľvek zásahy do občianskych práv fyzických osôb. Výrazom zásady primeranosti je obmedzenie rozsahu trestných činov, v prípade ktorých možno nariadiť odpočúvanie a záznam telekomunikačnej prevádzky.²¹

Samotné odpočúvanie sa realizuje prostredníctvom technických prístrojov. Existujú viaceré technické možnosti. V prvom prípade to sú právnické osoby (operátor a prevádzkovateľ telekomunikačnej siete), ktoré musia v zmysle zákona poskytnúť súčinnosť. Operátor zaznamenáva hovory, textové správy, ako aj iné údaje o uskutočnenom hovore, ktoré musí poskytnúť orgánom činným v trestnom konaní, resp. súdu na základe ustanovenia § 10 ods. 21 Trestného poriadku v zmysle ktorého: „Prevádzkovatelia verejných telefónnych sietí, poskytovatelia elektronických telekomunikačných sietí, poskytovatelia elektronických telekomunikačných služieb, poštový podnik, dopravcovia a iní zasielateľia a ich zamestnanci sú povinní poskytnúť nevyhnutnú súčinnosť pri použití informačno-technických prostriedkov; pritom sa nemôžu dovolávať povinnosti mlčanlivosti podľa osobitných zákonov.“ Druhá možnosť je realizácia odpočúvania, samozrejme za zákonom splnených podmienok, Policajným zborom (Slovenskou informačnou službou), ktoré má špecifické pracoviská zameriavajúce sa na realizáciu odpočúvania.

Na zreteli je potrebné mať aj zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním), ktorý upravuje podmienky využívania informačno-technických prostriedkov. V zmysle predstaveného zákona je možné informačno-technické prostriedky, teda aj odpočúvanie a záznam telekomunikačnej prevádzky použiť len vtedy, ak je to v demokratickej spoločnosti nevyhnutné na zabezpečenie bezpečnosti štátu, obranu štátu, predchádzanie a objasňovanie trestnej činnosti alebo na ochranu práv a slobôd iných. Použitím informačno-technického prostriedku sa môže základné právo alebo sloboda obmedziť len v nevyhnutnom rozsahu a nie dlhšie, ako je to nevyhnutné na dosiahnutie zákonom uznaného cieľa, na ktorý slúži.²²

Záver

Na viacerých miestach prezentovanej štúdie bolo zdôraznené, že samotnou realizáciou odpočúvania, resp. záznamu telekomunikačnej prevádzky dochádza k výraznému zásahu do základných práv a slobôd dotknutej osoby. Špecifikom využívania tohto informačno-technického prostriedku je, že dotknutá osoba sa dozvie o realizácii tohto inštitútu až ex post.

Bez pochyb využíváním odpočúvania a záznamu je možné zistiť významné skutočnosti pre trestné konanie. Trestný poriadok však nabáda na prioritné využívanie iných dostupných trestnoprávných inštitútov prostredníctvom, ktorých je možné takéto informácie získať. Odpočúvanie a záznam, nakoľko sú realizované utajovaným spôsobom, však umožňujú získať hodnotné a hodnoverné informácie, ktoré môžu mať zásadný význam pre trestné konanie, resp. pre samotné rozhodovanie o vine a treste.

Na tomto mieste je preto nevyhnuté apelovať na všetky orgány, priority orgány činné v trestnom konaní a súdy, aby striktné dodržiavali zákonné podmienky nevyhnutné na využívanie tohto inštitútu. Absencia niektorej z podmienok (napr. nedostačujúce odôvodnenie príkazu, ktorým sa nariadi odpočúvanie), môže predstavovať zásadnú vadu, ktorá môže viesť k zmareniu

²¹ Pozri bližšie. ČENTĚŠ, J. 2013. *Odpočúvanie – procesnoprávne a hmotnoprávne aspekty*. Bratislava: C. H. Beck. 2013, s. 93.

²² Pozri bližšie: § 3 zákona č. 166/2003 Z. z. o ochrane pred odpočúvaním.

účelu trestného konania. Zároveň dochádza k narušeniu práva na súkromie u dotknutej osoby, ktorej, potom čo sa dozvie o realizácii odpočúvania vo vzťahu k nej, vzniká právo podať v lehote dvoch mesiacov návrh na preskúmanie zákonnosti príkazu na odpočúvanie a záznam telekomunikačnej prevádzky najvyššiemu súdu. Dotknutá osoba zároveň môže využiť aj iné dostupné prostriedky ochrany svojich osobnostných práv, ktoré sú garantované Ústavou, ako aj inými zákonnými normami nižšej právnej sily (napr. zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov). Aby bolo možné vyhnúť sa takýmto situáciám je nevyhnutné dodržiavať zásadu legality, legitimity a proporcionality, ktoré sú zárukou efektívnej a účinnej realizácie odpočúvania a záznamu telekomunikačnej prevádzky.

Zároveň je nutné brať do úvahy aj rozhodovaciu činnosť ústavného súdu, ako aj najvyššieho súdu, ktoré sú bez pochyb garantom práv jednotlivcov a zároveň svojou činnosťou dopĺňajú zákonné ustanovenia pojednávajúce o odpočúvaní a zázname telekomunikačnej prevádzky. Ako píše Čentéš: „Len taký záznam telekomunikačnej prevádzky (telekomunikačných činností), ktorý vyhovuje požiadavkám obsiahnutým v uvedených rozhodnutiach ústavného súdu a najvyššieho súdu, je v súlade s ústavným poriadkom a môže byť použiteľným dôkazom v trestnom konaní. Zároveň pri aplikovaní uvedeného inštitútu je potrebné rešpektovať právo na obhajobu v intenciách rozhodnutia najvyššieho súdu.“²³

Správnou zákonnou aplikáciou zo strany dotknutých orgánov a s prihliadnutím na rozhodovaciu činnosť ústavného súdu a najvyššieho súdu je možné garantovať, že odpočúvanie a záznam telekomunikačnej prevádzky bude efektívnym trestnoprávnym inštitútom, ktorým bude možné získať hodnotné informácie pre trestné konanie, pričom do základných práv a slobôd dotknutých osôb bude zasahované zákonným spôsobom.

Zoznam literatúry:

- ČENTÉŠ, J. 2013. *Odpočúvanie – procesnoprávne a hmotnoprávne aspekty*. Bratislava: C. H. Beck. 2013, s. 93
- ČENTÉŠ, J. 2012. Legalita, legitimita a proporcionalita odpočúvania a zaznamenávania telekomunikačnej prevádzky. In. *Magister Officiorum*. 2/2012. s. 27 ISSN: 1338-5569
- IVOR, J. a kol. 2010. *Trestné právo procesné*. Druhé, doplnené a prepracované vydanie. Bratislava: IuraEdition. 2010, s. 4037
- IVOR, J. kolektív. 2006. *Trestné právo procesné*. Bratislava: IuraEdition. 2006, s. 403
- KORGO, D. a kolektív. 2013. *Trestné právo procesné*. Plzeň: Aleš Čeněk. 2013, s. 196
- MINÁRIK, Š. a kolektív. 2010. *Trestný poriadok*. Stručný komentár, Druhé, prepracované a doplnené vydanie. Bratislava: IuraEdition. 2010, s. 370–371
- TITLOVÁ, M. 2015. *Korupcia. Vybrané kriminologické a trestnoprávne aspekty*. Bratislava: Wolters Kluwer. 2015, s. 125
- Zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov
- Zákon č. 351/2011 Z. z. o elektronických komunikáciách
- Zákon č. 141/1961 Zb. o trestnom konaní súdnom
- Zákon č. 249/1994 Z. z. o boji proti legalizácii príjmov z najzávažnejších, najmä organizovaných foriem trestnej činnosti a o zmenách niektorých ďalších zá
- Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností
- Zákona č. 166/2003 Z. z. o ochrane pred odpočúvaním
- Zákon č. 140/1961 Zb. Trestný zákon

²³ ČENTÉŠ, J. 2012. Legalita, legitimita a proporcionalita odpočúvania a zaznamenávania telekomunikačnej prevádzky. In. *Magister Officiorum*. 2/2012. s. 27.

Zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov

Zákon 178/1990 Zb. (novela zákona č. 141/1961 Zb. o trestnom konaní súdnom)

Zákon č. 558/1991 Zb. (novela zákona č. 141/1961 Zb. o trestnom konaní súdnom)

Zákon 247/1994 Zb. (novela zákona č. 141/1961 Zb. o trestnom konaní súdnom)

Zákon č. 366/2000 Z. z. (novela zákona č. 141/1961 Zb. o trestnom konaní súdnom)

Zákon č. 253/2001 Z. z. (novela zákona č. 141/1961 Zb. o trestnom konaní súdnom)

Zákon č. 422/2002 Z. z. (novela zákona č. 141/1961 Zb. o trestnom konaní súdnom)

Zákon č. 457/2003 Z. z. (novela zákona č. 141/1961 Zb. o trestnom konaní súdnom)

Zákon č. 262/2011 Z. z. a zákonom č. 220/2011 Z. z. (novela zákona č. 141/1961 Zb. o trestnom konaní súdnom)

Zákon č. 204/2013 Z. z. (novela zákona č. 141/1961 Zb. o trestnom konaní súdnom)

Nález I. ÚS 274/2005

Teoretické a praktické problémy odpočúvania a záznamu telekomunikačnej prevádzky v trestnom konaní¹

Theoretical and Practical Problems of Interception and Recording of Telecommunications in Criminal Proceeding

Marcela Tittlová²

Abstrakt: Odpočúvanie a záznam telekomunikačnej prevádzky v trestnom konaní predstavuje jednak zaistovací inštitút vo vzťahu k informáciám, no súčasne je to aj jeden z dôkazných prostriedkov a jeden z informačno-technických prostriedkov v trestnom konaní. Svojou povahou, ale hlavne utajeným spôsobom používania, smeruje k získavaniu pokiaľ možno čo najobjektívnejších a neskreslených informácií, ktoré sú významné pre trestné konanie. Na strane druhej, pomerne intenzívne tento inštitút zasahuje do oblasti základných ľudských práv a slobôd. V dôsledku tohto sa v ustanoveniach Trestného poriadku formulujú prísne podmienky, na ktorých splnenie sa použitie tohto prostriedku v trestnom konaní viaže. Aj napriek tomu, že úprava tohto inštitútu je pomerne podrobná, na mnohých miestach bol a je zákonodarca veľmi nedôsledný a nepresný. Výsledkom toho je celý rad teoretických a aj aplikačných problémov, ktoré ovplyvňujú možnosti využitia tohto prostriedku a informácií, ktoré sa prostredníctvom jeho získajú.

Abstract: Interception and recording of telecommunications in criminal proceedings is both locking Institute in relation to the information, but at the same time it is also one proof and one of the information-technical means in criminal proceedings. These means nature and mainly covert uses, toward acquiring as possible the most objective and unbiased information that is relevant for criminal proceedings. On the other hand, quite intense this institute interferes with fundamental human rights and freedoms. As a result of the provisions of the Criminal Procedure formulate strict conditions to which it will use this means of enforcement related. Although the treatment of this institute is quite detailed in many places was a legislator is very inconsistent and inaccurate. The result is a range of theoretical and application problems and affecting possibilities of this device and the information that through his profit.

Kľúčové slová: informačno-technické prostriedky, ľudské práva, vecná pôsobnosť, návrh a príkaz, časové súvislosti, informovanie dotknutých osôb, preskúmanie príkazu, použitie informácií v inej trestnej veci.

Keywords: information and technical resources, human rights, substantive scope, design and order, respect time, inform the persons concerned, review of the order, use the information in another criminal case.

Úvod

Odpočúvanie a záznam telekomunikačnej prevádzky v trestnom konaní predstavuje podľa systematického zaradenia druhý informačno-technický prostriedok, ktorá má v trestnom konaní povahu dôkazného prostriedku, ako aj zaistovacieho inštitútu vo vzťahu k informáciám, ktoré sú určitým spôsobom významné pre trestné konanie. Predstavuje moderný, spravodajským spôsobom vykonávaný a silne ofenzívny prostriedok využívaný tak v procese odhaľovania, ako aj v procese dokazovania korupčnej trestnej činnosti. Do úvahy je potrebné vziať tak jeho trestno-procesnú úpravu, teda v rámci trestného konania (na podklade ustanovení Trestného poriadku), ako aj nezávisle na ňom, čiže na podklade osobitných predpisov. V rámci trestného ko-

¹ Táto práca bola podporovaná Agentúrou na podporu výskumu a vývoja na základe Zmluvy APVV-15-0272.

² JUDr. Marcela Tittlová, PhD. Ústav verejného práva FP PEVŠ, Tomášikova 20, 821 02 Bratislava, marcela.tothova26@gmail.com.

ania ide o využitie tohto inštitútu na podklade § 115 Trestného poriadku (Zákon č. 301/2005 Z. z. v znení neskorších právnych predpisov, ďalej len „TP“ alebo „Trestný poriadok“). Výkon odpočúvania a záznamu telekomunikačnej prevádzky je zverený útvarom Policajného zboru, ktorý disponuje osobitnými, na tieto účely skonštruovanými zariadeniami, ktoré umožnia odpočúvanie a zaznamenávanie telekomunikačnej prevádzky. Mimo rámca trestného konania je možné použitie tohto prostriedku aj na podklade Zákona o ochrane osobných údajov, hoci týmito prostriedkami môžu disponovať a používať ich aj iné štátne zložky napríklad SIS, orgány Finančnej správy, útvary Policajného zboru, Zbor väzenskej a justičnej stráže. Súhrnne však platí, že pre Železničnú políciu, pre Finančnú správu a aj pre Zbor väzenskej a justičnej stráže tieto prostriedky využíva a ich použitie zabezpečuje Policajný zbor.³

1. Možnosti použitia s ohľadom na stret s rovinou ľudských práv

Odpočúvanie a záznam telekomunikačnej prevádzky predstavuje informačno-technický prostriedok, ktorý veľmi intenzívne zasahuje do oblasti základných ľudských práv. Okrem práva na súkromie a práva na rodinný život treba spomenúť aj právo na zachovávanie tajomstva ústne oznamovaných, súkromných správ a celý rad osobnostných práv, ktoré sú výkonom tohto inštitútu dotknuté. Okrem relevantného čl. 16 ods. 1 a 2 Ústavy SR (Zákon č. 460/1992 Zb. v znení neskorších ústavných zákonov, ďalej len „Ústava SR“) je potrebné poukázať aj na európsky či medzinárodný rozmer týchto práv, a to konkrétne na čl. 8 Dohovoru o ochrane základných ľudských práv. Tu sa jednak tieto práva garantujú, no súčasne sa uvádza, že sú možné určité zásahy do týchto práv, keďže to nie sú práva absolútne. Presne sa tu určujú podmienky, za splnenia ktorých je možné určité zásahy do týchto garantovaných práv považovať za ospravedlniteľné a za celkom legálne. Aby mohli štátne orgány do týchto garantovaných práv zasahovať, musia byť splnené podmienky, že ide o zásahy, ktoré:

³ Odpočúvanie a záznam telekomunikačnej prevádzky ako informačno-technický prostriedok možno použiť iba vtedy, ak je to v demokratickej spoločnosti nevyhnutné na zabezpečenie bezpečnosti štátu, obrany štátu, predchádzanie a objasňovanie trestnej činnosti alebo na ochranu práv a slobôd iných. Použitím informačno-technického prostriedku sa môže základné právo alebo sloboda obmedziť len v nevyhnutnom rozsahu a nie dlhšie, ako je to nevyhnutné na dosiahnutie zákonom uznaného cieľa, na ktorý slúži. Odpočúvanie a záznam telekomunikačnej prevádzky je možné využiť iba na základe predošlého písomného súhlasu zákonného sudcu a na nevyhnutný čas. Najdlhšie na 6 mesiacov. Lehota začína plynúť dňom udelenia súhlasu. Ak je nevyhnutné použiť naraz alebo následne niekoľko druhov informačno-technických prostriedkov, každý z nich možno použiť len v rozsahu výslovne udeleného súhlasu. Ak sa má tento informačno-technický prostriedok použiť v miestach, ktoré nie sú verejne prístupné, zákonný sudca rozhodne aj o tom, či sa súhlas vzťahuje aj na vstup na tieto miesta. Zákonný sudca, ktorý vydal pôvodný súhlas, môže na základe novej žiadosti dobu použitia predĺžiť, zakaždým však najviac o ďalších 6 mesiacov, ktoré začnú plynúť dňom udelenia ďalšieho súhlasu. Zákonný sudca, ktorý dal súhlas, je povinný sústavne skúmať trvanie dôvodov ich použitia. Ak dôvody pominuli, je povinný bezodkladne rozhodnúť o ukončení ich používania. PZ vo výnimočnom prípade, ak existuje dôvodné podozrenie z páchania trestného činu, pri ktorom možno použiť tento informačno-technický prostriedok na plnenie úloh PZ, **vec neznesie odklad a súhlas zákonného sudcu nemožno vopred získať**, môže použiť informačno-technický prostriedok **aj bez** predchádzajúceho súhlasu. PZ je povinný **oznámiť začatie** použitia tohto informačno-technického prostriedku zákonnému **sudcovi do jednej hodiny** od začatia použitia informačno-technického prostriedku a predložiť zákonnému sudcovi **žiadosť** o použitie prostriedku **do 6 hodín** od začatia použitia tohto prostriedku; žiadosť musí obsahovať aj čas začatia použitia tohto informačno-technického prostriedku. Ak PZ **nedostane dodatočný písomný súhlas** zákonného sudcu **do 12 hodín od začiatku použitia** tohto prostriedku alebo ak zákonný sudca **nevyhoví** žiadosti o dodatočný súhlas, jeho použitie **sa bezodkladne skončí**. Takto získané informácie **nesmú byť použité** a musia byť **bezodkladne zničené**, o čom orgán štátu, ktorý ich zničil, bezodkladne písomne informuje zákonného sudcu.

- a.) sú v súlade so zákonom a
- b.) sú nevyhnutné v právnej a demokratickej spoločnosti v záujme zachovávanía alebo udržiavania národnej alebo aj medzinárodnej bezpečnosti, hospodárskeho blahobytu, prevencie nepokojov a trestnej činnosti, na účely ochrany zdravia alebo morálky, prípadne aj vtedy, ak je to potrebné na účely ochrany práv a slobôd iných osôb.

Ochrana týchto práv a možné zásahy štátnych orgánov do takýchto garantovaných práv boli viackrát aj predmetom posudzovacej a rozhodovacej činnosti ESLP. V jeho pomerne bohatej judikatúre k týmto otázkam je možné vidieť, ako sa súd pôvodne zasadzoval za absolútnu ochranu týchto práv, no postupne, hlavne pod vplyvom rozvoja organizovaných foriem zločinu, ktoré začali ohrozovať Európu a jej obyvateľov, sa priklonil k tomu, že predsa len určité zásahy do tohto práva sú možné. Sú síce možné, no je dôležité, aby boli naplnené všetky podmienky, ktoré postupne vo svojej judikatúre ESLP vykladal a interpretoval a v zásade možno povedať, že posudzoval. Výklad, ktorý k nim poskytoval je však výkladom veľmi prísny a striktným, keď súd ani také úpravy, ako je nemecká či britská, nepovažoval za dostatočné na to, aby splnili podmienky uvedené v čl. 8 Dohovoru a teda, aby sa zásahy do týchto práv dali považovať za súladné s touto úpravou. V súvislosti s možnými zásahmi do práv garantovaných v čl. 8 Dohovoru súd konštatoval, že ak majú byť tieto zásahy prípustné a ospravedlniteľné, tak musia byť určené jasné limity, podmienky a rovnako tak aj rámec pre použitie týchto prostriedkov.

Ešte v roku 1968 ESLP v rozhodnutí „Belgický jazykový zákon“⁴ považoval tieto práva (právo na súkromie, na ochranu rodinného života, komunikovaných skutočností) za tak zásadné, že ich považoval za práva absolútne. Priamo tu konštatoval, že štátne orgány nemajú za žiadnych okolností možnosť a ani oprávnenie zasahovať do takýchto práv. Pomerne za krátko, o desať rokov na to, v roku 1978 priamo v súvislosti s odpočúvaním a záznamom telekomunikačnej prevádzky konštatoval, že takéto zásahy do práva na súkromie možné síce sú, no musia splniť požiadavky, ktoré sú uvedené v čl. 8 ods. 2 Dohovoru. V prípade *Klass vs. Nemecko*⁵ vyjadril ESLP takýto názor a odôvodnil ho práve potrebou boja spoločnosti s rozmáhajúcim sa európskym organizovaným zločinom, ktorý ohrozuje Európu, jej štáty a jej obyvateľov a aj značným informačným a technologickým pokrokom spoločnosti. Povolil teda, že je možné sledovanie podozrivých osôb a na tieto účely sa dajú využívať aj prostriedky tajného dohľadu, ktorých úpravu obsahuje vnútroštátna právna úprava. ESLP tak vlastne sám vo svojej judikatúre povolil možnosť, že budú v právnych úpravách štátov existovať takéto prostriedky tajného dohľadu nad telekomunikáciami, avšak ich existencia a používanie musia smerovať k prevencii zločinnosti a s cieľom národnej bezpečnosti, teda len vo výnimočných prípadoch. V ustanovení čl. 8 ods. 2 Dohovoru nachádzame konštatovanie, že použitie týchto prostriedkov musí byť nevyhnutné a priamo nutné. Vo vzťahu k týmto pojmom nie je možné využívať ako synonymá pojmy „potrebný“ alebo „vhodný“. Uvedené požiadavky nevyhnutnosti a nutnosti sú tak veľmi striktné, že nie je možné s nimi narábať pružne v tom smere, že by sa pod túto požiadavku mohli zahrnúť prípady, kedy je použitie takýchto prostriedkov zasahujúcich do predmetných práv vhodné alebo ak by to bolo užitočné. Prostriedky tajného dohľadu nad telekomunikáciami nie sú prostriedkami, ktoré používajú demokratické a právne štáty. Sú to prostriedky, ktoré používajú štáty policajné, takže ak aj pripustíme ich používanie v štátoch právnych, tak toto je veľmi obmedzené a skutočne odôvodnené nutnosťou a nevyhnutnosťou spájajúcou sa s daným prípadom. Ak teda v právnych a demokratických štátoch existujú možnosti využívania takýchto prostriedkov, musí súčasne existovať aj dostatočný systém garancií nezneužitia týchto prostriedkov, resp. sys-

⁴ Rozsudok ESLP z 23. júla 1968 vo veci „Belgický jazykový zákon“.

⁵ Rozsudok ESLP zo 6. septembra 1978 vo veci *Klass a ostatní vs. Nemecko*.

tém záruk na účely ochrany týchto práv pred neoprávnenými zásahmi do nich a pred zneužitím takýchto prostriedkov. Podmienky použitia takýchto prostriedkov musia vždy stanovovať právne predpisy – zákony. Obsahujú komplex podmienok a požiadaviek, ktoré je potrebné naplniť na to, aby sme mohli uvažovať o legálnych zásahoch do predmetných ľudských práv. Kritériá pre posúdenie týchto záruk sú veľmi variabilné a líšia sa vzhľadom na rôzne prípady. Do úvahy však možno vziať:

- a.) podstatu a tiež aj trvanie (dobu použitia) týchto prostriedkov tajného dohľadu,
- b.) rozsah, v akom sa tieto prostriedky tajného dohľadu používajú,
- c.) právny základ, na podklade ktorého je možné doceliť vydanie príkazu alebo povolenia na použitie takýchto prostriedkov,
- d.) kontrolný mechanizmus pre využívanie týchto prostriedkov,
- e.) povahu a druh štátneho orgánu, ktorý má možnosť vydať povolenie alebo príkaz na použitie týchto prostriedkov,
- f.) dostupné opravné prostriedky, ktorými je možné dosiahnuť preskúmanie rozhodnutia, ktorým sa udelil súhlas, povolilo, nariadilo použitie takýchto prostriedkov.

Práve tieto kritériá ESLP vo svojej rozhodovacej činnosti posudzoval veľmi prísne a striktné. Už vo vyššie zmienenom prípade *Klass vs. Nemecko* súd konštatoval, že nemecká právna úprava nie je dostačujúca z hľadiska existujúcich garancií a limitov pre zásahy do práva na súkromie. Neposkytuje ani dostatočné garancie pred zneužitím nástrojov tajného dohľadu nad telekomunikáciami. Rovnako takýto záver vyslovil ESLP vo veci *Malone vs. Veľká Británia*.⁶ Aj tento prípad sa priamo dotýkal odpočúvania a záznamu telekomunikačnej prevádzky (už uskuutočnenej). Tu ESLP len znova zdôraznil to, čo už raz konštatoval v prípade *Klass vs. Nemecko*, keď uviedol, že právne úpravy, ktoré dovoľujú využívanie prostriedkov tajného dohľadu, musia byť dostatočne jasné, presné a musia vytvárať systém dostatočných garancií ochrany dotknutých práv a nezneužívania dotknutých inštitútov. Konštatoval tiež, že ani britský zákon nespĺňa tieto požiadavky, keďže z hľadiska formulácie, ktorú obsahuje, je nadmerne vágny. Orgány výkonnej moci síce môžu mať k dispozícii voľnú úvahu, no táto nemôže byť neohraničená. Aj tieto orgány musia byť pri svojej voľnej úvahe ako jednom z ich oprávnení dôsledne limitované a obmedzované. Priamo zákon by mal určiť rámec voľnej úvahy pre tieto orgány a to tak, aby sa z hľadiska jednotlivcov poskytovala aj dostatočná ochrana ich práv. Do práva na súkromie a aj do práva na ochranu korešpondencie, do práva na rodinný život veľmi intenzívne zasahujú prostriedky tajného dohľadu. Tak samotné odpočúvanie a záznam telekomunikačnej prevádzky, ako aj mnohé iné informačno-technické prostriedky alebo prostriedky operatívno-pátracej činnosti, veľmi intenzívne zasahujú do týchto práv. Ak sa majú povoliť takéto zásahy do práv jednotlivcov, tak súčasne s týmto musia právne úpravy stanovovať aj dostatočný systém garancií pred svojvoľným, neoprávneným, neopodstatneným či nezákonným používaním a výkonom týchto prostriedkov. Každému sa musí garantovať takáto ochrana jeho práv v zmysle Dohovoru a preto aj vnútroštátne predpisy musia byť dostatočne jasné a presné, musia smerovať k dosahovaniu legitímneho cieľa a, prirodzene, použitie týchto prostriedkov musí splniť aj test proporcionality. Aj k takému-to záveru dospel ESLP vo svojom rozhodnutí *Kopp vs. Švajčiarsko*.⁷

⁶ Rozsudok ESLP z roku 1984 vo veci *Malone vs. Spojené kráľovstvo*.

⁷ Rozsudok ESLP zo dňa 25. 3. 1998 vo veci *Kopp vs. Švajčiarsko*, § 64, § 72 a § 75.

2. Odpočúvanie a záznam telekomunikačnej prevádzky ako trestno-procesný inštitút

V rámci trestného konania sa tento prostriedok považuje za jeden z informačno-technických prostriedkov a súčasne aj za jeden zo zaistovacích inštitútov vo vzťahu k informáciám dôležitým pre trestné konanie. V literatúre sa niekedy označuje aj ako malý alebo ako telefonický odposluch.⁸ Veľmi vhodne sa využíva jednak v procese odhaľovania, no súčasne aj v procese dokazovania korupčnej trestnej činnosti. Svojou povahou sa označuje ako informačno-technický prostriedok, hoci to nie je celkom tak. Ide iba o konkrétnu činnosť – teda o odpočúvanie a zaznamenávanie telekomunikačnej prevádzky a táto sa vykonáva pomocou špeciálnej a na tieto účely vyhotovenej techniky, pomocou informačno-technických prostriedkov. Aj preto sa tieto inštitúty niekedy samé označujú ako informačno-technické prostriedky (hoci ide len o konkrétnu činnosť vykonávanú pomocou nich).

Pomocou tohto inštitútu je možné získať cenné, viac menej objektívne informácie, ktoré budú dôležité pre trestné konanie. Je tomu tak s ohľadom na spravodajský spôsob jeho výkonu, ktorý predpokladá priamo ustanovenie § 10 ods. 21 TP, ktoré vymedzuje informačno-technické prostriedky v trestnom konaní. Teda dotknuté osoby nemajú a ani mať nemôžu v čase jeho použitia vedomosť o tom, že sa tieto prostriedky vo vzťahu k nim používajú. Priamo takýto výkon tohto prostriedku priamo predpokladá zákonná úprava. Ak by mali vedomosť o jeho používaní v určitom čase a na istom mieste, zrejme by prispôbili povahu svojho konania tak, aby sa pre trestné konanie zistili len bežné informácie, ktoré nasvedčujú úplne legálnym aktivitám a komunikácii, vzťahom. Práve spravodajský spôsob použitia týchto prostriedkov umožňuje získanie cenných a objektívnych poznatkov, ktoré sú z hľadiska trestného konania veľmi dôležité a významné. Veľmi efektívne sa za pomoci tohto prostriedku môžu získavať informácie o korupčnej trestnej činnosti, o korupčnej dohode a pod. Napríklad sú to cenné informácie o:

- a.) mieste aj čase, kedy korupčné konanie prebieha, prebiehalo, bude prebiehať,
- b.) plnení, ktoré má povahu úplatku a bude sa odovzdávať (preberať), prípadne, ktoré sa sľubuje alebo sa necháva sľúbiť si v budúcnosti (miesto budúceho plnenia, povaha budúceho plnenia, hodnota tohto plnenia a pod.),
- c.) tom, čo sa za úplatok poskytuje ako protihodnota,
- d.) všetkých osobách, ktoré sa určitým spôsobom podieľajú na korupčnej dohode a to tak v pozícii priamych subjektov (korumpovaný – korumpujúci), ako aj o sprostredkovateľoch, tretích osobách vystupujúcich pri nepriamej korupcii, pri plneniach, ktoré sa získavajú pre iné osoby (rodinných príslušníkov, priateľov a pod.),
- e.) niekedy aj o legendách, pomocou ktorých sa korupčné konanie zakrýva alebo aj o spôsoboch utajovania korupcie.

S ohľadom na povahu týchto informácií a na to, že spravodajský spôsob ich získavania umožňuje zadovážovať cenné a spravidla aj objektívne informácie pre trestné konanie, použitie tohto prostriedku v procese odhaľovania korupcie je veľmi významné. Navyše informácie, ktoré sa použitím tohto prostriedku získajú, ak je jeho použitie legálne, majú v trestnom konaní povahu dôkazu.

„Odpočúvanie a záznam telekomunikačnej prevádzky je trestno-procesný inštitút umožňujúci zaznamenávať telefónne hovory a iné skutočnosti oznamované prostredníctvom elektronic-

⁸ Tittlová, M.: Korupcia (vybrané kriminologické a trestnoprávne aspekty). Bratislava: Wolters Kluwer, 2015, s. 119 a nasl.

kej komunikačnej siete, ak sú svojim obsahom významné pre trestné konanie.“⁹ Nejde o prostriedok, ktorý by sa vzťahoval výhradne na skutočnosti komunikované prostredníctvom pevnej alebo mobilnej komunikačnej (telekomunikačnej) siete, ale vzťahuje sa aj na skutočnosti, ktoré sa oznamujú prostredníctvom faxov, prostredníctvom textových správ, na informácie komunikované elektronickou poštou aj vysielačkami. Trestno-procesne je to inštitút smerujúci k zaisťovaniu informácií dôležitých pre trestné konanie, ktorý sa silne dotýka vybraných ľudských práv. Z hľadiska aktuálnej trestno-procesnej úpravy, len ťažko možno diskutovať o tom, ako by túto právnu úpravu hodnotil ESLP z hľadiska naplnenia podmienok, ktoré stanovuje v čl. 8 ods. 2 Dohovoru a z hľadiska existencie systému záruk nezneužívania takýchto prostriedkov a dôslednej garancie ochrany ľudských práv. Naša trestno-procesná úprava, hoci stanovuje podmienky použitia tohto prostriedku a aj ďalšie aspekty jeho využívania, nie je v mnohých prípadoch celkom bezproblémová. V rámci našej úpravy sa riešia dôležité aspekty použitia tohto prostriedku, keď sa stanovuje:

- a.) okruh prípadov (trestných činov), pri odhaľovaní (a aj dokazovaní) ktorých sa môže tento prostriedok použiť,
- b.) štádium, kedy je možné tento prostriedok využiť,
- c.) subjekty, ktoré vzhľadom na určité štádiá trestného konania povoľujú použitie tohto prostriedku,
- d.) návrh na použitie tohto prostriedku,
- e.) príkaz, ktorým sa povoľuje použitie a jeho náležitosti (vrátane časového horizontu používania a možností predlžovania),
- f.) použitie získaných informácií ako dôkazov v trestnom konaní a, prípadne, aj podmienky použitia takto získaných informácií v inom trestnom konaní,
- g.) informovanie dotknutých osôb.

V tomto prípade ide o výpočet kritérií, podľa ktorých je možné hodnotiť právnu úpravu týchto prostriedkov z hľadiska súladnosti s európskou úpravou a aj z hľadiska možných zásahov do základných ľudských práv a slobôd. Týka sa to jednak samotného odhaľovania korupcie, ale aj procesu využívania informácií získaných za pomoci týchto prostriedkov v rámci dokazovania nielen korupčnej trestnej činnosti. V tejto časti práce sa bližšie venujeme práve tým aspektom trestno-procesnej úpravy, ktoré sú dôležité z hľadiska odhaľovania korupcie a v nasledujúcej sa venujeme dokazovaniu korupcie pomocou týchto prostriedkov. V oboch prípadoch je však potrebné mať na zreteli problematiku našej trestno-procesnej úpravy a to hneď vo viacerých smeroch.

3. Vecná pôsobnosť inštitútu v trestnom konaní

Ustanovenie § 115 ods. 1 TP vymedzuje okruh trestných činov, pri odhaľovaní (a následne aj dokazovaní) ktorých je možné tieto prostriedky použiť. V trestnom konaní o týchto trestných činoch je tak možné doceliť vydanie príkazu na použitie tohto prostriedku:

- a.) o zločinoch,
- b.) o korupčných trestných činoch,
- c.) o trestných činoch extrémizmu,
- d.) o trestných činoch legalizácie príjmov z trestnej činnosti,
- e.) o trestnom čine zneužívania právomoci verejného činiteľa,

⁹ Ivor, J. a kol.: Trestné právo procesné. Druhé, doplnené a prepracované vydanie. Bratislava: IURA EDITION, 2010, s. 403.

- f.) o inom úmyselnom trestnom čine, na konanie o ktorom Slovenskú republiku zaväzuje medzinárodná zmluva, ktorou je Slovenská republika viazaná,
 - ak súčasne pre tieto (vyššie uvedené) prípady platí, že je možné dôvodne predpokladať, že takto budú získané informácie dôležité pre trestné konanie a súčasne, ak takto sledovaný účel nie je možné dosiahnuť inak, prípadne, ak je dosiahnutie tohto účelu takýmto iným spôsobom podstatne sťažené,
- g.) o iných úmyselných trestných činoch, avšak výhradne so súhlasom užívateľa odpočúvaného a zaznamenávaného zariadenia.

To, že týmto postupom sa získajú poznatky významné pre trestné konanie, plyní ako *odôvodnený predpoklad* z materiálov, podkladov, ktoré sa získali pred tým. Nejde len o nejaký odhad, že by sa takéto poznatky mohli získať. Ide o predpoklad odôvodnený, čo vyjadruje vyššiu mieru istoty, že sa takéto poznatky cenné pre trestné konanie získajú. Podstatne viac možno predpokladať, že sa takéto významné poznatky pre trestné konanie týmto postupom získajú, ako že sa nezískajú. Súčasne je nutné mať na zreteli aj uvedenú *zásadu subsidiarity* a teda, že vždy, ak je to ešte možné a efektívne vzhľadom na vynaloženú námahu, náklady a pod., by sa mali takéto poznatky získavať miernejšími, menej intenzívnymi prostriedkami.

Trestno-procesná úprava tiež diferencuje možné použitie tohto prostriedku z hľadiska fázy trestného konania a tomu prispôsobuje aj okruh subjektov, resp. subjekty, ktoré majú možnosť vydať príkaz na použitie tohto prostriedku. Intenzívnosť zásahu do dotknutých ľudských práv je možné vidieť aj v tom, že tento prostriedok je možné využiť v:

- a.) postupe pred začatím trestného stíhania (teda už v štádiu, kedy ešte nevystupuje ani konkrétny obvinený, nezačalo ešte trestné stíhanie).
- b.) v prípravnom konaní,
- c.) v konaní pred súdom.

V závislosti od štádia trestného konania, v ktorom sa informačno-technické prostriedky využívajú, je odlišný aj subjekt, ktorý vydáva príkaz na ich použitie. V konaní pred súdom je to, jednoznačne, predseda senátu a v prípravnom konaní a v postupe pred začatím trestného stíhania, je to sudca pre prípravné konanie. Niekedy sa stretáme s názorom, že takto sa do určitej miery oslabuje postavenie prokurátora, ktoré je v predsúdnom konaní charakterizované ako *dominus litis*. V prípravnom konaní by prokurátor mal byť pánom tohto konania, avšak rozhodovanie o zásahoch do ľudských práv, v podstate o tých najzávažnejších zásahoch vlastne nie je oprávnený rozhodnúť. Má však významné návrhové oprávnenia, keďže je jediným subjektom, ktorému sa takéto oprávnenie priznáva a teda len a len prokurátor má možnosť podať takýto návrh. Vo vzťahu k vydaniu takéhoto príkazu má návrhové oprávnenie. O vydaní príkazu teda vždy a to aj v celom predsúdnom konaní, rozhoduje sudca pre prípravné konanie. Uvedenú konštrukciu nemožno vnímať celkom ako oslabenie pozície prokurátora v predsúdnom konaní, keďže mu je zverené dôležité, návrhové oprávnenie vo vzťahu k odposluchom. Nikto iný, len a len prokurátor má možnosť navrhnúť vydanie príkazu na použitie tohto inštitútu v predsúdnom konaní vo vzťahu k sudcovi pre prípravné konanie. Prokurátor teda sám má možnosť iniciovať použitie tohto prostriedku. Požiadavka na vydávanie príkazu súdom (sudcom pre prípravné konanie a v konaní pred súdom predsedom senátu) garantuje, že nutnosť a nevyhnutnosť využitia tohto inštitútu bude vždy posudzovať nestranný a nezávislý súd. Práve takéto posúdenie má zabezpečiť skutočne dôsledné preskúmanie návrhu a podmienok, ktoré je potrebné splniť pre vydanie príkazu a rozhodnutie vo veci nestranným a nezávislým súdom. Hlavne v postupe pred začatím trestného stíhania je tento informačno-technický prostriedok veľmi dôležitým inštitútom, pomocou ktorého sa preverujú podnety a konkrétnejšie trestné oznámenia. Práve tento inštitút umožňuje získať veľmi cenné informácie, ktoré determinujú ďalší postup vo

veci a prijímané rozhodnutia. Navyše, najmä v predsúdnom konaní je vhodné, že sa stanovuje požiadavka na súdne rozhodovanie o použití tohto inštitútu. Zabezpečuje sa tak vhodná judiciarita a teda rozhodovanie o vydaní príkazu sa prenáša na nestranný a nezávislý súd, neostáva len v rovine orgánov činných v trestnom konaní, u ktorých by sa možno dalo dosiahnuť vydanie príkazu jednoduchšie. Navyše, za samotné vydanie príkazu a použitie uvedeného inštitútu takto preberá zodpovednosť nestranný a nezávislý súd.

Môže sa stať, že vec neznesie odklad a v takto krátkej lehote, v časovej tiesni, nebude možné doceliť vydanie príkazu sudcom pre prípravné konanie. V týchto prípadoch sa dovoľuje, aby vydal predbežne príkaz aj prokurátor, no iba za splnenia nasledujúcich podmienok:

- a.) ide o prípad typický časovou tiesňou, kedy sa nedá z hľadiska časového dosiahnuť vydanie príkazu sudcom pre prípravné konanie,
- b.) ide o prípady, kedy sú naplnené podmienky pre vydanie príkazu a teda, ak by sa podával návrh sudcovi, tak je zrejme možné predpokladať, že aj sudca by príkaz na použitie týchto prostriedkov vydal,
- c.) ide o ojedinelú situáciu, vonkoncom nie o klasický postup,
- d.) odpočúvane a záznam telekomunikačnej prevádzky sa v tomto prípade nemôže spájať so vstupom do obydlija,
- e.) v lehote do 24 hodín od vydania príkazu prokurátorom je nutné, aby vydanie potvrdil sudca pre prípravné konanie; inak by sa poznatky, resp. informácie, ktoré sa aj použitím tohto prostriedku získali, nedali v trestnom konaní použiť, museli by sa predpísaným spôsobom zničiť a to aj bez ohľadu na to, že by sa mohli zistiť potenciálne informácie cenné pre trestné konanie.

4. Návrh, príkaz na použitie a časové súvislosti použitia v trestnom konaní

V trestno-procesných ustanoveniach nie je riešený žiadny minimálny rozsah náležitostí, ktoré by mal návrh prokurátora adresovaný súdu obsahovať. Jednoznačne možno súhlasiť s názorom, že tieto náležitosti determinujú samotný obsah príkazu a teda návrh by mal byť formulovaný tak, aby obsahoval všetky náležitosti, ktoré sa neskôr premietajú v príkaze na použitie tohto informačno-technického prostriedku. Okruh náležitostí návrhu tu však nie je výslovne riešený. Napríklad v Zákone o ochrane súkromia pred odpočúvaním, priamo v ustanovení § 4 ods. 3 sa uvádza výpočet náležitostí, ktoré by mal návrh (v tomto prípade žiadosť) obsahovať. Konkrétne by tak mala písomná žiadosť obsahovať:

- a.) popis informačno-technického prostriedku, ktorý sa má využiť,
- b.) miesto používania, ak to dovoľuje povaha tohto prostriedku,
- c.) navrhovaný čas používania.
- d.) údaje o osobe alebo osobách, voči ktorým sa má použiť,
- e.) informácie o predošlom postupe, ktorý bol neúčinný alebo sťažený pri odhaľovaní a dokumentovaní konkrétnej trestnej činnosti, na ktorú sa vzťahuje žiadosť,
- f.) dôvody pre použitie daného prostriedku.

Priamo sa stanovuje, že ak nemá žiadosť tieto náležitosti, sudca o nej nemôže rozhodnúť a vráti ju žiadateľovi. Takýmto spôsobom sa posilňuje zodpovednosť subjektu podávajúceho žiadosť o vydanie príkazu na použitie informačno-technického prostriedku a toto možno vítať aj v trestnom konaní. Pre prokurátora sa nestanovuje žiadny okruh náležitostí, ktoré by návrh mal mať. Stanovenie podobného okruhu náležitostí by do určitej miery posilnilo zodpovednosť prokurátora za formálnu a obsahovú stránku návrhu a uľahčilo rozhodovanie sudcov o podanom

návrhu. Takže zavedenie takéhoto alebo obdobného výpočtu možno len odporúčať. Tiež treba poukázať na aplikačný problém, tak ako uvádza aj Perhács,¹⁰ že to, že návrhy nemajú presne určené náležitosti, často spôsobuje ich rôzne posudzovanie z pohľadu posudzujúceho sudcu. Benevolentnejší sudca vydá príkaz aj na podklade návrhov o vydanie, ktoré by iný sudca považoval za nedostatočné a na ich podklade by príkaz nevydal. Často sa zo strany navrhujúcich subjektov priamo a vyslovene vyčkáva, kým bude službu konajúcim sudcom ten menej benevolentnejší, u ktorého sa vydanie príkazu docieli jednoduchšie a to, prirodzene, tiež nie je správny postup. Zavedenie uvedeného aspoň minimálneho výpočtu náležitostí návrhu aj do trestno-procesných ustanovení, by tak postup sudcov pri rozhodovaní o vydaní príkazu len uľahčili a zjednotili.

Príkaz ako forma rozhodnutia v trestnom konaní, sa povinne vydáva v písomnej forme a musí sa v každom prípade odôvodňovať. Kým všeobecné ustanovenia o príkaze ako forme rozhodnutia v trestnom konaní niekedy odôvodnenie ani nepožadujú, v prípade použitia informačno-technických prostriedkov sa priamo žiada, aby bol tento príkaz písomný a odôvodnený. Musí sa odôvodniť pre každú účastnícku linku alebo zariadenie osobitne. Okrem iného sa v príkaze uvádza aj údaj o dĺžke používania tohto prostriedku. Nejde o používanie jednorazové, teda z hľadiska časového trvá niekoľko týždňov, spravidla mesiacov. Najviac sa môže tento prostriedok používať, resp. povoliť jeho používanie na 6 mesiacov. V príkaze sa uvádza konkrétna dĺžka, konkrétna doba používania tohto prostriedku. Je tu aj možnosť dosiahnuť predĺženie tejto doby, znova na podklade žiadosti subjektu, ktorý pôvodne rozhodoval, a to vždy o ďalšie dva mesiace. Problém tohto ustanovenia je vo viacerých veciach. Jednak sa nestanovuje maximálna možná lehota, počas ktorej by bolo možné určité osoby odpočúvať a zaznamenávať ich komunikáciu a jednak toto ustanovenie nie je riešené z hľadiska lehôt. V prvom prípade ide o to, že nie je stanovená maximálna možná prípustná doba odpočúvania a zaznamenávania telekomunikačnej prevádzky a ani maximálny možný počet žiadostí o predĺženie. V zásade sa tak dá povedať, že odpočúvanie môže trvať niekoľko rokov a jeho trvanie je limitované len existenciou dôvodov na použitie tohto prostriedku. V zásade aj časovo neobmedzené, na podklade návrhov o predĺženie, by sa mohli osoby odpočúvať. Je tak možné klásť si otázku, kedy ešte existujú dôvody na použitie tohto informačno-technického prostriedku? Ak sa počas niekoľkých mesiacov nezistia skutočnosti dôležité pre trestné konanie, prečo by sa malo žiadať o predĺženie príkazu na použitie, a to opakovane a znova? Takto sa dostávame k tomu, že využitie tohto prostriedku je v zásade časovo neobmedzené a limitované len existenciou dôvodov pre jeho použitie. Navyše, z hľadiska lehôt, nie je riešené vôbec to, v akej lehote by mali útvary vykonávajúce odpočúvanie a záznam žiadať o predĺženie. Je zrejmé, že predlžovať platnosť možno len pri niečom, čo ešte trvá. Takže jednoznačne počas platnosti pôvodného príkazu. Nie je ale riešené v akom časovom horizonte pred uplynutím doby používania tohto prostriedku. Napríklad, pri väzbe je tento postup riešený. V prípade povoľovania predĺženia informačno-technických prostriedkov nie. Takže útvary môžu spokojne o predĺženie požiadať niekoľko málo dní pred uplynutím lehoty na odpočúvanie v pôvodnom príkaze a sudca sa dostane do veľmi zložitej pozície, kedy v krátkom čase bude musieť posúdiť opodstatnenie požiadavky na predĺženie príkazu. Alebo sa mu návrh doručí pomerne skoro a teda nemusí obsahovať aktuálne údaje a informácie. V oboch prípadoch je pozícia sudcu značne sťažená a keďže sa vo vzťahu k nemu bude vyvodzovať zodpovednosť za prípadné nepredĺženie príkazu alebo predĺženie v prípade, ak to nebolo nutné a nevyhnutné, tak by bolo správne zakotviť do tohto ustanovenia aj pre príslušné orgány určitú lehotu, v ktorej by mali o predĺženie požiadať tak, aby sudca mal k dispozícii dostatok času na preskúmanie tohto návrhu a rozhodnutie o ňom.

¹⁰ Perhács, Z., Perhácsová, A.: Právna úprava používania informačno-technických prostriedkov (2. časť). In *Justičná revue* č. 5/2013, s. 708.

Na druhej strane ale majú orgány realizujúce odposluchy povinnosť, a to kedykoľvek počas trvania príkazu na odpočúvanie a záznam telekomunikačnej prevádzky, dôsledne skúmať, či sú stále naplnené dôvody, pre ktoré sa nariadilo použitie tohto prostriedku. Ak by kedykoľvek aj počas trvania tohto príkazu zistili, že už pominuli dôvody pre odpočúvanie a záznam telekomunikačnej prevádzky, musia ukončiť odpočúvanie a túto skutočnosť oznámiť subjektu, ktorý vydal príkaz na použitie tohto prostriedku. V prípravnom konaní to oznamujú vždy aj prokurátorovi.

5. Použitelnosť získaných informácií a informovanie dotknutých osôb

Ako už bolo uvedené, odpočúvanie a záznam telekomunikačnej prevádzky je informačno-technický prostriedok a súčasne zaistovací inštitút vo vzťahu k informáciám dôležitým pre trestné konanie. Jeho použitie je veľmi cenné vzhľadom na spravodajský spôsob realizácie, kedy sa aj na účely odhaľovania závažnej trestnej činnosti získavajú veľmi cenné poznatky. Nie je však možné využívať také informácie, ktoré by sa zistili z rozhovorov obhajcu s jeho obvineným (obžalovaným). Takéto záznamy a ani informácie na nich zachytené sa nemôžu v trestnom konaní použiť. Podmienkou toho je, že:

- a.) ide o komunikáciu obhajcu s jeho obvineným (obžalovaným), ktorého tento advokát ako obhajca zastupuje v danom trestnom konaní,
- b.) ide o ich komunikáciu vo veciach, ktoré sa týkajú prípadu, v ktorom obhajca tohto obvineného zastupuje v trestnom konaní,
- c.) tieto informácie sa týkajú skutočností, ktoré sa spravidla stali v minulosti, teda nejde o prípady plánovanej trestnej činnosti, pripravovanej činnosti do budúcnosti.

Jednak obvinený (obžalovaný) má právo radiť sa so svojim obhajcom a to aj bez prítomnosti tretej osoby a súčasne aj obhajca má povinnosť zachovávať mlčanlivosť o skutočnostiach, o ktorých sa v rámci svojho povolania dozvedel. Jedinou výnimkou z tejto povinnosti je iná zákonná povinnosť – teda povinnosť oznámiť trestný čin, o ktorom sa hodnoverne z komunikácie s obvineným (obžalovaným) dozvie. Ak by sa takto dozvedel, že sa plánuje alebo pripravuje určitá trestná činnosť, potom má aj obhajca oznamovaciu povinnosť vo vzťahu k týmto trestným činom v zmysle relevantnej skutkovej podstaty. Problémom však je, že ak majú útvary vykonávajúce odpočúvanie a záznam telekomunikačnej prevádzky skutočne posúdiť komunikáciu osôb a navyše aj jej povahu, tak sa musia predsa len oboznámiť s jej obsahom a to pomerne dôkladne (aby vedeli, či ide skutočne o rozhovor vo veciach, v ktorých obhajca obvineného zastupuje). Aj keď takéto informácie a ani záznamy nemôžu v trestnom konaní použiť, tak predsa len už disponujú určitým poznatkom, ktorý takto získali a ten môže zamerať ich činnosť určitým smerom, ktorým by sa neuberala, keby tento poznatok nemali.

V slede posledných novelizácií trestných predpisov sa upravila povinnosť informovania dotknutých osôb o použití tohto prostriedku voči nim, čím sa im podstatne kvalitnejšie zabezpečilo právo domáhať sa ochrany svojich práv súdnou a inou cestou. Platí teda, že ak sa použitím tohto prostriedku nezistia skutočnosti dôležité pre trestné konanie, orgány činné v trestnom konaní alebo útvary Policajného zboru bezodkladne zničia takéto záznamy a zápisnicu zo zničenia zkladajú do spisu. Už toto ustanovenie je sporné z hľadiska toho, čo sa rozumie „skutočnosťami, ktoré nie sú významné pre trestné konanie“. Orgány činné v trestnom konaní majú v zmysle vyhládávacej zásady povinnosť vyhľadávať tak dôkazy svedčiacie v prospech ako aj v neprospech obvineného. Ak sa aj použitím tohto prostriedku zistia skutočnosti, ktoré by nepreukazovali, vyvracali alebo poľahčovali vinu konkrétnej osoby alebo podozrenie z určitej trestnej činnosti,

stále sú to skutočnosti významné a dôležité pre trestné konanie. Na ich základe sa v tomto konaní prijímajú ďalšie rozhodnutia a uvedené skutočnosti môžu byť aj základom pre meritórne rozhodnutie vo veci. Pre to nemožno túto formuláciu považovať za vhodne zvolenú. A v konečnom dôsledku je nutné sa zamyslieť nad tým, že ak sa aj získajú poznatky, ktoré vyvracajú vinu konkrétnej osoby alebo ju nepreukazujúce poznatky, poznatky vyvracajúce alebo nepreukazujúce podozrenie z určitej trestnej činnosti, aj toto sú relevantné dôkazy pre trestné konanie. Je tak otázne, prečo by sa mali v trestnom konaní zničiť a prečo by nemali ostať zachované do budúcnosti ako jeden z dôkazov, na základe ktorého sa rozhodlo pre prípadné budúce štádiá trestného konania.

Osoby dotknuté odpočúvaním a záznamom telekomunikačnej prevádzky sa musia o tomto zničení záznamu informovať, ak sú známe. Povinnosť informovať ich má polícia alebo prokurátor, ktorých rozhodnutím vec právoplatne skončila v konaní pred súdom, je to predseda senátu súdu I. stupňa, ktorým vec právoplatne skončila. Stanovuje sa na tieto účely lehota do 3 rokov od právoplatného skončenia trestného stíhania. Toto informovanie sa realizuje, prirodzene, až po zničení záznamov a po právoplatnom skončení veci. Táto informácia musí obsahovať nasledovné údaje:

- a.) označenie súdu, ktorý vydal alebo ktorý potvrdil príkaz na použitie tohto prostriedku,
- b.) dĺžku odpočúvania a
- c.) dátum ukončenia odpočúvania,
- d.) poučenie o možnosti (o práve) podania žiadosti na preskúmanie zákonnosti príkazu (v lehote dvoch mesiacov od doručenia) NS SR.

Takúto informáciu musí dotknutej osobe podať orgán, ktorého rozhodnutím vec právoplatne skončila v lehote do 3 rokov od právoplatnosti rozhodnutia, ktorým táto vec skončila. Takéto informácie sa však nepodávajú v prípade, ak ide o osoby, ktoré majú právo nahliadať do spisov podľa Trestného poriadku, alebo ak sa vedie trestné konanie pre obzvlášť závažný zločin, pre zločiny spáchané teroristickou, zločineckou či organizovanou skupinou, alebo ak sa na trestnom čine podieľalo viac osôb a ešte vo vzťahu aspoň k jednému z nich nebolo trestné stíhanie právoplatne zastavené (skončené), prípadne, ak by poskytnutie tejto informácie mohlo smerovať k zmareniu účelu trestného stíhania.

Táto úprava nadobudla účinnosť od 1. januára 2016, pričom išlo o novelizáciu zákonom č. 397/2015 Z. z. Nadväzne na možnosť dotknutých osôb domáhať sa preskúmania príkazu na NS SR sa zaviedli nové ustanovenia týkajúce sa tohto konania. Konkrétne ide o nové ustanovenia § 362f a § 352g TP, kde sa stanovuje, že ak podáva dotknutá osoba takýto návrh, NS SR preskúmava na verejnom zasadnutí tento príkaz. Pred rozhodovaním si vyžiada stanovisko sudcu, ktorý rozhodoval o vydaní alebo potvrdení príkazu. Ak by zistil, že príkaz sa vydal alebo vykonal v rozpore so zákonom, formou uznesenia vyslovuje porušenie zákona. Toto jeho rozhodnutie je konečné a nie je voči nemu možné podať žiadny opravný prostriedok. Rovnako tak, ale aj keby NS SR konštatoval, že nedošlo k vydaní, alebo výkonom príkazu k porušeniu zákona, vysloví, že zákony porušené takto neboli a ani voči tomuto rozhodnutiu nie je možné podať opravný prostriedok. Ide teda o rozhodnutie konečné. Faktom je, že toto ustanovenie (§ 115 ods. 9 TP) nadväzuje na predošlý odsek (§ 115 ods. 8 TP), v ktorom sa konštatuje, že informovať dotknuté osoby treba v prípade, ak sa nezistia skutočnosti významné pre trestné konanie a záznamy takto získané sa predpísaným spôsobom zničia. Už problematickosť tohto ustanovenia sa premietla do problematiky nasledujúceho (v ods. 9).

Táto úprava účinná od začiatku januára 2016 nahradila pôvodnú, v ktorej sa konštatovalo, že ak sa použitím týchto prostriedkov nezistia skutočnosti dôležité pre trestné konanie, záznamy sa predpísaným spôsobom zničia. Ich zničenie zabezpečuje orgán činný v trestnom konaní ale-

bo určitý príslušník Policajného zboru, spíše o tom zápisnicu a túto vkladá do spisu. Dotknuté osoby by sa o tomto mali informovať, ak nemajú právo nahliadať do spisov a ak sa teda zistili skutočnosti, ktoré nie sú dôležité pre trestné konanie. Problematickým bola formulácia, že sa takto nezistia skutočnosti dôležité pre trestné konanie a osoba nebude mať právo nahliadať do spisu. Táto formulácia pritom ostala v predmetnom ustanovení aj po zmene účinnej od 1. januára 2016 (ods. 8 – ak sa nezistili skutočnosti významné pre trestné konanie – záznamy sa zničia – v ods. 9 sa konštatuje, že o zničení záznamu sa upovedomí osoba dotknutá výkonom tohto prostriedku, ale len tá, pri ktorej sa nezistili skutočnosti významné pre trestné konanie a z toho dôvodu sa záznam podľa ods. 8 zničil). Ako sme už naznačili vyššie, je diskutabilné, čo zákonodarca rozumel pod spojením „nezistia sa skutočnosti významné pre trestné konanie“. V zmysle vyhľadávacej zásady majú orgány činné v trestnom konaní povinnosť rovnako zisťovať skutočnosti svedčiace v prospech, ako aj v neprospech obvineného. Ak aj použitie tohto informačno-technického prostriedku vyvráti možné podozrenie z trestnej činnosti, osoba už nebude ani podozrivá, ale zistili sa skutočnosti dôležité pre trestné konanie, takže túto osobu nebude potrebné informovať. To, že sa zistia skutočnosti vyvracajúce jej podozrenie, je v každom prípade skutočnosťou dôležitou pre trestné konanie, lebo na tomto poznatku je potrebné zakladať ďalší postup vo veci a rozhodnutie v nej (odmietnutie trestného oznámenia, zastavenie trestného stíhania a pod.). Keďže sa však zistia informácie dôležité pre trestné konanie, túto osobu, ktorá už nebude ani podozrivou, netreba o použití tohto prostriedku informovať. V predmetnom ustanovení teda bola nešťastne použitá táto formulácia a aj po novele účinnej od 1. januára 2016 tam táto formulácia naďalej ostala, hoci by bolo jednoznačne možné odporúčať jej zmenu. Zákonodarca mal zrejme na mysli prípady, keď sa nezistia skutočnosti, ktoré potvrdzujú podozrenie, usvedčujú určité osoby z trestnoprávne relevantného konania a pod. Ibaže ani toto nie sú skutočnosti, ktoré by neboli pre trestné konanie významné, lebo determinujú ďalší postup v nej a odôvodnia určité rozhodovanie vo veci. Navyše, orgány činné v trestnom konaní majú rovnako tak v zmysle vyhľadávacej zásady povinnosť zisťovať skutočnosti svedčiace v prospech, ako aj v neprospech obvineného. Napokon, v predmetnom ustanovení, ktoré sa týka informovania dotknutých osôb ide o zásah do práva týchto osôb na súkromie. Bez ohľadu na to, aké skutočnosti sa použitím tohto prostriedku zistili, do práva na súkromie ním bolo zasiahnuté. Dotknuté osoby by tak mali mať právo domáhať sa súdnej a inej ochrany svojich práv voči nezákonným zásahom do nich bez ohľadu na skutočnosti, aké sa týmto zásahom zistia. Odhliadnuc od povahy zistených skutočností, do práva na súkromie zasiahnuté bolo a toto je skutočnosť, ktorá odôvodňuje potrebu informovania dotknutých osôb – nie len vybraných skupín osôb, ako to konštatuje § 352f a § 352g TP.

6. Použitie získaných informácií v inej trestnej veci

V súlade s ustanovením § 115 ods. 6 TP, ak sa informácie získané použitím odpočúvania a záznamu telekomunikačnej prevádzky na podklade § 115 TP majú v trestnom konaní využiť ako dôkazy, je potrebné vyhotoviť k nim prepis v rozsahu skutočností, ktoré sú pre trestné konanie významné, ak to dovoľuje povaha záznamu. Neprepisujú sa celé hodiny, týždne či mesiace záznamov, ale vyhotovia sa len prepisy skutočností, ktoré sú dôležité pre trestné konanie. Prepisy vykonávajú príslušníci Policajného zboru, ktorí vykonávali odpočúvanie. Uvádzajú sa súčasne všetky údaje o mieste a čase odpočúvania, o tom, kto vykonával túto činnosť a údaje o zákonnosti odposluchu. Takto vyhotovený prepis sa zakladá do spisu a už nepodlieha utajeniu. Utaľovať by sa mohol iba vtedy, ak by obsahoval skutočnosti, ktoré sú chránené podľa osobitných

predpisov ako zákonom vymedzené tajomstvá. Záznam z telekomunikačnej prevádzky sa aj tak uchováva na vhodnom nosiči priamo v spisovom materiály, a teda je dostupný na možné vyhotovovanie kópií z neho (významné sú aj z hľadiska možného opravného konania). Prepisy v rozsahu, aký považujú za vhodné a potrebné, si na svoje náklady môže vyžiadať tak obvinený (obžalovaný) a jeho obhajca, avšak, samozrejme, až po tom, čo sa odpočúvacia činnosť skončí. Všeobecne platí, že informácie, ktoré sa získali legálnym použitím tohto prostriedku, sa ako dôkazy dajú v trestnom konaní využiť až po tom, čo sa táto činnosť už ukončila. Pred tým, teda počas reálneho odpočúvania, nie je možné takéto informácie ako dôkazy využiť. Ako bolo naznačené v kapitole práce týkajúcej sa odhaľovania korupcie, nie je možné používať ako dôkazy také informácie, ktoré by sa získali odpočúvaním a záznamom telekomunikačnej prevádzky medzi obvineným (obžalovaným) a obhajcom o veciach, kde obhajca tohto obvineného (obžalovaného) zastupuje v trestnom konaní.

V prípravnom konaní je možné, aby sa záznam telekomunikačnej prevádzky použil aj bez jeho prepisu. Podmienkou je, že ide o prípady, kedy sú záznamy dostatočne jasné a zrozumiteľné a ak takýto postup odôvodňujú okolnosti prípadu. Musí sa k nemu však pripojiť sprievodná správa, z ktorej bude vyplývať tak miesto, ako aj dátum odpočúvania a skutočnosti preukazujúce legálne použitie tohto prostriedku. Tiež sa tu musia uviesť osoby, ktorých sa použitie tohto prostriedku dotýkalo.

Na podklade ustanovenia § 115 ods. 7 TP informácie, ktoré sa získali použitím tohto informačno-technického prostriedku, je možné využiť jednak v tom konaní, v ktorom sa použitie tohto prostriedku nariadilo, no je ich možné využiť aj v inej trestnej veci za podmienky, že *súčasne* aj v tejto inej trestnej veci sa vedie trestné stíhanie pre taký trestný čin, pre ktorý je možné využiť tento prostriedok v trestnom konaní (§ 115 ods. 1 TP). Ak sa teda majú takto získané informácie využiť ako dôkazy aj v inej trestnej veci, musí byť súčasne aj v tejto trestnej veci vedené trestné stíhanie pre niektorý z vymedzených trestných činov. Zmyslom a podstatou tohto ustanovenia je napomôcť dokazovaniu tých najzávažnejších trestných činov tak, že dôkazy, ktoré sa získali v jednej trestnej veci sa budú dať tzv. sprostredkovane využiť aj v trestnej veci inej, ak sa v nej súčasne vedie trestné stíhanie (prvá procesná podmienka) a ak ide o konanie pre také trestné činy, pri ktorých je použitie tohto prostriedku možné (druhá hmotnoprávna podmienka). Kým druhá podmienka, teda okruh trestných činov, pre ktoré sa vedie aj v druhej trestnej veci trestné stíhanie, nespôsobuje problémy v aplikačnej praxi, prvá uvedená podmienka je veľmi sporná. Ide o spornosť toho, k akému momentu sa vzťahuje požiadavka na súčasné vedenie trestného stíhania. Táto požiadavka sa môže vzťahovať na moment, keď sa používa predmetný informačno-technický prostriedok, teda na moment, keď sa reálne odpočúva a zaznamenáva telekomunikačná prevádzka alebo až na moment, keď sa používajú záznamy získané použitím tohto prostriedku, teda keď sa využívajú informácie z nich získané ako dôkazy. Trestno-procesné ustanovenie Trestného poriadku tento problém vyslovene nerieši a ani neponúka konkrétny návod, akým by sa jednoznačne dal tento problém vyriešiť. Je však zaujímavé už len to, že použitie takýchto záznamov aj v inej veci sa podmieňuje vôbec nejakou takouto požiadavkou – požiadavkou na súčasné vedenie trestného stíhania aj v inej trestnej veci. Je to zaujímavé z dôvodu, že v neprocesnej rovine, teda tam, kde by právna úprava mala byť ešte o niečo prísnejšia a exaktnejšia, keďže ide mimo rámca trestného konania a teda v danej veci nie je ani podané trestné oznámenie, ani začaté trestné stíhanie či vznesené obvinenie, v tejto neprocesnej rovine sa nestanovujú žiadne takéto obmedzenia pre použiteľnosť získaných dôkazov. Ak sa prostredníctvom informačno-technických prostriedkov, ktoré sa používajú mimo rámca trestného konania na podklade osobitých predpisov, zistia skutočnosti dôležité pre trestné konanie, tieto sa dajú v trestnom konaní využiť ako dôkazy. Nie je tu vyjadrená žiadna požiadavka, že by v čase použí-

vania týchto prostriedkov alebo až po ich ukončení a v čase používania záznamov z nich získaných, muselo byť v trestnej veci vedené trestné stíhanie. Takže v neprocesnej línii, kde by úprava použitia takýchto dôkazov mala byť ešte prísnejšia, sa nestanovujú žiadne takéto obmedzenia, zatiaľ čo v rovine procesnej, teda pri existencii podozrenia plynúceho z trestného oznámenia alebo po začatí trestného stíhania a prípadne aj po vznesení obvinenia, sa takáto podmienka, resp. obmedzenie stanovuje. Teda tam, kde by takéto obmedzenia, s ohľadom na líniu použitia, existovať mali, tam neexistujú a tam, kde by existovať nemuseli, tam sa stanovujú. Prirodzene, že táto úprava je jednak nelogická a potom v každom prípade nesúladná. Chránia sa tak viac práva osôb vystupujúcich v trestnom konaní v určitej pozícii (podozrivého či obvineného) ako práva osôb, ktoré v takejto trestnoprocessnej pozícii nie sú.

Zmyslom ustanovenia § 115 ods. 7 TP je napomôcť dokazovaniu vybraných trestných činov, pre ktoré sa tento prostriedok môže nariadiť. Práve sporná podmienka súčasného vedenia trestného stíhania aj v inej trestnej veci však jeho použiteľnosť do značnej miery obmedzuje. Skutočnosť, že nie je celkom zrejmé, k akému momentu by sa malo vzťahovať súčasné vedenie trestného stíhania v inej trestnej veci, totiž vyvolala diskusiu k tejto otázke a to bez jednoznačného záveru. Rôzne trestné senáty NS SR sa v rámci svojej rozhodovacej činnosti nedokázali na riešení tohto problému zhodnúť. Jeden trestný senát NS SR vzťahuje požiadavku súčasného vedenia trestného stíhania v inej trestnej veci na moment, kedy sa využívajú výsledky odpočúvania a záznamu telekomunikačnej prevádzky, nie na moment použitia týchto prostriedkov a druhý trestný senát NS SR vykladá túto požiadavku presne naopak. Senát NS SR priamo konštatoval, že by bolo nelogické, ak by sa záznam získaný legálnym odpočúvaním vo veci, v ktorej sa nariadilo použitie tohto prostriedku (a to aj v čase ešte pred začatím trestného stíhania, teda v postupe pred začatím trestného stíhania), mohol v inej trestnej veci použiť iba za podmienky, že už v čase vykonávania odposluchu by muselo byť aj v inej trestnej veci začaté trestné stíhanie. Ak by sme trvali na požiadavke, že už v čase, keď sa vykonáva odpočúvanie a záznam telekomunikačnej prevádzky, muselo by byť v inej trestnej veci, kde sa má dôkaz použiť, začaté trestné stíhanie, je nelogická. Nič by tu nebránilo tomu, aby sa aj v tejto inej trestnej veci dosiahlo vydanie príkazu na legálne použitie tohto prostriedku a nebolo by potrebné využívať tzv. sprostredkované dôkazy získané z inej trestnej veci. Ak by sme vykladali požiadavku na súčasné vedenie trestného stíhania naopak, tak by sa zároveň obmedzovala použiteľnosť ustanovenia § 115 ods. 7 TP iba na minimum, ak vôbec na nejaké prípady a to, prirodzene, nie je zmyslom a podstatou tohto ustanovenia.¹¹ Nenapomáhalo by sa takto dokazovaniu aj iných trestných činov, pri ktorých sa tento prostriedok môže nariadiť (môže sa nariadiť jeho použitie) a toto bol zrejme zámer zákonodarcu pri tvorbe predmetného ustanovenia. Toto rozhodnutie teda vzťahuje požiadavku na súčasné vedenie trestného stíhania aj v inej trestnej veci na moment využívania záznamov, resp. používania informácií, ktoré sa týmto prostriedkom (legálnym použitím) získali.

Na druhej strane stojí presne opačný názor iného trestného senátu NS SR¹² a o tento sa oprel aj stanovisko GP SR.¹³ Tu sa konštatuje, že požiadavka súčasného vedenia trestného stíhania by sa mala vzťahovať k momentu, kedy sa odpočúvanie a záznam telekomunikačnej prevádzky realizujú. Priamo sa uvádza, že pod súčasným vedením trestného stíhania aj v inej trestnej veci treba rozumieť „*úkon, rozhodnutie alebo iný postup vykonávaný na základe TP, ku ktorému v inej trestnej veci došlo pred zabezpečením dotknutej dôkaznej informácie vo veci, v ktorej bol tento postup nariadený (jej zabezpečením, sledovaním osôb a vecí, vyhotovením obrazového, zvukového, obrazovo-zvukového záznamu, odpočúvaním a záznamom telekomunikačnej prevádzky,*

¹¹ Rozhodnutie NS SR 3 To 2/2011 z 21. septembra 2011.

¹² Rozhodnutie NS SR 2 To 5/2011 zo dňa 7. februára 2012.

¹³ Stanovisko GP SR IV/1 GPt 145/12-7 zo dňa 18. apríla 2011.

*prostredníctvom agenta alebo porovnaním údajov v informačných systémoch)*¹⁴ Za rozhodujúcu sa považuje časová súvislosť dvoch trestných vecí a trestných konaní o nich a to v momente, kedy došlo k zabezpečeniu dôkaznej informácie, ktorá sa má použiť aj v inej trestnej veci (teda duplicitne). Nie je možné do popredia stavať súvislosť vecnú, čo konštatoval aj trestný senát NS SR vo svojom rozhodnutí z februára 2012. Senát NS SR tu odmietol konštatovanie prvostupňového súdu, ktorý vzťahoval požiadavku súčasného vedenia trestného stíhania v inej veci na moment použitia takto získaných záznamov (resp. informácií z nich ako dôkazov v trestnom konaní). Podľa senátu NS SR sa tu súd prvého stupňa mýlil. „*Nezodpovedá vecnej logike, aby zákon požadoval ako podmienku dôkaznej použiteľnosti informácie súčasné vedenie trestného konania vo veci, v ktorej bola táto informácia legálne získaná a tento súbeh konaní mal byť daný ešte v čase, keď bude predmetná informácia v inom trestnom konaní použitá (teda v konečnom dôsledku na hlavnom pojednávaní v súdnom konaní). Použiteľnosť dôkazov v inom konaní by teda bola viazaná na podmienku, ktorá sa tohto (iného) konania vôbec netýka a závisí len od priebehu, resp. dĺžky konania v pôvodnej veci. Jediným vecne odôvodneným východiskom, ktoré je možné použiť pri výklade zákonnej požiadavky „súčasného vedenia trestného konania v inej trestnej veci“ (s príslušnou právnu kvalifikáciou činu) je časová paralela trestného konania v oboch dotknutých veciach, a to v momente zabezpečenia dôkaznej informácie, ktorá má byť použitá duplicitne (v oboch konaniach). Účelom úpravy, založenej na tomto princípe je vylúčenie zabezpečovania dôkazov „naslepo“, resp. preventívne bez toho, aby bol pre takýto postup dôvod, týkajúci sa možnosti spáchania určitého činu s jeho aspoň rámcovou identifikáciou, týkajúcou sa podstaty tohto skutku.*“¹⁵

Na podklade vyššie uvedeného možno jednoznačne konštatovať, že predmetná trestno-procesná úprava nariesi jasne moment, na ktorý sa požiadavka súčasného vedenia trestného stíhania v inej trestnej veci vzťahuje. Výklad tejto požiadavky je tak problematický a hlavne dovoľuje zaujatie odlišných stanovísk tak, ako je to vidieť aj z rôznych rozhodnutí rôznych senátov NS SR, kde jedno z nich bolo podopreté aj stanoviskom GP SR. V rámci možnosti NS SR prijímať zjednocujúce stanoviská smerujúce k jednotnej aplikácii a výkladu ustanovení právnych predpisov sa kolégium NS SR pokúsilo o prijatie zjednocujúceho stanoviska aj v tejto veci. Vo svojom návrhu sa však priklonilo k záveru obsiahnutému v stanovisku GP SR a súčasne aj v rozhodnutí NS SR z februára 2012. Avšak v konečnom dôsledku sa zjednocujúce stanovisko v tejto veci nepodarilo prijať a tak sa odporúčalo zákonodarcovi, aby tento problém vyriešil na úrovni legislatívnej. To sa dodnes ale nestalo.

Jednoznačne tak možno odporúčať, aby sa predmetné ustanovenie upravilo, pričom možnosti riešenia sú tu viaceré. Prvá vedie v zmysle a smerom jednoznačného výkladu tejto spornej požiadavky a predmetného ustanovenia. Jeho zmyslom je napomáhať dokazovaniu trestných činov, pri ktorých je možné nariadiť použitie tohto inštitútu. Je preto nelogické, aby sa táto možnosť komplikovala stanovovaním nezmyselných podmienok a obmedzení. Pritom, v neprocesnej rovine, ktorá by mala byť z hľadiska poskytovanej ochrany ešte prísnejšia, žiadna takáto požiadavka nie je stanovená. Po vzore práve tejto neprocesnej úpravy by sa preto mala požiadavka na súčasné vedenie trestného stíhania aj v inej trestnej veci z tohto ustanovenia odstrániť (to je druhá možná cesta riešenia tohto problému). Alebo by sa do ustanovenia § 115 ods. 7 TP mala doplniť vysvetľujúca formulácia, že súčasné vedenie trestného stíhania v inej trestnej veci sa viaže na moment používania výstupov získaných týmto prostriedkom, teda na moment používania získaných záznamov ako dôkazov. Bolo by nelogické, aby sa trestné stíhanie aj v inej veci muselo viesť už v čase, keď sa informačno-technické prostriedky vykonávajú, nakoľko už v tom-

¹⁴ Stanovisko GP SR IV/1 GPt 145/12-7 zo dňa 18. apríla 2011.

¹⁵ Rozhodnutie NS SR 2 To 5/2011 zo dňa 7. februára 2012, s. 17 a 18.

to čase by sa dalo v druhom trestnom konaní resp. stíhaní legálne dosiahnuť vydanie takéhoto príkazu. Nemuseli by sa sprostredkované používať takéto informácie. Navyše, ak sa aj v rámci jednej trestnej veci v rámci pôsobnosti konkrétneho informačno-technického zistia určité skutočnosti, tieto sú spravidla svojou povahou informáciami neopakovateľnými, aj preto možno vysloviť a skôr sa prikloniť k záveru a názoru o tom, že s výnimkou vecnej pôsobnosti inštitútu by sa možnosť sprostredkovaného využitia dôkazov aj v inej trestnej veci nemala obmedzovať vôbec. Ak by sa však zmeny úpravy uberala smerom vymedzenia časovej súvislosti požiadavky súčasného vedenia trestného stíhania v inej trestnej veci, stojí za zamyslenie aj zmena neprocesnej úpravy, kde sa použitie informácií takto získaných ako dôkazov v trestnom konaní nijako časovo ani vecne neobmedzuje.

Záver

Tak, ako naznačuje vyššie uvedené analytické spracovanie trestno-procesnej úpravy inštitútu odpočúvania a záznamu telekomunikačnej prevádzky, táto procesná úprava vykazuje viacero nie len teoretických, ale aj zásadných aplikačných a interpretačných problémov. Pritom je možné uvažovať o inštitúte, ktorý efektívne a účinne smeruje k odhaľovaniu a dokazovaniu závažnej trestnej činnosti. Popri personálnych súvislostiach použitia však toto efektívne a účinné použitie komplikuje celý rad teoretických a aplikačných problémov, ktoré sa otvárajú na základe samotnej trestno-procesnej úpravy. Je možno len zamýšľať sa nad tým, ako by resp. či by táto úprava použitia odpočúvania a záznamu telekomunikačnej prevádzky na podklade § 115 TP vyhovovala požiadavkám, ktoré na prípustnosť zásahov do garantovaných práv formuluje Dohovor a ktoré vo svojej judikatúre spresňuje ESLP. Odhliadnuc od tejto odpovede, efektívnosť a účinnosť boja so závažnou trestnou činnosťou jednoznačne odôvodňuje požiadavku na operatívnu a dôslednú úpravu predmetného ustanovenia s cieľom podporiť efektívnosť a účinnosť jeho používania.

Zoznam literatúry:

- Ivor, J. a kol.: Trestné právo procesné. Druhé, doplnené a prepracované vydanie. Bratislava: IURA EDITION, 2010.
- Perhács, Z., Perhácsová, A.: Právna úprava používania informačno-technických prostriedkov (2. časť). In *Jus-tičná revue* č. 5/2013.
- Tittlová, M.: Korupcia (vybrané kriminologické a trestnoprávne aspekty). Bratislava: Wolters Kluwer, 2015.
- Ústava SR (Zákon č. 460/1992 Zb. v znení neskorších ústavných zákonov).
- Dohovor o ochrane základných ľudských práv a slobôd.
- Trestný poriadok (zákon č. 301/2005 Z. z. v znení neskorších právnych predpisov).
- Rozsudok ESLP z 23. júla 1968 vo veci „Belgický jazykový zákon“.
- Rozsudok ESLP zo 06. septembra 1978 vo veci Klass a ostatní vs. Nemecko.
- Rozsudok ESLP z roku 1984 vo veci Malone vs. Spojené kráľovstvo.
- Rozsudok ESLP zo dňa 25.03. 1998 vo veci Kopp vs. Švajčiarsko.
- Rozhodnutie NS SR 3 To 2/2011 z 21. septembra 2011.
- Rozhodnutie NS SR 2 To 5/2011 zo dňa 7. februára 2012.
- Stanovisko GP SR IV/1 GPt 145/12-7 zo dňa 18. apríla 2011.

Vybrané ústavné a trestno-procesné aspekty vyhotovovania obrazových, zvukových alebo obrazovo-zvukových záznamov

Selective Constitutional and Criminal Procedural Aspects of Getting the Video, Audio or Video-audio records

Miloš Deset¹

Abstrakt: V tomto príspevku je venovaná pozornosť niektorým aspektom trestno-procesnej úpravy vyhotovovania obrazových, zvukových alebo obrazovo-zvukových záznamov. Cieľom skúmania je kriticky poukázať na niektoré problematické otázky, ako napríklad právomoc prokurátora vydávať príkazy na vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov s dočasnou platnosťou, či následná ochrana práva na súkromie dotknutej osoby, ktorá je pri tomto informačno-technickom prostriedku slabšia ako napríklad pri odpočúvaní a zázname telekomunikačnej prevádzky. V druhej časti sa z komparatívneho hľadiska v stručnosti analyzuje aj monitorovanie osôb podľa iných právnych predpisov (nie podľa Trestného poriadku).

Abstract: This paper is focused on selective aspects of legal regulation of getting the video-, audio- or video-audio records. The aim of the search is critically underline some problematic questions, e. g. the right of prosecutor to take the order for getting the video-, audio- or video-audio records with temporary validity, or the subsequent protection of the right to privacy of inflicted person, which is weaker in this case than the protection according to the legal regulation of tapping. In the second part of this paper, there is analysed the monitoring of persons according to the other acts (not according to the Criminal Procedure Act)

Kľúčové slová: informačno-technické prostriedky, vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov, monitorovanie, právo na súkromie.

Key words: information-technical means, getting of video-, audio- or video-audio records, the monitoring, the right to privacy.

Úvod

Objasňovanie závažných trestných činov, napríklad takých, ktoré sa páchajú organizovanou formou, a zisťovanie ich páchatelov je v niektorých prípadoch mimoriadne náročné a bez použitia špecifických prostriedkov na zabezpečovanie informácií by to v mnohých prípadoch bolo aj nemožné.

Podľa Ivora možno vo všeobecnosti tieto nové prostriedky a metódy boja s organizovanou kriminalitou charakterizovať najmä nasledovnými znakmi:

1. Ide o veľmi intenzívny zásah do základných práv a slobôd, garantovaných medzinárodnými dokumentmi a Ústavou, čo si vyžaduje veľmi precíznu a podrobnú zákonnú úpravu.
2. Ide o postupy, ktorých efektívnosť výsledku predpokladá utajenosť ich aplikácie. V tejto súvislosti sú niektoré kontrolné mechanizmy značne obmedzené ba úplne vylúčené.

¹ JUDr. Miloš Deset, PhD., Trnavská univerzita v Trnave, Právnická fakulta, Katedra trestného práva a kriminológie, milos.deset@truni.sk.

3. Pre dôkazné využitie týchto prostriedkov, za súčasného garantovania riadneho procesu (čl. 6 Dohovoru o ochrane ľudských práv a základných slobôd), sa predpokladá špeciálna legislatívna úprava a jej dôsledné dodržiavanie v aplikačnej praxi.²

Ivor charakterizuje vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov nasledovne: „Obrazovo-zvukovým záznamom je zachytený pohyb a činnosť osôb a vecí, verbálna komunikácia osôb prípadne ďalšie obrazové a zvukové informácie významné pre trestné konanie s vysokou mierou objektívnosti a vierohodnosti, závislou prakticky iba od technickej úrovne záznamového zariadenia a tiež jeho obsluhy. Obrazovo-zvukový záznam je možné vyhotoviť podrobnej analýze (zväčšením detailov, opakovaním záznamu, spomalením rýchlosti záznamu, identifikáciou objektov a pod.), pričom video resp. fonoskopickou expertízou je možné odhaliť akýkoľvek pokus o neoprávnenú manipuláciu či úpravu záznamu.“³

Vyhotovovanie obrazových, zvukových a obrazovo-zvukových záznamov je procesným prostriedkom, ktorého predmetom je utajené spracúvanie a vyhodnocovanie takýchto záznamov dôležitých pre rozhodnutie vo veci samej, t. j. všetkých skutočností, ktoré sú dôležité z hľadiska trestného práva hmotného a procesného, najmä takých, ktorými sa preveruje vierohodnosť a zákonnosť vykonávaných dôkazov.⁴

Naznačené charakteristické črty informačno-technických prostriedkov platia pre jednak pre vyhotovovanie obrazových, zvukových a obrazovo-zvukových záznamov a jednak aj pre odpočúvanie a záznam telekomunikačnej prevádzky. Pre oba prostriedky platia zásady, aké Európsky súd pre ľudské práva (ďalej len „Európsky súd“) sformuloval v súvislosti s posudzovaním zásahov do práva na súkromie, čo majú oba prostriedky taktiež spoločné.

Právo na súkromie je upravené vo viacerých právnych predpisoch, predovšetkým v Ústave Slovenskej republiky č. 460/1992 Zb. (ďalej len „Ústava“), Listine základných práv a slobôd (ďalej len „Listina“) či v Dohovore o ochrane ľudských práv a základných slobôd (ďalej len „Dohovor“).

V súvislosti so závažnosťou zásahu do súkromia, ktorý je nevyhnutne spojený s týmto prostriedkom možno spomenúť napríklad Nález Ústavného súdu SR, sp. zn. II. ÚS 5/2011 zo dňa 15. 12. 2011, v ktorom súd dospel k záveru, že procesné ustanovenie, podľa ktorého za dôkaz môžu slúžiť všetky prostriedky, ktorými možno zistiť a objasniť skutočný stav veci, pokiaľ sú v súlade s právnymi predpismi, treba z ústavnoprávneho hľadiska považovať za kolíziu verejného záujmu a ochrany práv. Ide totiž o stret medzi verejným záujmom na dôslednom objasnení rozhodujúcich skutočností potrebných na vydanie rozhodnutia v konaní a ochranu určitých práv, resp. oprávnených záujmov, ktoré bránia použitiu niektorého dôkazného prostriedku. Vo všeobecnej rovine možno konštatovať, že prednosť má verejný záujem na dôslednom objasnení rozhodujúcich skutočností potrebných na vydanie rozhodnutia, avšak za súčasného spolupôsobenia brzd daných s ohľadom na ochranu určitých práv, resp. oprávnených záujmov. Tým je dané, že nie všetky prostriedky, pomocou ktorých by objektívne bolo možné zistiť a objasniť skutočný stav veci, sa smú použiť v príslušnom konaní.⁵

To znamená, že pri strete dvoch záujmov, ku ktorému pri použití informačno-technických prostriedkov nevyhnutne dochádza, a to medzi záujmom na objasnení veci na strane jednej a ochranou súkromia na strane druhej, sa síce pripúšťa verejný záujem, ale tento záujem nemožno

² Ivor, J. Obrazovo-zvukový záznam ako dôkazný prostriedok v trestnom konaní. In Záhora, J. Teoretické a praktické problémy dokazovania. Bratislava: BVŠP, 2008, s. 70. Pozri tiež Aláč, M. Získavanie informácií na spravodajské účely a účely trestného konania. Bratislava: C. H. Beck, 2015, s. 108.

³ Ivor, J. Obrazovo-zvukový záznam ako dôkazný prostriedok v trestnom konaní. In Záhora, J. Teoretické a praktické problémy dokazovania. Bratislava: BVŠP, 2008, s. 73.

⁴ Čentés, J. a kol. Trestné právo procesné: Všeobecná a osobitná časť. Šamorín: Heuréka, 2012, s. 292.

⁵ Nález Ústavného súdu SR, sp. zn. II. ÚS 5/2011.

no interpretovať absolútne a bezvýnimočne. K zásahu môže dôjsť iba na základe striktne splnených podmienok, ktoré preň upravuje platné právo, pretože vždy treba brať ohľad aj na záujmy potenciálne dotknutých osôb a ich právo na súkromie.

Podľa Benedikovičovej vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov naráža na ústavné garantované právo na ochranu súkromia. Pri vyhotovovaní takýchto záznamov je potrebné ich posudzovať z pohľadu legality, legitimacy a proporcionality. Nezákonnosť vyhotovenia obrazového, zvukového alebo obrazovo-zvukového záznamu má za následok absolútnu neúčinnosť a nepoužiteľnosť tohto dôkazu v trestnom konaní.⁶

Abý sa tak nestalo, treba striktne dodržiavať právnu úpravu, ktorá tento prostriedok upravuje, avšak treba povedať, že aj na samotnej právnej úprave vyhotovovania obrazových, zvukových alebo obrazovo-zvukových záznamov je niekoľko kritických či problematických miest.

1. Vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov

Právna úprava vyhotovovania obrazových, zvukových a obrazovo-zvukových záznamov je obsiahnutá v § 114 TP. V podstate sa tu upravujú dva režimy vyhotovovania obrazových, zvukových a obrazovo-zvukových záznamov. Jednak ide o režim, ktorý nie je spojený so vstupom do obydľia, a jednak o režim, ktorý je spojený so vstupom do obydľia.

Vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov, ktoré nie sú spojené s priamym vstupom do obydľia je upravené v § 114 ods. 1 zákona č. 301/2005 Z. z., Trestného poriadku (ďalej len „Trestný poriadok“ alebo „TP“), podľa ktorého obrazový, zvukový alebo obrazovo-zvukový záznam možno vyhotoviť v trestnom konaní pre úmyselný trestný čin, na ktorý zákon ustanovuje trest odňatia slobody s hornou hranicou trestnej sadzby prevyšujúcou tri roky, korupciu alebo pre iný úmyselný trestný čin, o ktorom na konanie zaväzuje medzinárodná zmluva, ak možno dôvodne predpokladať, že ním budú zistené skutočnosti významné pre trestné konanie.

Podľa § 114 ods. 2 TP vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov, ktoré je spojené s priamym vstupom do obydľia, je prípustné len v trestnom konaní o zločine, korupcii, trestnom čine zneužívania právomoci verejného činiteľa, trestnom čine legalizácie príjmu z trestnej činnosti alebo pre iný úmyselný trestný čin, o ktorom na konanie zaväzuje medzinárodná zmluva.

Rovnaké ustanovenie taktiež upravuje, že príkaz na vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov vydáva písomne predseda senátu, pred začatím trestného stíhania alebo v prípravnom konaní sudca pre prípravné konanie na návrh prokurátora. Návrh musí byť odôvodnený podozrením z konkrétnej trestnej činnosti a tiež údajmi o osobách a veciach, ktorých sa vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov týka, ak sú tieto údaje známe. Ak ide o vec, ktorá neznesie odklad a vyhotovovanie obrazových, zvukových a obrazovo-zvukových záznamov nie je spojené so vstupom do obydľia a písomný príkaz sudcu pre prípravné konanie nemožno získať vopred, môže pred začatím trestného stíhania a v prípravnom konaní vydať príkaz prokurátor; takýto príkaz musí najneskôr do 24 hodín od jeho vydania potvrdiť sudca pre prípravné konanie, inak stráca platnosť a takto získané

⁶ Benedikovičová, A. Vyhotovenie obrazového, zvukového alebo obrazovo-zvukového záznamu ako dôkazný prostriedok v trestnom konaní. In Kalvodová, V., Hrušáková, M. a kolektív. Dokazování v trestním řízení. Právní, kriminologické a kriminalistické aspekty. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 221.

informácie nemožno na účel trestného konania použiť a musia sa predpísaným spôsobom bez meškania zničiť.

V príkaze podľa odseku 2 musí byť ďalej stanovený čas, v ktorom bude vykonávané vyhotovovanie obrazových, zvukových a obrazovo-zvukových záznamov; tento čas môže trvať najviac šesť mesiacov. Ten, kto vydal príkaz na vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov, môže čas ich trvania písomne predĺžiť vždy najviac o dva mesiace, a to aj opakovane.

Podľa odseku 4 vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov vykonáva príslušný útvar Policajného zboru. Tento odsek chráni aj dôvernoscť vzťahu medzi advokátom a klientom. Ak sa pri vyhotovovaní takýchto záznamov zistí, že obvinený komunikuje so svojím obhajcom, takto získané informácie nemožno použiť na účely trestného konania a musia sa predpísaným spôsobom bez meškania zničiť; to neplatí, ak ide o informácie, ktoré sa vzťahujú na vec, v ktorej advokát nezastupuje obvineného ako obhajcu.

Trestný poriadok taktiež ustanovuje aj povinnosť sústavného skúmania dôvodov vyhotovovania obrazových, zvukových alebo obrazovo-zvukových záznamov. Podľa § 114 ods. 5 TP policajt alebo príslušný útvar Policajného zboru je povinný sústavne skúmať trvanie dôvodov, ktoré viedli k vydaniu príkazu na vyhotovovanie takýchto záznamov. Ak dôvody pominuli, musí sa vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov skončiť, a to aj pred uplynutím času, ktorý ustanovuje zákon. Túto skutočnosť bez meškania písomne oznámi tomu, kto vydal príkaz, v prípravnom konaní tiež prokurátorovi.

Na tejto úprave je však problematických hneď niekoľko vecí, predovšetkým ide o rozdiel medzi vyhotovovaním záznamov v obydli a v iných priestoroch, v ktorých vyhotovovanie takýchto záznamov nie je spojené so vstupom do obydla.

Európsky súd v prípadoch Niemietz proti Nemecku (rozhodnutie zo 16. decembra 1992) a Chappell proti Spojenému kráľovstvu (rozhodnutie z 30. marca 1989) pri výklade pojmov „home“ a „domicile“ nerobil rozdiel medzi obydli v zmysle priestoru určeného na bývanie a iným priestorom, ktorý neslúži na bývanie a v ktorom dotknutá osoba spravidla vykonáva svoju profesiu, resp. prácu, ale ktorý tejto osobe poskytuje určitú mieru súkromia.⁷ Aj vo veci Klass a ostatní proti Spolkovej republike Nemecko (rozhodnutie zo 6. septembra 1978) Európsky súd konštatoval, že aj aktivita profesionálnej povahy môže spadať pod pojem „súkromný život“ a „korešpondencia“,⁸ v prípade Gillow proti Spojenému kráľovstvu (rozhodnutie z 24. novembra 1986) zasa Európsky súd definoval obydlie ako miesto, kde osoba býva alebo vykonáva svoju obvyklú profesiu.⁹ Relevantné sú aj ďalšie rozhodnutia Európskeho súdu, konkrétne Société Colas Est. proti Francúzsku (rozhodnutie zo 16. apríla 2002), v ktorom súd zdôraznil, že požiadavka na ochranu obydla sa vzťahuje aj na sídla spoločností a čl. 8 Dohovoru preto zahŕňa aj požiadavku rešpektu k súkromiu sídla spoločností, pobočiek či podnikov právnických osôb,¹⁰ či rozhodnutie vo veci Crémieux proti Francúzsku z 25. februára 1993 a rozhodnutie vo veci Mialhe proti Francúzsku z 25. februára 1993, v ktorých súd pod túto ochranu zaradil aj kancelárske priestory.¹¹ Tieto rozhodnutia treba brať na zreteľ z toho dôvodu, že Európsky súd poskytol iným

⁷ Niemietz proti Nemecku (rozhodnutie zo 16. decembra 1992) a Chappell proti Spojenému kráľovstvu (rozhodnutie z 30. marca 1989).

⁸ Klass a ostatní proti Spolkovej republike Nemecko (rozhodnutie zo 6. septembra 1978).

⁹ Gillow proti Spojenému kráľovstvu (rozhodnutie z 24. novembra 1986).

¹⁰ Société Colas Est. proti Francúzsku (rozhodnutie zo 16. apríla 2002).

¹¹ Crémieux proti Francúzsku (rozhodnutie z 25. februára 1993) a Mialhe proti Francúzsku (rozhodnutie z 25. februára 1993).

priestorom, ktoré neslúžia na bývanie, ale užívateľom poskytujú istú mieru súkromia, rovnakú ochranu ako priestorom, ktoré slúžia na bývanie.

Pri pohľade na tieto rozhodnutia sa však naše právo javí ako nesúladne s interpretáciou obydli, tak ako ho vyložil Európsky súd. Problematickým je v tejto súvislosti nielen trestno-procesná úprava prehliadky iných priestorov a pozemkov, ale aj úprava informačno-technických prostriedkov či prostriedkov operatívno-pátracej činnosti. Ak je totiž ochrana súkromia pokiaľ ide o bydlie kladená na roveň ochrane súkromia, ktoré užívateľovi poskytuje napríklad sídlo jeho spoločnosti alebo jeho kancelária, rovnaké by mali byť aj podmienky, za splnenia ktorých je do týchto priestorov možné zasiahnuť. Z tohto dôvodu by nemali byť robené rozdiely v ochrane súkromia, ak ide o nariadenie domovej prehliadky, kde príkaz na domovú prehliadku môže vydať iba sudca pre prípravné konanie a v konaní pred súdom predseda senát, a nariadenie prehliadky iných priestorov, ktoré neslúžia na bývanie a pod ktorými sa rozumejú aj napríklad sídla spoločností či kancelárie. V týchto prípadoch totiž môže vydať príkaz na prehliadku týchto priestorov aj prokurátor, čo celkom nezodpovedá judikatúre Európskeho súdu. Ak by sme mali trvať na dôslednom dodržiavaní judikatúry Európskeho súdu a jej aplikovateľnosti v podmienkach Slovenskej republiky, tak aj v prípade prehliadky iných priestorov by mal príkaz vydať sudca pre prípravné konanie, resp. predseda senátu v konaní pred súdom, tak ako je tomu napríklad v Českej republike. Ústavný súd ČR v Náleze zo dňa 8. júna 2010, sp. zn. Pl. ÚS 3/09, dospel aj pomocou odkazov na rozhodovaciu činnosť Európskeho súdu pre ľudské práva k záveru, že právo na rešpektovanie obydli zahŕňa tiež požiadavku rešpektovať súkromie sídla spoločnosti, pobočiek či prevádzkarní právnických osôb. A dospel tiež k záveru, že dodržanie tohto práva vyžaduje, aby príkaz na prehliadku iných priestorov a pozemkov dával nezávislý orgán, ktorým môže byť len súd, pričom podľa predchádzajúcej právnej úpravy to mohol byť štátny zástupca a s jeho súhlasom aj policajný orgán.¹²

Podobne tak aj pri právnej úprave informačno-technických prostriedkov či prostriedkov operatívno-pátracej činnosti by sa v záujme ochrany súkromia nemali robiť rozdiely takpovediac medzi rôznymi stupňami právnej ochrany. Podistým kritické sú v tejto súvislosti ustanovenia § 113 ods. 4 Trestného poriadku, § 115 ods. 2 a § 117 ods. 6 Trestného poriadku, ktoré upravujú vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov, ktoré nie je spojené so vstupom do obydli, odpočúvanie a záznam telekomunikačnej prevádzky, ktoré taktiež nie je spojené so vstupom do obydli, resp. použitie agenta, ktoré rovnako nie je spojené so vstupom do obydli. Vo všetkých troch prípadoch v prípravnom konaní alebo pred začatím trestného stíhania môže príkaz vydať prokurátor, hoci takýto príkaz je časovo obmedzený na 24 hodín (pokiaľ ide o vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov a odpočúvanie a záznam telekomunikačnej prevádzky), resp. na 72 hodín (pokiaľ ide o použitie agenta), počas ktorých ho musí potvrdiť sudca pre prípravné konanie, ale aj napriek tomu treba povedať, že ak by sme mali striktne vychádzať z judikatúry Európskeho súdu a ochranu obydli klásť na roveň iným priestorom, ktoré neslúžia na bývanie, nie je dôvodné robiť takéto rozdiely, a zásahy do oboch priestorov by mali byť podmienené rovnako. A rovnaká by mala byť aj forma rozhodnutí, ktorými sa takéto zásahy nariaďujú, čo sa vzťahuje na § 117 ods. 6 Trestného poriadku, ktorý pripúšťa, aby príkaz na použitie agenta mohol prokurátor vydať predbežne aj ústne, čo nepovažujem za dostatočnú mieru právnej ochrany súkromia potenciálne dotknutých osôb.

Pokiaľ ide o čas, na ktorý môže príkaz vydať prokurátor – 24 hodín pri vyhotovovaní obrazových, zvukových alebo obrazovo-zvukových záznamov a pri odpočúvaní a zázname teleko-

¹² Nález Ústavného súdu ČR, sp. zn. Pl. ÚS 3/09.

munikačnej prevádzky, resp. 72 hodín pri použití agenta –, treba povedať, že takáto úprava je, samozrejme, odôvodnená určitou flexibilitou, pružnosťou či väčšou akcieschopnosťou orgánov činných v trestnom konaní, no na druhej strane by k väčšej miere ochrany súkromia mohla prispieť úprava, ktorá by takúto možnosť nepripúšťala a ktorá by dôsledne trvala na tom, aby sa tieto informačno-technické prostriedky a agent mohli použiť hneď od začiatku iba na základe príkazu sudcu pre prípravné konanie. K väčšej flexibilitate použitia informačno-technických prostriedkov a prostriedkov operatívno-pátracej činnosti by mohlo prispieť, keby príkazy mohli vydávať všetky okresné sudy a nielen okresné sudy v sídlach krajských súdov (porovnaj § 24 ods. 4 Trestného poriadku), pretože v pri vydávaní príkazov nejde ešte o náročnosť dokazovania trestných vecí, tak ako pri rozhodovaní o vine a treste v závere hlavného pojednávania, ale iba posúdenie opodstatnenosti zásahu do práva na súkromie a ochranu tohto práva.

Nie je preto dôvod robiť rozdiely medzi úpravou vyhotovovania obrazových, zvukových alebo obrazovo-zvukových záznamov v obydlí a v inom priestore, ktoré v súčasnosti neinterpretujeme ako obydlie, ale ako iný priestor, ktorý neslúži na bývanie a pod ktorým rozumieme napríklad aj kancelárie či iné priestory spoločností, kde dotknuté osoby vykonávajú svoje profesie. Taktiež nie je dôvod robiť rozdiely v úprave obrazových, zvukových a obrazovo-zvukových záznamov podľa § 114 ods. 1 TP na jednej strane a úprave odpočúvania a záznamu telekomunikačnej prevádzky na strane druhej.

Podobne problematickou je aj úprava následnej ochrany dotknutej osoby, ktorej bolo vyhotovovaním obrazových, zvukových alebo obrazovo-zvukových záznamov zasiahnuté do práva na súkromie. Podľa § 114 ods. 8 TP ak sa pri vyhotovovaní obrazových, zvukových alebo obrazovo-zvukových záznamov nezistili skutočnosti významné pre trestné konanie, orgán činný v trestnom konaní alebo príslušný útvar Policajného zboru musí získaný záznam predpísaným spôsobom bez meškania zničiť. Zápisnica o zničení záznamu sa založí do spisu. O zničení záznamu osobu uvedenú v odseku 2, ktorá nemá možnosť nazerať do spisu podľa Trestného poriadku, upovedomí orgán, ktorého rozhodnutím sa vec právoplatne skončila, a v konaní pred súdom predseda senátu súdu prvého stupňa do troch rokov od právoplatného skončenia trestného stíhania v danej veci; to neplatí, ak sa koná o obzvlášť závažnom zločine alebo zločine spáchanom organizovanou skupinou, zločineckou skupinou alebo teroristickou skupinou alebo ak sa na trestnom čine podieľalo viac osôb a vo vzťahu aspoň k jednému z nich nebolo trestné stíhanie právoplatne skončené, alebo ak by poskytnutím takej informácie mohol byť zmarený účel trestného konania.

Pri pohľade na toto ustanovenie totiž vyplýva, že ochrana súkromia dotknutej osoby aj jej následné možnosti právnej ochrany, to znamená ochrany po vykonanom zásahu do jej práva na súkromie, sú oveľa slabšie ako možnosti osoby, ktorej bolo do súkromia zasiahnuté odpočúvaním, pretože v citovanom ustanovení, na rozdiel od § 115 ods. 9 TP, absentuje možnosť, aby dotknutá osoba mohla podať návrh na preskúmanie zákonnosti na Najvyšší súd SR. Ak zoberieme do úvahy závažnosť zásahov do práva na súkromie, ktoré ako to už bolo spomenuté, môže byť spojené aj so vstupom do obydlia, nie je dôvod, aby právna ochrana dotknutej osoby a jej súkromia bola v tomto prípade upravená benevolentnejšie a neposkytovala jej rovnaké možnosti ako osobe, ktorej bolo do súkromia zasiahnuté odpočúvaním. Zákonodarca by preto mal vziať do úvahy túto závažnosť zásahov do súkromia v podobe vyhotovovania obrazových, zvukových alebo obrazovo-zvukových záznamov a dotknutej osobe týmto zásahom poskytnúť rovnaké možnosti právnej ochrany ako osobe, ktorej bolo do súkromia zasiahnuté odpočúvaním.

2. Monitorovanie osôb podľa iných právnych predpisov

Od vyhotovovania obrazových, zvukových alebo obrazovo-zvukových záznamov treba odlišiť monitorovanie osôb podľa zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. Sledovanie či monitorovanie osôb na mieste prístupnom verejnosti možno vyložiť ako sledovanie (koho, čo) pomocou monitorovacieho zariadenia, v tomto prípade pomocou videozáznamu alebo audiozáznamu.¹³ § 10 ods. 7 cit. zákona umožňuje monitorovanie len za splnenia nasledujúcich podmienok:

1. monitorovať možno len priestor prístupný verejnosti,
2. monitorovať možno len na stanovený účel, ktorým môže byť
 - a. zabezpečenie verejného poriadku a bezpečnosti,
 - b. odhaľovanie kriminality alebo
 - c. narušenie bezpečnosti štátu,
 - d. ochrany majetku alebo zdravia,
3. monitorovaný priestor musí byť zreteľne označený.

V prípade splnenia všetkých zákonných podmienok a získania relevantných informácií možno vyhotovený záznam použiť výlučne na účely trestného konania alebo konania o priestupkoch. V poslednom období sa tak monitorujú najmä verejne prístupné priestory bánk, finančných ústavov, čerpacích staníc, hypermarketov, staníc hromadnej dopravy, pešie zóny miest, hraničné priechody, ako aj iné miesta s potenciálnym narušením verejného poriadku ale zvýšeným rizikom páchania trestnej činnosti. Pre použitie monitorovacieho zariadenia sa nevyžaduje súhlas súdu, ako je tomu v prípadoch využitia informačno-technických prostriedkov, prevádzkovateľ musí spĺňať iba zákonom predpísané požiadavky. Súhlas dotknutej (monitorovanej) osoby je realizovaný predovšetkým zreteľným označením priestoru ako monitorovaným, pričom osoba vstupom do označeného priestoru dáva tak konkludentne súhlas na vyhotovenie obrazovo-zvukového záznamu.¹⁴

Ivor poukazuje na niektoré spoločné a zároveň aj rozdielne znaky medzi vyhotovovaním obrazových, zvukových alebo obrazovo-zvukových záznamov a monitorovaním osôb podľa zákona o ochrane osobných údajov. Medzi **spoločné znaky** podľa neho patrí:

1. vyhotovovanie obrazovo-zvukových záznamov za pomoci špeciálnej techniky,
2. zákonom vymedzený subjekt oprávnený vykonávať vyhotovovanie záznamov a režim jeho realizácie,
3. povinnosť zničiť nevyužiteľné záznamy v stanovenej dobe,
4. zákonná ochrana pred zneužitím získaných záznamov.

Ako **rozdielne znaky** pomenúva:

1. postup podľa § 114 TP je možný len u taxatívne vymedzených, najzávažnejších trestných činov, monitorovanie osôb podľa zákona o ochrane osobných údajov je možné pre zadookumentovanie akéhokoľvek trestného činu i priestupku,
2. postup podľa § 114 TP predpokladá vydanie príkazu sudcu pre prípravné konanie, monitorovanie osôb iba splnenie podmienok uvedených v § 10 ods. 7 zákona o ochrane osobných údajov,

¹³ Ivor, J. Obrazovo-zvukový záznam ako dôkazný prostriedok v trestnom konaní. In Záhora, J. Teoretické a praktické problémy dokazovania. Bratislava: BVŠP, 2008, s. 76.

¹⁴ Ivor, J. Obrazovo-zvukový záznam ako dôkazný prostriedok v trestnom konaní. In Záhora, J. Teoretické a praktické problémy dokazovania. Bratislava: BVŠP, 2008, s. 76.

3. postup podľa § 114 TP oprávňuje vyhotovovať obrazovo-zvukové záznamy nielen na miestach verejnosti prístupných, ale i v obydlí, monitorovanie osôb podľa zákona o ochrane osobných údajov výlučne v priestoroch prístupných verejnosti,
4. postup podľa § 114 TP je časovo limitovaný, monitorovanie osôb nie je časovo limitované, je určované iba jeho účelom,
5. informácie získané použitím ustanovenia § 114 TP sú využiteľné ako dôkaz výlučne pre účely trestného konania, informácie z monitorovania osôb sú využiteľné ako v trestnom konaní, tak i v správnom konaní,
6. postup podľa § 114 TP sa predpokladá iba v rámci začatého trestného konania, monitorovanie je možné vykonávať za splnenia zákonných podmienok mimo trestného konania,
7. postup podľa § 114 TP sa realizuje utajeným spôsobom, monitorovanie osôb predpokladá naopak zreteľné označenie monitorovaného priestoru.¹⁵

Bez ohľadu na uvedené spoločné či rozdielne charakteristické znaky oboch prostriedkov získavania informácií možno konštatovať, že oba prostriedky môžu byť významnými zdrojmi informácií, ktoré môžu byť využiteľné v trestnom konaní a ktoré môžu mať veľmi významnú dôkaznú hodnotu. Predpokladom však je identifikácia osoby, ktorá je na zachytenom zázname. Ak by šlo len o hlasový záznam, nevyhnutným pre trestné konanie bude podrobiť tento záznam fonoskopickému znaleckému skúmaniu. Pokiaľ by išlo o obrazový či obrazovo-zvukový záznam, identifikácia osoby by prichádzala do úvahy jednak laickou rekogničnou formou, ale takisto aj znaleckou expertízou.

Ivor sa v tejto súvislosti zamýšľa nad možnosťami identifikácie osoby podľa získaného záznamu a píše: „Ľudský mozog úplne automaticky porovnáva obraz tváre uloženej vo svojej pamäti s predlohou, ktorú bezprostredne vníma a má ju pred sebou. Proces identifikácie známej osoby spracovaný na základe obrazových informácií tváre trvá mozgu zlomok sekundy. Doterajšie vedecké výskumy potvrdili, že ľudské vnímanie a rozlišovanie osôb podľa tváre je absolútne odlišné od čohokoľvek iného, má svoje špecifiká a je stále zahalené rúškom tajomstva. Vedecká verejnosť si je však absolútne istá, že mozog nie je žiadny super počítač. Napriek tomu v 20. a 21. storočí je vzhľad tváre pre identifikačné účely dôsledne vedecky skúmaný. Primárnym cieľom je strojové (počítačové) vyhľadávanie a rozpoznávanie ľudských tvárí so širokou škálou praktického využitia. Výskum a rozvoj biometrickej metódy identifikácie osoby pomocou jej tváre je dnes požadovaný z mnohých reálnych a rýdzo praktických dôvodov, ktorých význam neobyčajne vzrástol po teroristickom útoku 11. septembra 2001. V literatúre bolo publikovaných veľké množstvo najrôznejších metód a algoritmov pre počítačovú rekogníciu založenú na podobe ľudskej tváre. Rozdelenie týchto metód do určitých kategórií závisí na odlišných kvalifikačných kritériách (napr. štatisticky orientované metódy, znalostné metódy, metódy založené na geometrických tvaroch a identifikačných markantoch, metódy neurónových sietí, atď.). Pre detekciu, lokalizáciu a identifikáciu tváre sa v praxi stretávame obvyčajne so vzájomnou kombináciou viacerých metód. Napriek všetkým dosiahnutým pozitívnym výsledkom sa však musí konštatovať, že identifikácia osoby na základe jej tváre má zatiaľ v porovnaní s metódou odtlačkov prstov alebo očnej dúhovky nižšiu identifikačnú jednoznačnosť.¹⁶

Obdobné monitorovanie (monitorovanie kamerovým systémom) pripúšťa aj zákon č. 1/2014 Z. z. o organizovaní verejných športových podujatí a o zmene a doplnení niektorých zákonov. Podľa § 21 ods. 1 až 4 cit. zákona pri organizovaní rizikového podujatia je organizá-

¹⁵ Ivor, J. Obrazovo-zvukový záznam ako dôkazný prostriedok v trestnom konaní. In Záhora, J. Teoretické a praktické problémy dokazovania. Bratislava: BVŠP, 2008, s. 76.

¹⁶ Ivor, J. Obrazovo-zvukový záznam ako dôkazný prostriedok v trestnom konaní. In Záhora, J. Teoretické a praktické problémy dokazovania. Bratislava: BVŠP, 2008, s. 79.

tor podujatia povinný zriadiť pri vchodoch a východoch športového zariadenia a v priestoroch športového zariadenia kamerový systém, ktorý umožní v čase konania podujatia nepretržité monitorovanie uvedených priestorov a identifikáciu fyzickej osoby alebo iného predmetu a zabezpečí záznam v digitálnej forme. Túto povinnosť má organizátor podujatia na futbalovom podujatí a hokejovom podujatí najvyššej celoštátnej súťaže v kategórii dospelých, ak to ustanovujú požiadavky medzinárodnej športovej organizácie alebo národného športového zväzu.

Kamerový systém byť zriadený tak, aby nezasahoval do súkromia fyzických osôb, ktoré nie sú účastníkmi podujatia. Priestory monitorované kamerovým systémom musia byť zreteľne označené ako monitorované pri každom vstupe do športového zariadenia.

Záznamy vyhotovené z kamerového systému je možné využiť len na účely trestného konania, priestupkového konania, správneho konania, občianskeho súdneho konania, disciplinárneho konania, vedenia a využívania informačného systému podľa § 22 a na účely plnenia úloh na úseku verejného poriadku a bezpečnosti štátu.

Záver

Vychádzajúc z príslušných rozhodnutí Európskeho súdu a Nálezu Ústavného súdu ČR, sp. zn. Pl. ÚS 3/09, v ktorých oba súdy vyjadrili názor, že právo na rešpektovanie obydlia zahŕňa tiež súkromie v sídle spoločnosti, pobočiek či prevádzkarní právnických osôb, ktoré sú na Slovensku považované iba za iné priestory, ktoré neslúžia na bývanie, možno dospieť k záveru, že pri právnej úprave informačno-technických prostriedkov či prostriedkov operatívno-pátracej činnosti by sa v záujme ochrany súkromia nemali robiť rozdiely medzi podmienkami, ak ich použitie je, alebo nie je spojené so vstupom do obydlia. Nejde pritom o problémy, ktoré sa týkajú iba vyhotovovania obrazových, zvukových či obrazovo-zvukových záznamov, ale napríklad aj odpočúvania či použitia agenta.

Podistým kritické sú v tejto súvislosti ustanovenia § 114 ods. 4 Trestného poriadku, § 115 ods. 2 Trestného poriadku a § 117 ods. 6 Trestného poriadku, ktoré upravujú vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov, odpočúvanie a záznam telekomunikačnej prevádzky, ktoré nie sú spojené so vstupom do obydlia, resp. použitie agenta, ktoré taktiež nie je spojené so vstupom do obydlia. Vo všetkých troch prípadoch v prípravnom konaní alebo pred začatím trestného stíhania môže vydať príkaz prokurátor, hoci takýto príkaz je časovo obmedzený (na 24 hodín, pokiaľ ide o vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov a odpočúvanie, resp. na 72 hodín, ak ide o použitie agenta) a do stanoveného času ho musí potvrdiť sudca pre prípravné konanie. Avšak aj napriek tomu treba povedať, že ak by sme mali striktne vychádzať z judikatúry Európskeho súdu a ochranu obydlia klásť na roveň iným priestorom, ktoré neslúžia na bývanie, nie je dôvodné robiť takéto rozdiely, a aj zásahy napríklad do kancelárií, sídiel či pobočiek právnických osôb, by mali byť podmienené rovnako ako zásahy do obydlia, pretože aj tieto priestory poskytujú užívateľom určitú mieru súkromia. (A rovnaká by mala byť aj forma rozhodnutí, ktorými sa takéto zásahy nariaďujú, čo sa vzťahuje na § 117 ods. 6 Trestného poriadku, ktorý pripúšťa, aby príkaz na použitie agenta mohol prokurátor vydať predbežne aj ústne, čo nemožno považovať za dostatočnú mieru právnej ochrany súkromia potenciálne dotknutých osôb).

Takáto úprava je, samozrejme, odôvodnená určitou flexibilitou, pružnosťou či väčšou akcioskopnosťou orgánov činných v trestnom konaní, no na druhej strane by k väčšej miere ochrany súkromia mohla prispieť úprava, ktorá by takúto možnosť nepripúšťala a ktorá by dôsledne trvala na tom, aby sa tieto informačno-technické prostriedky a agent mohli použiť hneď od začiatku

iba na základe príkazu sudcu pre prípravné konanie, čím by sa dosiahla súdna kontrola zásahov do súkromia, ak by sa uvedené prostriedky mali použiť napríklad v kanceláriách firiem. Samozrejme, príslušná právna úprava by sa tým stala rigidnejšou, no ako kompenzácia by k jej väčšej flexibilitě mohla prispieť úprava, keby príkazy mohli vydávať všetky okresné sudy a nielen okresné sudy v sídlach krajských súdov (porovnaj § 24 ods. 4 Trestného poriadku), pretože v pri vydávaní príkazov nejde ešte o náročnosť dokazovania trestných vecí, tak ako pri rozhodovaní o vine a treste v závere hlavného pojednávania, ale iba posúdenie opodstatnenosti a zákonnosti zásahu do práva na súkromie a ochranu tohto práva.

Pri vyhotovovaní obrazových, zvukových alebo obrazovo-zvukových záznamov je okrem už zmienených pripomienok problematickou aj úprava následnej ochrany dotknutej osoby, ktorej bolo vyhotovovaním týchto záznamov zasiahnuté do práva na súkromie, podľa § 114 ods. 8 TP. Prvým problematickým bodom na tejto úprave je zbytočne dlhá, až trojročná doba o právoplatného skončenia trestného stíhania, v rámci ktorej má byť osoba dotknutá vyhotovovaním týchto záznamov informovaná o zásahu do jej práva na súkromie (bližšie pozri závery k odpočúvaniu). Druhým problémom je, že ochrana súkromia dotknutej osoby aj jej následné možnosti právnej ochrany, to znamená ochrany po vykonanom zásahu do jej práva na súkromie, sú oveľa slabšie ako možnosti osoby, ktorej bolo do súkromia zasiahnuté odpočúvaním, pretože v citovanom ustanovení, na rozdiel od § 115 ods. 9 TP, abscentuje možnosť, aby dotknutá osoba mohla podať návrh na preskúmanie zákonnosti príkazu na vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov na Najvyšší súd SR. Zákonodarca by preto mal vziať do úvahy závažnosť zásahov do súkromia v podobe vyhotovovania obrazových, zvukových alebo obrazovo-zvukových záznamov a osobe dotknutej týmto zásahom poskytnúť rovnaké možnosti právnej ochrany ako osobe, ktorej bolo do súkromia zasiahnuté odpočúvaním. V oboch prípadoch je totiž zásah do súkromia veľmi porovnateľný, rozdiel je len v technickom prevedení tohto zásahu.

Literatúra

1. Právne predpisy

Dohovor o ochrane ľudských práv a základných slobôd.

Listina základných práv a slobôd.

Ústava Slovenskej republiky č. 460/1992 Zb.

Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

Zákon č. 301/2005 Z. z., Trestný poriadok.

Zákon č. 1/2014 Z. z. o organizovaní verejných športových podujatí a o zmene a doplnení niektorých zákonov.

2. Odborné publikácie

Aláč, m. Získavanie informácií na spravodajské účely a účely trestného konania. Bratislava: C. H. Beck, 2015, 165 s. ISBN 978-80-89603-32-9.

Benedikovičová, A. Vyhotovenie obrazového, zvukového alebo obrazovo-zvukového záznamu ako dôkazný prostriedok v trestnom konaní. In Kalvodová, V., Hrušáková, M. a kolektiv. Dokazování v trestním řízení. Právní, kriminologické a kriminalistické aspekty. Brno: Masarykova univerzita, Právnická fakulta, 2015, 864 s. ISBN 978-80-89122-75-2.

Čentěš, J. a kol. Trestné právo procesné: Všeobecná a osobitný časť. Šamorín: Heuréka, 2012, 503 s. ISBN 978-80-210-8072-0.

Ivor, J. Obrazovo-zvukový záznam ako dôkazný prostriedok v trestnom konaní. In Záhora, J. Teoretické a praktické problémy dokazovania. Bratislava: BVŠP, 2008, 304 s. ISBN 978-80-89363-17-9.

3. Judikatura

Crémieux proti Francúzsku (rozhodnutie z 25. februára 1993).

Gillow proti Spojenému kráľovstvu (rozhodnutie z 24. novembra 1986).

Chappell proti Spojenému kráľovstvu (rozhodnutie z 30. marca 1989).

Klass a ostatní proti Spolkovej republike Nemecko (rozhodnutie zo 6. septembra 1978).

Miailhe proti Francúzsku (rozhodnutie z 25. februára 1993).

Nález Ústavného súdu ČR, sp. zn. Pl. ÚS 3/09.

Nález Ústavného súdu SR, sp. zn. II. ÚS 5/2011.

Niemietz proti Nemecku (rozhodnutie zo 16. decembra 1992).

Société Colas Est. proti Francúzsku (rozhodnutie zo 16. apríla 2002).

Informačno-technické prostriedky v trestnom konaní – analýza niektorých aspektov aktuálnej právnej úpravy s dôrazom na interpretačné problémy

Information Technical Means in Criminal Proceedings – an Analysis of Some Aspects of Current Legislation with an Emphasis on Interpretation Problems

Remig Kubička¹

Abstrakt: Autor v príspevku poukazuje na niektoré z pohľadu trestno-právnej praxe a autora problematické a sporné časti právnej úpravy trestno-procesných inštitútov súvisiacich s informačno-technickými prostriedkami, prezentuje možný výklad niektorých problematických častí právnej úpravy predmetnej problematiky a ponúka námety na novelizáciu ustanovení vzťahujúcich sa danú problematiku. Po úvahách o vzťahu pojmov informačno-technický prostriedok, dôkazný prostriedok, dôkaz a prameň dôkazov, ustálení znakov trestno-právneho pojmu informačno-technický prostriedok sa autor zaoberá konkrétnymi dôkaznými prostriedkami využívajúcimi informačno-technické prostriedky s dôrazom na problematické a sporné časti právnej úpravy.

Abstract: In this paper, the author points out some parts of the legislation of criminal procedure institutes related to information technical means which are problematic and controversial from the point of view of criminal law practice and the author; he presents a possible interpretation of some problematic parts of the legislation of the problem area and offers suggestions for amendment of the provisions applicable to the given issues. After considering the relationship of terms of information technical means, means of proof, evidence and source of evidence, having stabilized the elements of the criminal and legal concept of information technical means, the author deals with specific means of proof using information technical means with an emphasis on problematic and controversial parts of legislation.

Kľúčové slová: Informačno-technický prostriedok, dôkazný prostriedok, dôkaz, odpočúvanie a záznam telekomunikačnej prevádzky, obrazové, zvukové, obrazovo-zvukové záznamy, zadržanie zásielok.

Keywords: information technical means, means of proof, evidence, interception and recording of telecommunication operation, visual, audio, audio-visual recordings, detention of mail.

Úvod

Právna úprava súvisiaca s využitím informačno-technických prostriedkov predstavuje oblasť bohatú na interpretačné problémy. Úkony súvisiace s využívaním informačno-technických prostriedkov sa zväčša vyznačujú naliehavosťou a s tým súvisiacou časovou tiesňou orgánov rozhodujúcich o ich použití. Preto je namieste, aby právna úprava zvlášť v tejto oblasti bola precízna, zrozumiteľná, jednoznačná a minimalizovala podmienky pre nutnosť riešiť v časovej tiesni aplikačné problémy zo strany orgánov činných v trestnom konaní a súdu. Právna úprava v uvedenej oblasti má v tomto smere rezervy. Domnievam sa, že pokiaľ nie je potrebné riešiť negatívny dopad predmetnej právnej úpravy na ľudské práva a slobody, tejto oblasti je venovaná pri novelizáciách Trestného poriadku len okrajová pozornosť. Môže tomu tak byť preto, že zo strany orgánov aplikujúcich trestné právo nie je vyvíjaná dostatočná iniciatíva na dosiahnutie legisla-

¹ JUDr. Remig Kubička, Okresná prokuratúra Bratislava IV, Hanulova 9/A, Bratislava.

tívnych zmien, keďže sa zväčša nejedná o „každodenne“ sa vyskytujúce právne inštitúty v trestno-právnej praxi.

Pri tvorbe zákonov sa nemožno vyhnúť celkom nedostatkom, ktoré odhalí až právna prax. Legislatívny proces by však mal pružnejšie reagovať na signály z právnej praxe a podnety právnej teórie.

Príspevok si kladie za cieľ najmä upozorniť na niektoré interpretačné problémy v predmetnej oblasti, nedostatky v právnej úprave a poskytnúť námety na úvahy o novelizácii niektorých ustanovení súvisiacich s danou problematikou.

Informačno-technický prostriedok, dôkazný prostriedok, dôkaz a prameň dôkazov

Trestný poriadok obsahuje legálnu definíciu pojmu informačno-technické prostriedky v ustanovení § 10 odsek 21 Trestného poriadku, podľa ktorého *„informačno-technickými prostriedkami sa na účely tohto zákona rozumejú elektrotechnické, rádioradiotechnické, fototechnické, optické, mechanické, chemické a iné technické prostriedky a zariadenia alebo ich súbory použité utajovaným spôsobom pri odpočúvaní a zázname prevádzky v elektronických komunikačných sieťach (ďalej len „odpočúvanie a záznam telekomunikačnej prevádzky“), obrazových, zvukových alebo obrazovo-zvukových záznamov alebo pri vyhľadávaní, otváraní a skúmaní zásielok, ak sa ich použitím zasahuje do základných ľudských práv a slobôd.“*

Na úvod je žiaduce vysvetliť vzťah medzi pojmami informačno-technické prostriedky, dôkazné prostriedky, prameň dôkazov a dôkazy v ich trestno – procesnom ponímaní.

Trestno-právna teória dôsledne rozlišuje medzi pojmami dôkazný prostriedok a dôkaz. Trestný poriadok je už pri rozlišovaní pojmov dôkazný prostriedok a dôkaz menej dôsledný.

Dôkazný prostriedok možno pre oblasť trestného práva procesného definovať ako Trestným poriadkom upravený alebo uznávaný² postup získavania dôkazov z prameňa dôkazov. Dôkaz predstavuje informáciu alebo poznatok získaný z prameňa dôkazov. Prameň dôkazov je zdrojom, z ktorého možno čerpať dôkazy.

Trestný poriadok síce rozlišuje medzi pojmami dôkaz a dôkazný prostriedok, keď v ustanovení § 119 odsek 2 uvádza, že *„za dôkaz môže slúžiť všetko, čo môže prispieť na náležité objasnenie veci a čo sa získalo z dôkazných prostriedkov podľa tohto zákona alebo podľa osobitného zákona.“* V ďalšej vete ustanovenia § 119 odsek 2 Trestného poriadku však zákonodarca práve vo vzťahu k informačno-technickým prostriedkom (a prostriedkom operatívno-pátracej činnosti) už tieto pojmy fakticky stotožňuje, keď uvádza, že *„dôkaznými prostriedkami sú najmä výsluch obvineného, svedkov, znalcov, posudky a odborné vyjadrenia, preverka výpovede namieste, rekognícia, rekonštrukcia, vyšetrovací pokus, obhliadka, veci a listiny dôležité pre trestné konanie, oznámenie, informácie získané použitím informačno-technických prostriedkov alebo prostriedkov operatívno-pátracej činnosti.“* Informácie získané použitím informačno-technických prostriedkov (rovnako ako prostriedkov operatívno-pátracej činnosti) však predstavujú dôkaz. Napriek tomu zákonodarca v druhej vete ustanovenia § 119 odsek 2 Trestného poriadku informácie získané použitím informačno-technických prostriedkov (alebo prostriedkov operatívno-pátracej činnosti) označuje za dôkazný prostriedok.

² Trestný poriadok č. 301/2005 Z. z. v ustanovení § 119 odsek 2 uznáva ako použiteľné v trestnom konaní nielen dôkazné prostriedky upravené v Trestnom poriadku, ale taktiež dôkazné prostriedky podľa osobitného zákona.

Povahu dôkazného prostriedku má odpočúvanie a záznam telekomunikačnej prevádzky, vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov a vyhľadávanie, otváranie a skúmanie zásielok.

Prameňom dôkazu je napríklad odpočúvaný telefonický rozhovor, skúmaná zásielka, na obrazový, zvukový alebo obrazovo-zvukový záznam zachytená osoba alebo vec a zaznamenaný skutkový dej.

Pre úplnosť je namieste dodať, že veci a listiny označené v § 119 odsek 2 Trestného poriadku za dôkazný prostriedok je správne zaradiť medzi pramene dôkazov.

Informačno-technickými prostriedkami sú prostriedky konkretizované v ustanovení § 10 odsek 21 Trestného poriadku (elektrotechnické, rádiotechnické, fototechnické, optické, mechanické, chemické a iné technické prostriedky a zariadenia alebo ich súbory použité utajovaným spôsobom), ktoré sú využívané pri odpočúvaní a zázname telekomunikačnej prevádzky, pri vyhotovovaní obrazových, zvukových alebo obrazovo-zvukových záznamov alebo pri vyhľadávaní, otváraní a skúmaní zásielok.

Odpočúvanie a záznam telekomunikačnej prevádzky, vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov a vyhľadávanie, otváranie a skúmanie zásielok je konkrétnou činnosťou, ktorá sa prostredníctvom nich realizuje.³

„*Informačno-technický prostriedok je technické zariadenie určené na získavanie informácií a nie činnosť.*“⁴

V tejto súvislosti možno dodať, že niekedy osoby činné v trestno-právnej praxi označením informačno-technické prostriedky nesprávne označujú odpočúvanie a záznam telekomunikačnej prevádzky (činnosť).

Úvahy o vzťahu medzi pojmi informačno-technické prostriedky, dôkazné prostriedky, pramene dôkazov a dôkazy je možné ukončiť záverom, v zmysle ktorého nie je vhodné, aby Trestný poriadok na niektorom mieste pojmy dôkazný prostriedok a dôkaz rozlišoval a v rozpore s tým inde uvedené pojmy stotožňoval tak, ako je tomu v ustanovení § 119 odsek 2 Trestného poriadku. Zákonodarca v ustanovení § 119 odsek 2 Trestného poriadku uvedené pojmy v prvej vete rozlišuje (čo možno považovať samo o sebe za správne), zatiaľ čo v druhej vete *práve v súvislosti s informačno-technickými prostriedkami* (a prostriedkami operatívno-pátracej činnosti) tieto pojmy fakticky stotožňuje, keď za dôkazný prostriedok označuje informácie získané použitím informačno-technických prostriedkov, teda to čo fakticky predstavuje dôkaz. Trestný poriadok, ako každý iný právny predpis, by mal používať ten istý pojem vždy v rovnakom význame. Druhú vetu ustanovenia § 119 odsek 2 Trestného poriadku by bolo preto namieste novelizovať. Mohla by mať znenie: „**Dôkaznými prostriedkami sú najmä výsluch obvineného, svedkov, znalcov, posudky a odborné vyjadrenia, previerka výpovede namieste, rekognícia, rekonštrukcia, vyšetrovací pokus, obhliadka, predloženie vecí stranám a čítanie listín dôležitých pre trestné konanie, oznámenie, odpočúvanie a záznam telekomunikačnej prevádzky, vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov, vyhľadávanie, otváranie a skúmanie zásielok alebo prostriedky operatívno-pátracej činnosti.**“

Na to, aby bolo možné určiť prostriedok alebo zariadenie považovať za informačno-technický prostriedok v zmysle Trestného poriadku musí spĺňať kumulatívne podmienky uvedené v ustanovení § 10 odsek 21 Trestného poriadku, ktoré sa týkajú nasledovných znakov:

- technická charakteristika (elektrotechnické, rádiotechnické, fototechnické, optické, mechanické, chemické a iné technické prostriedky a zariadenia alebo ich súbory)

³ Obdobne ZÁHORA, Jozef a kol. *Dokazovanie v trestnom konaní*. Praha: Leges. 2013, s. 254–255.

⁴ ALÁČ, Michal. *Získavanie informácií na spravodajské účely a na účely trestného konania*. Bratislava: C. H. Beck. 2015, s. 54.

- spôsob použitia (utajovaný spôsob použitia)
- *účel použitia* (na odpočúvanie a záznam telekomunikačnej prevádzky, vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov, vyhľadávanie, otváranie a skúmanie zásielok)
- *následok použitia* (použitím sa zasahuje do základných ľudských práv a slobôd).

K utajovanému spôsobu použitia je vhodné uviesť, že utajený spôsob použitia nemožno chápať len ako nepostrehnuteľnosť prostriedku alebo zariadenia zmyslami osoby, do ktorej základných ľudských práv a slobôd sa zasahuje. Použitie informačno-technického prostriedku môže byť zo strany takejto osoby vnímateľné, avšak o skutočnom účele jeho použitia nemá mať vedomosť. Napríklad o utajený spôsob použitia pôjde aj v tom prípade, ak osoba, do ktorej práv a slobôd je zasahované, vníma vyhotovovanie obrazového záznamu, nemá však vedomosť o tom, že záznamom je dokumentovaná jej činnosť, nakoľko subjekt vyhotovujúci záznam predstiera, že zaznamenáva kultúrnu pamiatku, ktorá sa nachádza za záujmovou osobou.

Odpočúvanie a záznam telekomunikačnej prevádzky (odpočúvanie a záznam prevádzky v elektronických komunikačných sieťach)

Názvom odpočúvanie a záznam telekomunikačnej prevádzky zákonodarca označil ustanovenia § 115 a § 116 Trestného poriadku.

Právny inštitút upravený v § 115 Trestného poriadku *„smeruje k zisteniu obsahu telekomunikačnej prevádzky prebiehajúcej v konkrétnej forme buď v aktuálnom čase, alebo v budúcnosti.“*⁵ Ustanovenie § 116 Trestného poriadku, nazvané *„Oznámenie údajov o telekomunikačnej prevádzke“*, upravuje postup pri zisťovaní a oznámení údajov o telekomunikačnej prevádzke, ktorá sa uskutočnila v minulosti.

Mám za to, že inštitút upravený v ustanovení § 116 Trestného poriadku, napriek tomu, že spolu s inštitútom upraveným v ustanovení § 115 Trestného poriadku má spoločný názov „odpočúvanie a záznam telekomunikačnej prevádzky“, nepredstavuje využitie informačno-technických prostriedkov tak, ako to má na mysli ustanovenie § 10 odsek 21 Trestného poriadku. Činnosť uskutočňovaná pri postupe podľa § 116 Trestného poriadku sa neuskutočňuje utajovaným spôsobom.

V praxi orgánov činných v trestnom konaní a súdu je v niektorých prípadoch problematické posudzovanie, či na určitú činnosť možno aplikovať procesný postup upravený v ustanovení § 115 Trestného poriadku.

Aby bolo možné zákonne získavať dôkazy prostredníctvom dôkazného prostriedku upraveného v ustanovení § 115 Trestného poriadku, je nevyhnutné poznať obsah pojmu „odpočúvanie a záznam telekomunikačnej prevádzky“. V rámci toho je opodstatnené vrátiť sa k ustanoveniu § 10 odsek 21 Trestného poriadku, z ktorého je zrejmé, že *„odpočúvanie a záznam telekomunikačnej prevádzky“* predstavuje skrátené označenie *„odpočúvania a záznamu prevádzky v elektronických komunikačných sieťach“*.

Podľa § 2 odsek 1 zákona č. 351/2011 Z. z. o elektronických komunikáciách *„elektronická komunikačná sieť (ďalej len „sieť“) je funkčne prepojená sústava prenosových systémov, a ak je to potrebné, prepájacích alebo smerovacích zariadení, vrátane sieťových prvkov, ktoré nie sú aktívne, ktoré umožňujú prenos signálov po vedení, rádiovými, optickými alebo inými elektromagnetickými prostriedkami, vrátane družicových sietí, pevných sietí s prepájaním okruhov a s prepájaním pake-
tov, internetu a mobilných pozemských sietí, sietí na rozvod elektrickej energie v rozsahu, v ktorom*

⁵ MINÁRIK, Štefan a kol. *Trestný poriadok. Stručný komentár*. Bratislava: IURA EDITION. 2006, s. 351.

sa používajú na prenos signálov, sietí pre rozhlasové a televízne vysielanie a káblových distribučných systémov bez ohľadu na druh prenášaných informácií.“

„Odpočúvaním sa rozumie utajené a účelové vnímanie komunikácie medzi účastníkmi telekomunikačnej prevádzky, ktoré je sprostredkované telekomunikačnými zariadeniami tretej osoby.“⁶ „Záznamom sa rozumie jednak proces zachytenie takto vnímanej komunikácie prebiehajúcej v telekomunikačnej prevádzke na dátový nosič, ktorý umožní uchovanie komunikácie a reprodukciu zachytenej komunikácie v budúcnosti, a jednak to, čo nosič obsahuje.“⁷ „Určitú činnosť možno označiť za komunikáciu, ak ide o dorozumievanie sa, resp. o výmenu informácií medzi pôvodcom informácie a príjemcom informácie, adresátom. Legálne vymedzenie pojmu ‚komunikácia‘ v právnom poriadku Slovenskej republiky neexistuje.“⁸

Odpočúvanie a záznam telekomunikačnej prevádzky sa môže „vzťahovať na prenos informácií prostredníctvom faxov, pevných telefónnych liniek, mobilných telefónov, na prenos krátkych textových správ, vysielačiek a taktiež prenos informácií elektronickou poštou.“⁹ „O použitie informačno-technického prostriedku ide predovšetkým pri odpočúvaní a zaznamenávaní telekomunikačnej prevádzky uskutočnenej prostredníctvom zabezpečených telekomunikačných sietí.“¹⁰ „Pri odpočúvaní a zaznamenávaní telekomunikačnej prevádzky realizovanej prostredníctvom nezabezpečených sietí, najmä formou rádiokomunikácie, nie je potrebný... príkaz sudcu, a preto nejde o použitie informačno-technických prostriedkov v pravom zmysle.“¹¹

Charakter telekomunikačnej prevádzky (prevádzky v elektronických komunikačných sieťach) má výmena informácií prostredníctvom elektronických komunikačných sietí. Podľa M. Aláča „nepôjde o telekomunikačnú prevádzku, ak pôvodca informácie vytvorí informáciu na technickom prostriedku a adresát sa oboznámi s touto informáciou prostredníctvom tohto prostriedku bez toho, aby došlo k akémukoľvek šíreniu informácie prostredníctvom elektronickej komunikačnej siete, ...“¹² „Je nevyhnutné, aby došlo k výmene informácie prostredníctvom dvoch koncových zariadení, resp. jedného koncového zariadenia, avšak prostredníctvom dvoch užívateľských kont.“¹³ „Ak dôjde k záznamu informácie, ktorú záujmová osoba nikam nedistribuovala, ale ju len vytvorila... v trestnom konaní sa tieto informácie získavajú prostredníctvom inštitútu ‚uchovanie a vydanie počítačových údajov‘ upraveného v § 90 Trestného poriadku.“¹⁴

Pokiaľ informácia už bola prenesená prostredníctvom elektronickej komunikačnej siete a je potrebné pre účely trestného konania zistiť obsah už prenesenej informácie (napríklad správy zaslanej prostredníctvom elektronickej pošty), postup podľa § 115 Trestného poriadku už neprichádza do úvahy. Domnievam sa, že na zistenie obsahu takejto správy nemožno využiť ani postup v zmysle § 116 Trestného poriadku (oznámenie údajov o telekomunikačnej prevádzke).

⁶ MINÁRIK, Štefan a kol. *Trestný poriadok. Stručný komentár*. Bratislava: IURA EDITION. 2006, s. 351.

⁷ NOVOTNÁ, Jaroslava. *K některým otázkám dokazování odposlechem a záznamem telekomunikačního provozu* (BECK-ONLINE). In: *Trestněprávní revue*. 2003, č. 10, s. 290.

⁸ ALÁČ, Michal. *Získavanie informácií na spravodajské účely a na účely trestného konania*. Bratislava: C. H. Beck. 2015, s. 72–73.

⁹ ZÁHORA, Jozef a kol. *Dokazovanie v trestnom konaní*. Praha: Leges. 2013, s. 255.

¹⁰ ALÁČ, Michal. *Získavanie informácií na spravodajské účely a na účely trestného konania*. Bratislava: C. H. Beck. 2015, s. 72.

¹¹ ALÁČ, Michal. *Získavanie informácií na spravodajské účely a na účely trestného konania*. Bratislava: C. H. Beck. 2015, s. 72–73.

¹² ALÁČ, Michal. *Získavanie informácií na spravodajské účely a na účely trestného konania*. Bratislava: C. H. Beck. 2015, s. 74.

¹³ ALÁČ, Michal. *Získavanie informácií na spravodajské účely a na účely trestného konania*. Bratislava: C. H. Beck. 2015, s. 74.

¹⁴ ALÁČ, Michal. *Získavanie informácií na spravodajské účely a na účely trestného konania*. Bratislava: C. H. Beck. 2015, s. 74.

Podľa dôvodovej správy k Trestnému poriadku č. 301/205 Z. z. „v § 116 je upravený postup pri poskytovaní a zaobstarávaní registrácie telekomunikačnej prevádzky, napr. aj mobilných telefónov ku konkrétnej osobe alebo osobám. Pôjde najmä o záznamy, ktoré obsahujú identifikačné a účastnícke číslo mobilného telefónu, dátum a čas počiatku hovoru, dobu trvania hovoru, číslo volanej stanice, označenie základnej stanice, ktorá zachytávala hovor v okamžiku spojenia a označenie základnej stanice, ktorá sprostredkovala hovor v okamžiku ukončenia.“¹⁵ Vzhľadom na vyššie citovanú časť dôvodovej správy, ktorá nestratila na aktuálnosti ani po úplnej novelizácii ustanovenia § 116 Trestného poriadku a s ohľadom na v ustanovení § 116 odsek 1 Trestného poriadku použitú formuláciu „príkaz na zistenie a oznámenie **údajov** o telekomunikačnej prevádzke“ sa nazdávam, že postupom podľa § 116 Tr. por. nemožno zisťovať obsah informácií prenesených prostredníctvom telekomunikačnej prevádzky, ale „sprievodné“ údaje viažuce sa ku prenosu informácie. Obsah už prenesenej správy preto podľa môjho názoru je možné získať len postupom podľa § 90 Trestného poriadku (uchovanie a vydanie počítačových údajov).

Podľa § 115 odsek 1 Trestného poriadku „*trestnom konaní o zločine, korupcii, trestných činoch extrémizmu, trestnom čine zneužívania právomoci verejného činiteľa, trestnom čine legalizácie príjmu z trestnej činnosti alebo pre iný úmyselný trestný čin, o ktorom na konanie zaväzuje medzinárodná zmluva, možno vydať príkaz na odpočúvanie a záznam telekomunikačnej prevádzky, ak možno dôvodne predpokladať, že budú zistené skutočnosti významné pre trestné konanie. Príkaz možno vydať, ak nemožno sledovaný účel dosiahnuť inak alebo ak by bolo jeho dosiahnutie iným spôsobom podstatne sťažené. Ak sa pri odpočúvaní a zaznamenávaní telekomunikačnej prevádzky zistí, že obvinený komunikuje so svojim obhajcom, takto získané informácie nemožno použiť na účely trestného konania a musia sa predpísaným spôsobom bez meškania zničiť; to neplatí, ak ide o informácie, ktoré sa vzťahujú na vec, v ktorej advokát nezastupuje obvineného ako obhajcu.*“

Právnu úpravu okruhu trestných činov, pri ktorých je prípustné vydať príkaz na odpočúvanie a záznam telekomunikačnej prevádzky možno z hľadiska trestno-právnej praxe považovať za nie celkom praktickú. Problematická je identifikácia „iných úmyselných trestných činov, o ktorých na konanie zaväzuje medzinárodná zmluva“. Samotný výklad výrazu „iný úmyselný trestný čin, na konanie o ktorom zaväzuje medzinárodná zmluva“ môže byť sporný z toho hľadiska, či má ísť o trestný čin, na konanie o ktorom priamo a bezprostredne zaväzuje medzinárodná zmluva alebo „má ísť aj o všetky ďalšie trestné činy, ktoré majú podklad alebo nadväzujú na medzinárodné zmluvy, obsahujúce záväzok pre štáty, ako ich zmluvné strany, stíhať alebo postihovať niektoré konania v skutkových podstatách týchto trestných činov popísaných, i keď konkrétny vnútroštátny postih sa zásadne vykonáva podľa skutkových podstat trestných činov, ktoré sú súčasťou vnútroštátneho právneho poriadku“.¹⁶ Ak akceptujeme druhý z uvedených názorov, ktorý je zrejme prevažujúci, treba priznať, že pre orgány činné v trestnom konaní a súd je reálne obtiažne a nepraktické identifikovať jednotlivé trestné činy podraditeľné pod slovné spojenie „iný úmyselný trestný čin, o ktorom na konanie zaväzuje medzinárodná zmluva“. V tejto súvislosti je potrebné zohľadniť, ako už bolo naznačené vyššie, že orgány vyhodnocujúce dôvodnosť postupu podľa § 115 Trestného poriadku konajú nezriedka v časovej tiesni a preto je identifikovanie označeného okruhu trestného činu zvlášť problematické. Považujem preto za opodstatnené zamyslieť sa nad možnosťou taxatívneho výpočtu trestných činov v ustanovení § 115 odsek 1 Trestného poriadku, pri ktorých možno využiť odpočúvanie a záznam telekomunikačnej prevádzky, ktoré však nie sú zločinom, korupciou, trestnými činmi extrémizmu, zneužívania právomoci verejného činiteľa a trestným činom legalizácie príjmu z trestnej činnosti.

¹⁵ Dôvodová správa k zákonu č. 301/2005 Z. z., k § 115 a § 116.

¹⁶ KYJAC, Zuzana. POUŽITIE INFORMANO-TECHNICKÝCH PROSTRIEDKOV V TRESTNOM KONANÍ. *Odpočúvanie a záznam telekomunikačnej prevádzky*. Bratislava: Wolters Kluwer, s. r. o. 2015, s. 122.

Vyššie uvedeného úvahy platia aj vo vzťahu k ustanoveniu § 114 odsek 1 Trestného poriadku (vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov), používajúcemu taktiež pojem „*iný úmyselný trestný čin, o ktorom na konanie zaväzuje medzinárodná zmluva*“.

V rámci literatúry zaoberajúcej sa predmetnou problematikou sa možno stretnúť s názormi o opodstatnenosti doplnenia absolútneho zákazu vykonávať odpočúvanie a záznam telekomunikačnej prevádzky medzi obhajcom a obvineným. Domnievam sa, že takýto absolútny zákaz (okrem ďalších okolností, pre ktoré by bolo možné namietat' opodstatnenosť absolútneho zákazu) by ani nebolo možné prakticky dodržať. Pri realizácii odpočúvania v niektorých prípadoch ani nie je možné hneď identifikovať, že obvinený komunikuje s obhajcom.

Podľa § 115 odsek 2 Trestného poriadku „*príkaz na odpočúvanie a záznam telekomunikačnej prevádzky vydáva predseda senátu, pred začatím trestného stíhania alebo v prípravnom konaní sudca pre prípravné konanie na návrh prokurátora. Ak ide o vec, ktorá neznesie odklad, a príkaz sudcu pre prípravné konanie nemožno získať vopred, môže taký príkaz pred začatím trestného stíhania alebo v prípravnom konaní vydať prokurátor, ak odpočúvanie a záznam telekomunikačnej prevádzky nie je spojené so vstupom do obydľia, ktorý však musí najneskôr do 24 hodín od jeho vydania potvrdiť sudca pre prípravné konanie, inak stráca platnosť a takto získané informácie nemožno použiť na účely trestného konania a musia sa predpísaným spôsobom bez meškania zničiť*“.

Pri postupe v zmysle druhej vety ustanovenia § 115 odsek 2 Trestného poriadku je sporná forma rozhodnutia, ktorou má sudca pre prípravné konanie potvrdiť príkaz vydaný prokurátorom.

Podľa § 162 odsek 1 Trestného poriadku „*súd rozhoduje rozsudkom, trestným rozkazom alebo príkazom, kde to zákon výslovne ustanovuje; v ostatných prípadoch rozhoduje, ak zákon neustanovuje niečo iné alebo ak rozhodnutie nemá technicko-organizačnú alebo operatívnu povahu, uznesením*“.

Možno sa stretnúť s názormi, že sudca pre prípravné konanie pri postupe podľa druhej vety § 115 ods. 2 Trestného poriadku príkaz prokurátora potvrdzuje taktiež príkazom. V zmysle § 162 odsek 1 Trestného poriadku predpokladom toho, aby súd zákonne rozhodol príkazom je, že tak zákon výslovne ustanovuje. Je otázne, či zákonné ustanovenie ukladajúce prokurátorovi rozhodovať formou príkazu, možno vykladať tak rozširujúco, že predstavuje tiež výslovné ustanovenie formy rozhodnutia pre sudcu pre prípravné konanie na potvrdenie príkazu prokurátora. Domnievam sa, že tomu tak nie je. Preto mám za to, že v danej veci prichádza do úvahy len rozhodnutie podľa časti ustanovenia § 162 odsek 1 Trestného poriadku za bodkočiarkou (nejedná sa ani o výslovné ustanovenie formy rozhodnutia rozsudkom alebo trestným rozkazom). Zastávam taktiež názor, že rozhodnutie sudcu pre prípravné konanie nemá v tomto prípade technicko-organizačnú ani operatívnu povahu. Súd by mal teda v takom prípade rozhodovať uznesením, proti ktorému logicky nie je prípustná sťažnosť (§ 185 odsek 2 Trestného poriadku). Naznačený postup by zároveň umožnil podľa § 115 odsek 2 Trestného poriadku, druhá veta „*a contrario*“ rozhodnúť uznesením s odôvodnením aj o nepotvrdení príkazu prokurátora v rámci 24-hodinovej lehoty od vydania príkazu prokurátora.

V záujme odstránenie vyššie naznačených pochybností by bolo prospešné v Trestnom poriadku výslovne uviesť formu rozhodnutia, ktorou sudca pre prípravné konanie potvrdzuje príkaz prokurátora vydaný v zmysle § 115 odsek 2 Trestného poriadku.

Za sporné možno považovať tiež, či ustanovenie § 115 Trestného poriadku pokrýva aj zisťovanie lokalizačných údajov identifikujúcich polohu odpočúvaného zariadenia. Zisťovanie lokalizačných údajov predstavuje fakticky zisťovanie informácií o polohe a pohybe osoby alebo

pohybe vecí¹⁷ a teda sledovanie osôb a vecí, predstavujúce inštitút upravený v § 113 Trestného poriadku. Domnievam sa preto, že získavanie dôkazov zabezpečovaním lokalizačných údajov „on line“ by malo byť predmetom výslovnej úpravy v Trestnom poriadku.

Ďalšou spornou otázkou je použiteľnosť dôkazov získaných odpočúvaním a záznamom telekomunikačnej prevádzky v prípade, ak dôjde ku zmene právnej kvalifikácie skutku na trestný čin neuvedený v ustanovení § 115 odsek 1 Trestného poriadku.

Riešenie tejto otázky považujem za veľmi problematické. Podľa jednej skupiny názorov dôkazy získané postupom podľa § 115 Trestného poriadku je možné použiť aj po vyššie naznačenej zmene právnej kvalifikácie, ak v čase ich získania bola dôvodná právna kvalifikácia skutku ako trestný čin uvedený v § 115 odsek 1 Trestného poriadku. Akceptovanie tohto názoru však môže vytvoriť podmienky na to, aby orgán činný v trestnom konaní alebo súd účelovo, s cieľom predĺžiť možnosť získavania dôkazov postupom podľa § 115 Trestného poriadku, vykonal s oneskorením dôkaz, pri ktorom existuje predpoklad, že odôvodní zmenu právnej kvalifikácie na trestný čin neuvedený v § 115 odsek 1 Trestného poriadku. Po zmene právnej kvalifikácie na trestný čin neuvedený v § 115 odsek 1 Trestného poriadku môže byť tiež sporné, kedy reálne nastali podmienky pre takúto zmenu právnej kvalifikácie a tým aj na stratu zákonnej možnosti získavania dôkazov postupom podľa § 115 Trestného poriadku (inými slovami, kedy nastal moment, do ktorého ešte bolo možné získavať zákonné a použiteľné dôkazy odpočúvaním a záznamom telekomunikačnej prevádzky).

Ako najlogickejší považujem názor, podľa ktorého pri prekvalifikovaní skutku na trestný čin neuvedený v § 115 odsek 1 Trestného poriadku, by nepoužiteľnosť dôkazov získaných postupom podľa § 115 Trestného poriadku mala pôsobiť spätne aj na obdobie do zmeny právnej kvalifikácie skutku. Teda pokiaľ by bolo zistené na základe vykonaného dokazovania, že skutok nie je dôvodné posudzovať v zmysle právnej kvalifikácie uvedenej v § 115 odsek 1 Trestného poriadku, dôkazy získané odpočúvaním a záznamom telekomunikačnej prevádzky nie je možné od začiatku použiť ako dôkaz. Aj takéto riešenie spojené so spätným vylúčením dôkazov získaných postupom podľa § 115 Tr. por. (napríklad pred vyhlásením rozsudku) môže byť problematické. Problematické sa javí byť napríklad vylúčenie takýmto spôsobom získaných dôkazov preukazujúcich nevinu obžalovaného v prípade, ak po ich vylúčení z podkladov pre rozhodnutie dôvody na oslobodenie obžalovaného spod obžaloby nebudú existovať.

Vyššie naznačený aplikačný problém sa týka aj inštitútov sledovanie osôb a vecí podľa § 113 Trestného poriadku a vyhotovovania obrazových, zvukových alebo obrazovo-zvukových záznamov podľa § 114 Trestného poriadku.

Možno povedať, že v trestno-právnej praxi a literatúre už bola venovaná pomerne veľká pozornosť výkladu ustanovenia § 115 odsek 7 Trestného poriadku, podľa ktorého *„v inej trestnej veci, ako je tá, v ktorej sa odpočúvanie a záznam telekomunikačnej prevádzky vykonal, možno záznam ako dôkaz použiť len vtedy, ak sa súčasne aj v tejto veci vedie trestné konanie pre trestný čin uvedený v odseku 1“*. Problematická je odpoveď na otázku, či požiadavka vedenia trestného konania pre trestný čin uvedený v odseku 1 sa vzťahuje k okamihu realizácie odpočúvania alebo až k okamihu použitia výsledku odpočúvania v inej trestnej veci.

Podľa uznesenia Najvyššieho súdu SR sp. zn. 3 To 2/2011 *„slovko ‚súčasne‘ je potrebné správne vzťahovať až k okamžiku použitia výsledkov odposluchu a nie už k okamihu vykonávania odposluchu.“*

¹⁷ Na základe zistenia lokalizačných údajov možno napríklad získať informácie o pohybe mobilného telefónu získaného páchatelom pri lúpeží, čo fakticky predstavuje sledovanie pohybu vecí (mobilného telefónu).

Opačný názor je konštatovaný v rozsudku Najvyššieho súdu SR sp. zn. 2To 5/2011, podľa ktorého „slovom ‚súčasne‘ uvedeným v § 115 odsek 7 Trestného poriadku ako podmienky pre použitie záznamu telekomunikačnej prevádzky ako dôkazu v inej trestnej veci, ako je tá, v ktorej sa odpočúvanie vykonalo a záznam vyhotovil, sa rozumie vedenie trestného konania v inej trestnej veci už v čase vykonania záznamu telekomunikačnej prevádzky vo veci, v ktorej bol vydaný príkaz na odpočúvanie a záznam telekomunikačnej prevádzky podľa § 115 ods. 2 Trestného poriadku, teda nie vedenie trestného konania v oboch dotknutých veciach až v čase použitia záznamu v inej trestnej veci ako dôkazu.“

V rámci výkladu ustanovenia § 115 odsek 7 Trestného poriadku sa stotožňujem s prvým z vyššie uvedených názorov. Druhý z uvedených názorov by mal opodstatnenie, ak by v prvej časti ustanovenia § 115 odsek 7 Trestného poriadku bol použitý prítomný čas namiesto použitého minulého času („vykonáva“ namiesto použitého „vykonal“). Či však tento názor zodpovedá zámeru zákonodarcu je otázne aj vzhľadom na použitý výraz „súčasne“. Zákonodarca mohol len nedopatrením použiť v ostatnej časti nesprávnu formuláciu.

Vzhľadom na vyššie uvedené a nejednotný výklad § 115 odsek 7 Trestného poriadku a zároveň nie ojedinelú potrebu riešenia naznačeného aplikačného problému, sa novelizácia označeného ustanovenia javí byť naliehavou.

Obdobné nejasnosti sa týkajú aj výkladu ustanovení § 113 odsek 9 Trestného poriadku (sledovanie osôb a vecí) a § 114 odsek 7 Trestného poriadku (vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov).

Sledovanie osôb a vecí s použitím informačno-technického prostriedku a vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov

Na niektoré problematické ustanovenie trestno-procesnej úpravy sledovania osôb a vecí s použitím informačno-technického prostriedku a vyhotovovania obrazových, zvukových alebo obrazovo-zvukových záznamov už bolo poukázané vyššie v rámci pojednania o zodpovedajúcich ustanoveniach Trestného poriadku vzťahujúcich sa na odpočúvanie a záznam telekomunikačnej prevádzky.

Pochybnosti vyvoláva už samotné identifikovanie rozdielu medzi prípadmi, pri ktorých možno zákonne získavať dôkazy prostredníctvom sledovania osôb a vecí s použitím informačno-technického prostriedku a prípadmi, keď má zákonné opodstatnenie získavanie dôkazov vyhotovovaním, obrazových, zvukových alebo obrazovo-zvukových záznamov. Vysvetlenie rozdielu možno nájsť v uznesení Najvyššieho súdu SR sp. zn. 6 Tdo 31/2016, podľa ktorého „postup podľa § 113 Trestného poriadku možno označiť ako tzv. ‚in move‘, a teda sledovanie v pohybe, naproti tomu postup podľa § 114 Trestného poriadku je určený prioritne na stacionárne ‚sledovanie‘ ako tzv. ‚steady‘ procesný prostriedok.“

So správnosťou vyššie uvedeného rozlišovania dôvodnosti postupu podľa § 113 a § 114 Trestného poriadku možno vyjadriť pochybnosti.

P. Šamko v tejto súvislosti uvádza, že „ustanovenie § 113 ods. 1 TP síce hovorí o tom, že sledovaním osôb a vecí sa rozumie získavanie informácií o pohybe a činnosti osoby alebo pohybe vecí, avšak to automaticky neznamená, že musí byť v pohybe aj sledovacie zariadenie. Neznamená to ani, že sa musí sledovať pohyb osoby, či veci na každom mieste, kde sa táto vec alebo osoba počas sledovania nachádza. Napríklad, sledovať pohyb a činnosť určitej osoby možno aj tak, že sa monitoruje jej pohyb a činnosť na jednom konkrétnom záujmovom mieste (napríklad výskyt tejto osoby

na takomto mieste a jej činnosť na tomto konkrétnom mieste). V takomto prípade je sledovanie stationárne s tým, že je zamerané na konkrétne miesto a sleduje akýkoľvek pohyb a činnosť na tomto konkrétnom mieste a vyhodnocuje sa výskyt a činnosť záujmovej osoby na tomto mieste.“¹⁸

Domnievam sa, že použitie dôkazného prostriedku vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov má opodstatnenie, keď je potrebné získavať informácie o veci, ktorá nie je v pohybe (sledovanie veci je naopak zamerané na získavanie informácií o pohybe veci – vid' § 113 odsek 1 Trestného poriadku). Napríklad vyhotovovanie obrazových záznamov je namieste, keď sa má potvrdiť podozrenie, že dutina v strome je využívaná ako tzv. mŕtva schránka pri distribúcii drog a predmetom vyhotovovania záznamu je dutina v strome, teda nehybná vec.

Identifikovať nespochybniteľný rozdiel medzi sledovaním osoby s využitím informačno-technického prostriedku a vyhotovovaním obrazových, zvukových alebo obrazovo-zvukových záznamov, na ktorom majú byť zaznamenávané prejavy osoby zrejme ani nie je možné. Je tomu tak preto, že sledovanie osoby zahŕňa nielen získavanie poznatkov o pohybe, ale aj o činnosti osoby. Sledovaná osoba pritom len ťažko bude nečinná a súčasne aj nevykonávajúca pohyb, ktorý je predmetom záujmu.

Možno sa tiež zamyslieť nad tým, či na ukladanie informácií získaných použitím informačno-technického prostriedkov pri sledovaní osôb a vecí na hmotný nosič dát (zhotovenie záznamu zo sledovania s použitím informačno-technického prostriedku) nie je potrebné okrem príkazu podľa § 113 odsek 4 Trestného poriadku vydať aj príkaz podľa § 114 Trestného poriadku. Takúto úvahu však zrejme je opodstatnené uzavrieť konštatovaním, že toto nebolo zámerom zákonodarcu vzhľadom na ustanovenie § 113 odsek 7 Trestného poriadku, podľa ktorého „ak sa má záznam vyhotovený pri sledovaní použiť ako dôkaz, postupuje sa primerane podľa § 115 ods. 6.“ Teda samotný § 113 Trestného poriadku pripúšťa pri postupe podľa jeho ustanovení vyhotovovať záznam zo sledovania.

Vyhľadávanie, otváranie a skúmanie zásielok

S používaním informačno-technických prostriedkov súvisia právne inštitúty upravené v ustanoveniach § 108 Tr. por. (zadržanie zásielok) a § 109 Trestného poriadku (otvorenie zásielok).

Vzhľadom na stanovený cieľ príspevku považujem za vhodné podrobiť analýze najmä ustanovenie § 108 odsek 1 Trestného poriadku.

Podľa § 108 odsek 1 Trestného poriadku „ak je na objasnenie skutočností závažných pre trestné konanie nevyhnutné zistiť obsah nedoručených telegramov, listov alebo iných zásielok, ktoré pochádzajú od obvineného alebo sú mu určené, predseda senátu a pred začatím trestného stíhania alebo v prípravnom konaní prokurátor alebo s jeho súhlasom policajt vydá príkaz, aby mu ich pošta alebo právnická osoba, ktorá vykonáva ich prepravu, vydali.“

Podľa § 10 odsek 12 Trestného poriadku „ak z povahy veci nevyplýva niečo iné, obvineným sa rozumie aj obžalovaný a odsúdený.“

Podľa § 33 Trestného poriadku „toho, kto je podozrivý zo spáchania trestného činu, možno považovať za obvineného a použiť proti nemu prostriedky určené týmto zákonom proti obvinenému až vtedy, ak bolo proti nemu vznesené obvinenie“.

Na podmienok uvedených v ustanovení § 108 odsek 1 Trestného poriadku teda môže byť vydaná len zásielka pochádzajúca od obvineného alebo určená obvinenému. Vzhľadom na vyššie

¹⁸ ŠAMKO, Peter. Aplikčné problémy pri vyhotovovaní obrazových záznamov zo sledovania osôb alebo vecí. Klientsky program ONLINE Aspi. In: Zo súdnej praxe. 2017, č. 1, s. 10–13.

citované ustanovenia § 10 odsek 12 a § 33 Trestného poriadku, podľa ktorých predpokladom toho, aby bolo možné určitú osobu označiť ako obvineného, je vznesenie obvinenia a pri zohľadnení faktu, že ku vzneseniu obvinenia môže dôjsť až po začatí trestného stíhania, oprávnenie prokurátora a policajta (so súhlasom prokurátora) vydať príkaz na vydanie zásielky v zmysle § 108 odsek 1 Trestného poriadku je nepoužiteľné v štádiu trestného konania pred začatím trestného stíhania. Označený vnútorný rozpor ustanovenia § 108 odsek 1 Trestného poriadku možno odstrániť v rámci novelizácie Trestného poriadku vypustením textu o uvedenom oprávnení prokurátora a policajta v štádiu pred začatím trestného stíhania.

Podľa § 108 odsek 2 Trestného poriadku *„v trestnom konaní o zločinoch, korupcii, trestnom čine zneužívania právomoci verejného činiteľa a trestnom čine legalizácie príjmu z trestnej činnosti môže predseda senátu a pred začatím trestného stíhania alebo v prípravnom konaní na návrh prokurátora sudcu pre prípravné konanie vydať príkaz, aby mu pošta alebo právnická osoba, ktorá vykonáva prepravu zásielok, vydala zásielku, pri ktorej je dôvodné podozrenie, že ňou bol spáchaný taký trestný čin alebo s takým trestným činom súvisí, ak je na objasnenie skutočností závažných pre trestné konanie nevyhnutné zistiť jej obsah.“*

Na rozdiel od ustanovenia § 108 odsek 1 Trestného poriadku ustanovenie § 108 odsek 2 Trestného poriadku stanovuje prísnejšie podmienky pre vydanie príkazu na vydanie zásielky. Domnievam sa, že zákonodarcu k stanoveniu prísnejších podmienok motivoval fakt, že vydanie zásielky v zmysle tohto ustanovenia je prípustné nielen pred vznesením obvinenia, ale tiež pred začatím trestného stíhania. Znenie ustanovenia § 108 ods. 1 Trestného poriadku taktiež pripúšťa vydanie zásielky v prípade, ak už bolo vznesené obvinenie, avšak zásielka nepochádza od obvineného ani nie je určená obvinenému. Napríklad môže ísť o zásielku obsahujúcu dôkazy o trestnom čine zasielanú medzi príbuznými obvineného. Sprísnenie podmienok pre postup podľa tohto ustanovenia je dané viacerými okolnosťami. Predmetný príkaz možno vydať v porovnaní s odsekom 1 len pri obmedzenom okruhu úmyselných trestných činov. Prokurátor pri postupe podľa § 108 odsek 1 Trestného poriadku disponuje v štádiu pred začatím trestného stíhania a v prípravnom konaní len oprávnením podať návrh na vydanie príkazu na vydanie zásielky, pričom na vydanie samotného príkazu je v uvedených štádiách trestného konania oprávnený len sudca pre prípravné konanie.

Podľa § 108 odsek 3 Trestného poriadku *„bez príkazu podľa odseku 2 možno prepravu zásielky zadržať na príkaz prokurátora alebo policajta, ale len vtedy, ak nemožno príkaz podľa odseku 2 vopred zadovážiť a vec neznesie odklad. Ak v takom prípade nedôjde pošte alebo právnickej osobe vykonávajúcej prepravu zásielok do troch dní príkaz predsedu senátu a v prípravnom konaní sudcu pre prípravné konanie, aby sa mu zásielky vydali, nesmie pošta alebo právnická osoba prepravu zásielok ďalej zadržiavať. Listovú zásielku alebo iný nosič informácií medzi obhajcom a obvineným nemožno zadržať.“*

Zákonodarca sa už v § 108 odsek 3 Trestného poriadku nezmieňuje o štádiu trestného konania pred začatím trestného stíhania. Je tomu tak zrejme preto, že vychádza z predpokladu, že už zadržanie prepravy zásielky na príkaz prokurátora alebo policajta predstavuje zaistovací a súčasne neodkladný úkon, ktorého vykonaním v zmysle § 199 odsek 1 Trestného poriadku začalo trestné stíhanie (a súčasne taktiež prípravné konanie). Teda v čase následného vydania príkazu sudcu pre prípravné konanie na vydanie zásielky už bude prebiehať prípravné konanie.

Ustanovenie § 108 odsek 3 Trestného poriadku dáva policajtovi a prokurátorovi oprávnenie vydať príkaz na zadržanie prepravy zásielky aj v štádiu konania pred súdom. Takýto výklad § 108 odsek 3 Trestného poriadku umožňuje v tomto ustanovení zakotvené oprávnenie predsedu senátu vydať príkaz na vydanie zadržanej zásielky v spojení s faktom, že iný subjekt ako pro-

kurátor alebo policajt nie sú osobami oprávnenými vydať príkaz na v tomto ustanovení upravené „predbežné“ zadržanie prepravy zásielky.

V zmysle poslednej vety ustanovenia § 108 odsek 3 Trestného poriadku („Listovú zásielku alebo iný nosič informácií medzi obhajcom a obvineným nemožno zadržať.“) nie je prípustné zadržať listovú zásielku alebo iný nosič informácií medzi obvineným a obhajcom, ani ak informácia majúca vyplývať zo zadržanej listovej zásielky alebo iného hmotného nosiča informácií sa vzťahuje na vec, v ktorej obhajca nezastupuje obvineného. Zákaz zadržania zásielky sa logicky vzťahuje aj na prípad, keď obhajca zastupuje obvineného v inej trestnej veci, ako je tá, v ktorej by mala byť zásielka zadržaná.

Možno sa prikloniť k názoru, že právnu úpravu rozsahu zákazu zadržať zásielku a iný nosič informácií prepravovaný medzi obvineným a obhajcom by bolo vhodné obmedziť len v rozsahu obdobnom ako je to v ustanovení § 115 ods. 1 Tr. por. (odpočúvanie a zaznamenávanie telekomunikačnej prevádzky).¹⁹

Záver

Ako vyplýva z vyššie uvedeného, trestno-právna úprava súvisiaca s používaním informačno-technických prostriedkov predstavuje bohatý zdroj interpretačných problémov. Ambíciou tohto príspevku nebolo vyčerpávajúce pomenovanie všetkých interpretačných problémov súvisiacich s danou problematikou. Naznačuje však ich rozsah, negatívne dôsledky a snaží sa posilniť hlasy požadujúce nutnosť novelizácie Trestného poriadku v predmetnej oblasti, ale zároveň upozorňuje aj okolnosti, ktoré by mali byť vzaté do úvahy pri novelizácii. Autor na záver vyjadruje pranie, aby ku podstatnej novelizácii v danej oblasti v dohľadnej dobe došlo.

Zoznam literatúry:

1. ALÁČ, Michal. *Získavanie informácií na spravodajské účely a na účely trestného konania*. Bratislava: C. H. Beck. 2015
2. KYJAC, Zuzana. *POUŽITIE INFORMANO-TECHNICKÝCH PROSTRIEDKOV V TRESTNOM KONANÍ. Odpočúvanie a záznam telekomunikačnej prevádzky*. Bratislava: Wolters Kluwer, s. r. o. 2015
3. MINÁRIK, Štefan a kol. *Trestný poriadok. Stručný komentár*. Bratislava: IURA EDITION. 2006
4. ZÁHORA, Jozef a kol. *Dokazovanie v trestnom konaní*. Praha: Leges. 2013
5. NOVOTNÁ, Jaroslava. *K některým otázkám dokazování odposlechem a záznamem telekomunikačního provozu* (BECK-ONLINE). In: *Trestněprávní revue*. 2003, č. 10
6. ŠAMKO, Peter. *Aplikačné problémy pri vyhotovovaní obrazových záznamov zo sledovania osôb alebo vecí*. Klientsky program ONLINE Aspi. In: *Zo súdnej praxe*. 2017, č. 1, s. 10–13.
7. Dôvodová správa k zákonu č. 301/2005 Z. z.
8. Uznesenie Najvyššieho súdu SR sp. zn. 3 To 2/2011
Rozsudok Najvyššieho súdu SR sp. zn. 2To 5/2011
Uznesenie Najvyššieho súdu SR sp. zn. 6 Tdo 31/2016
9. zákon č. 301/2005 Z. z. Trestný poriadok
10. zákon č. 351/2011 Z. z. o elektronických komunikáciách

¹⁹ Obdobne ALÁČ, Michal. *Získavanie informácií na spravodajské účely a na účely trestného konania*. Bratislava: C. H. Beck. 2015, s. 99.

Príkaz na odpočúvanie a záznam telekomunikačnej prevádzky podľa § 115 Trestného poriadku

Order on the Interception and Recording of the Communications Pursuant to Section 115 of the Code of Criminal Procedure

Nina Vančíková¹

Abstrakt: Príspevok sa zaoberá zákonnými podmienkami aplikácie príkazu na odpočúvanie a záznam telekomunikačnej prevádzky, pričom poukazuje na niektoré aplikačné problémy súvisiace s výkonom tohto inštitútu a načrtáva možnosti ich riešenia.

Abstract: The paper deals with the legal conditions of application of the order for interception and recording of the communications, points out some application problems related to the performance of the Institute and outlines possible solutions.

Kľúčové slová: Odpočúvanie a záznam telekomunikačnej prevádzky, príkaz, uchovanie záznamu, prepis záznamu, zničenie záznamu, dôkaz.

Key words: Interception and recording of telecommunications, command, data storage, transcribing, destruction of records, evidence.

Úvod

„Legitímne úsilie štátu potláčať závažnú spoločensky nebezpečnú a nežiadúcu kriminalitu nemôže byť realizované tak, že orgány činné v trestnom konaní uskutočnia k dosiahnutiu tohto účelu čokoľvek, čo považujú z hľadiska chceného a predsavzatého cieľa za vhodné.“²

„Legalitu zásahu štátu do práva na súkromie možno chápať, ako zásah, ktorý je možný len na základe zákona, či platného právneho predpisu, pričom pri posudzovaní splnenia tejto podmienky je potrebné vychádzať z toho, či bola rešpektovaná dostupnosť (verejné publikovanie právneho predpisu) a predvídateľnosť zákona. V rámci podmienky predvídateľnosti zákona judikatúra Európskeho súdu pre ľudské práva zdôrazňuje potrebu konkretizovania prostriedkov, ktorými štát disponuje pri zasahovaní do práv chránených článkom 8 Dohovoru o ochrane ľudských práv a základných slobôd v znení dodatkových Protokolov (ďalej len „Dohovor“), kladie teda dôraz na kvalitu relevantnej právnej úpravy.“ V rozhodnutí *Sallinen c. Fínsko* súd vyslovil záver, že vnútroštátne právo musí poskytovať jednotlivcovi ochranu proti arbitrárnemu zásahu do jeho práv zaručených článkom 8 Dohovoru, a preto musí dostatočne jasne v pojmoch poskytovať občanovi náležitú indikáciu podľa okolností a podmienok, za akých je verejná autorita zmocnená na zásah do jeho práva na súkromie.

„Podmienka legitímnosti zase vyžaduje, aby opatrenie umožňujúce zásah štátu do práva na súkromie zodpovedalo cieľu odôvodňujúcemu jeho legitimitu, ktorým môžu byť len záujmy výslovne špecifikované dohovorom, a teda záujem štátu (z dôvodu ochrany národnej bezpečnosti, verejnej bezpečnosti, predchádzania nepokojov a zločinnosti), záujem spoločnosti (z dôvodu ochrany zdravia alebo morálky, zabezpečenia hospodárskeho blahobytu krajiny) a záujem jednotlivcov (z dôvodu ochrany ich práv a slobôd).“

¹ JUDr. Nina Vančíková, externá doktorandka Fakulty práva Paneurópskej vysokej školy.

² Nález Ústavného súdu Českej republiky III. ÚS 501/04 z 3. 3. 2005.

„Kritérium proporcionality zásahu znamená dodržanie rovnováhy vo vzťahu medzi právom jednotlivca na súkromie a výberom prostriedkov, ktorými štát disponuje pri plnení legitímneho cieľa. Pri ich výbere je limitovaný tým, že zásah do práva na súkromie je možný len vtedy, keď to je nevyhnutné, a vykonať ho možno len v duchu požiadaviek kladených na demokratickú spoločnosť.“³

Podľa článku 13 odsek 4 zákona číslo 460/1992 Zb. Ústavy Slovenskej republiky (ďalej len „Ústava“) sa pri obmedzovaní základných práv a slobôd musí dbať na ich podstatu a zmysel, pričom takéto obmedzenia sa môžu použiť len na ustanovený cieľ. Právo na súkromie a právo na ochranu osobných údajov nemajú charakter absolútneho práva, t. j. zákonodarcia ich môže obmedziť, avšak len za podmienky, že ide o také obmedzenia, ktoré dbajú na jeho podstatu a zmysel a sú použité len na ustanovený legitímny cieľ.

Podľa článku 22 odsek 1 Ústavy listové tajomstvo, tajomstvo dopravovaných správ a iných písomností a ochrana osobných údajov sa zaručujú.

Podľa článku 22 odsek 2 Ústavy nikto nesmie porušiť listové tajomstvo ani tajomstvo iných písomností a záznamov, či už uchovávaných v súkromí, alebo zasielaných poštou, alebo iným spôsobom; výnimkou sú prípady, ktoré ustanoví zákon. Rovnako sa zaručuje tajomstvo správ podávaných telefónom, telegrafom alebo iným podobným zariadením.

Podľa článku 13 Listiny základných práv a slobôd (ďalej len „Listiny“) nikto nesmie porušiť listové tajomstvo ani tajomstvo iných písomností a záznamov, či už uchovávaných v súkromí alebo zasielaných poštou alebo iným spôsobom, s výnimkou prípadov a spôsobom, ktoré ustanoví zákon. Rovnako sa zaručuje tajomstvo správ podávaných telefónom, telegrafom alebo iným podobným zariadením.

Podľa článku 8 odsek 1 Dohovoru každý má právo na rešpektovanie svojho súkromného a rodinného života, obdobia a korešpondencie.

Podľa článku 8 odsek 2 Dohovoru štátny orgán nemôže do výkonu tohto práva zasahovať okrem prípadov, keď je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojov a zločinnosti, ochrany zdravia alebo morálky alebo ochrany práv a slobôd iných.

Podľa článku 52 odsek 1 Charty základných práv Európskej únie (ďalej len „Charta“) akékoľvek obmedzenie výkonu práv a slobôd uznaných v tejto Charte musí byť ustanovené zákonom a rešpektovať podstatu týchto práv a slobôd, pričom na základe zásady proporcionality sú takéto obmedzenia možné len vtedy, ak sú nevyhnutné a skutočne spĺňajú ciele všeobecného záujmu uznané Úniou, alebo potrebu chrániť práva a slobody iných.

V článku 8 Dohovoru sa odzrkadľuje tzv. negatívna povinnosť štátu spočívajúca v obmedzení zásahov verejnej moci do súkromného života každého nositeľa tohto práva. Zatiaľ čo článok 8 odsek 1 Dohovoru jednoznačne garantuje adresátovi tejto právnej normy právo na súkromie, odsek 2 citovaného článku prísne limituje a taxatívne vymedzuje povolené zásahy štátu do súkromnej sféry jednotlivca. Vzhľadom na skutočnosť, o akej svedčí závažnosť možných zásahov štátu do práva na súkromie, čo je veľakrát spojené s následkami ťažko napravitelnými, štrasburské orgány ochrany práva vnímajú v koncepcii práva na súkromie aj pozitívnu povinnosť štátu podniknúť všetky kroky proti porušovaniu tohto práva. Za prelomové možno považovať rozhodnutie EŠLP vo veci *Marckx c. Belgicko* z 13. júna 1979, ktoré rozšírilo ochranu práva na súkromie aj na prípady, keď štát nevytvoril podmienky proti porušeniu tohto práva, z čoho bol

³ Nález Ústavného súdu Slovenskej republiky PL. ÚS 10/2014-78 z 29. 4. 2015.

odvodený tzv. pozitívny záväzok štátu na vytvorenie takých podmienok, ktoré by znemožňovali porušenie práva na súkromie.⁴

1. Odpočúvanie a záznam telekomunikačnej prevádzky

Odpočúvanie a záznam telekomunikačnej prevádzky podľa § 115 zákona číslo 301/2005 Z. z. Trestného poriadku v znení neskorších právnych predpisov (ďalej len „Trestný poriadok“) možno charakterizovať ako zákonom povolený zásah orgánov verejnej moci do súkromia fyzickej osoby, umožňujúci im zistiť obsah telekomunikačnej prevádzky, a to v aktuálnom čase alebo v budúcnosti, alebo obsahové údaje alebo prevádzkové údaje, ktoré sú v reálnom čase prenášané prostredníctvom počítačového systému, ktorý je vykonávaný utajovaným spôsobom na účely zabezpečenia dôkazu v trestnom konaní.⁵

V § 10 odsek 21 Trestného poriadku sú definované informačno-technické prostriedky, ktorými sa na účely tohto zákona rozumejú elektrotechnické, rádiotechnické, fototechnické, optické, mechanické, chemické a iné technické prostriedky a zariadenia alebo ich súbory použité utajovaným spôsobom pri odpočúvaní a zázname prevádzky v elektronických komunikačných sieťach (ďalej len „odpočúvanie a záznam telekomunikačnej prevádzky“), obrazových, zvukových alebo obrazovo-zvukových záznamov alebo pri vyhľadávaní, otváraní a skúmaní zásielok, ak sa ich použitím zasahuje do základných ľudských práv a slobôd. Na spracúvanie informácií získaných použitím informačno-technických prostriedkov, ich evidenciu, dokumentáciu, ukladanie a vyraďovanie sa vzťahujú osobitné predpisy, ak tento zákon neustanovuje inak. Prevádzkovatelia verejných telefónnych sietí, poskytovatelia elektronických telekomunikačných sietí, poskytovatelia elektronických telekomunikačných služieb, poštový podnik, dopravcovia a iní zasielatelia a ich zamestnanci sú povinní poskytnúť nevyhnutnú súčinnosť pri použití informačno-technických prostriedkov; pritom sa nemôžu dovoľávať povinnosti mlčanlivosti podľa osobitných zákonov.

Podmienky na poskytovanie elektronických komunikačných sietí a elektronických komunikačných služieb, práva a povinnosti podnikov a užívateľov elektronických komunikačných sietí a elektronických komunikačných služieb, ochranu elektronických komunikačných sietí a elektronických komunikačných služieb, ochranu súkromia a ochranu spracúvania osobných údajov v oblasti elektronických komunikácií, pôsobnosť orgánov štátnej správy v oblasti elektronických komunikácií a ďalšie upravuje zákon číslo 351/2011 Z. z. o elektronických komunikáciách v znení neskorších právnych predpisov.

Na tomto mieste je potrebné uviesť, že existuje i odpočúvanie mimo trestného konania a to na základe zákona číslo 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) v znení neskorších právnych predpisov. Vzhľadom na rozsah príspevku a najmä na vytýčený cieľ, budeme sa ďalej venovať len odpočúvaniu v rámci trestného konania.

Podstatou odpočúvania podľa § 115 Trestného poriadku je pred účastníkmi aktuálne prebiehajúcej telekomunikačnej prevádzky utajené a účelové vnímanie ich komunikácie, ktoré je sprostredkované telekomunikačným zariadením, tretím subjektom. Záznamom sa v rôznych súvislostiach rozumie jednak zaznamenávanie takto vnímanej komunikácie prebiehajúcej v te-

⁴ Nález Ústavného súdu Slovenskej republiky III. ÚS 133/2010 z 27. 9. 2011.

⁵ ČENTĚŠ, J. Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. Bratislava: C. H. Beck. 2013. s. 92.

lekomunikačnej prevádzke na dátový nosič, ktorý umožní uchovanie komunikácie a reprodukciu zachytenej komunikácie v budúcnosti, a jednak to, čo nosič obsahuje.⁶

2. Zákonné podmienky vydania príkazu na odpočúvanie a záznam telekomunikačnej prevádzky

Príkaz je jednou z foriem rozhodovacej právomoci súdu alebo orgánov činných v trestnom konaní. Podľa § 162 odsek 1 Trestného poriadku „súd rozhoduje rozsudkom, trestným rozkazom alebo príkazom, kde to zákon výslovne ustanovuje; v ostatných prípadoch rozhoduje, ak zákon neustanovuje niečo iné alebo ak rozhodnutie nemá technicko-organizačnú alebo operatívnu povahu, uznesením. Orgány činné v trestnom konaní rozhodujú, ak zákon neustanovuje niečo iné alebo ak rozhodnutie nemá technicko-organizačnú alebo operatívnu povahu, uznesením. Príkazom rozhodujú, kde to zákon výslovne ustanovuje (§ 162 odsek 2 Trestného poriadku).“

Trestný poriadok v § 181 ustanovuje náležitosti príkazu a to:

- a) označenie orgánu, o ktorého rozhodnutie ide,
- b) dátum a miesto rozhodnutia,
- c) výrok príkazu s uvedením zákonných ustanovení, ktoré boli použité,
- d) skutok s uvedením právnej kvalifikácie trestného činu, ak z povahy veci nevyplýva niečo iné,
- e) písomné vyhotovenie príkazu musí obsahovať odôvodnenie vtedy, kde to zákon výslovne ustanovuje,

Jedná sa o všeobecné podmienky, pričom proti príkazu opravný prostriedok nie je prípustný. Z toho hľadiska je teda ihneď po vydaní právoplatný a vykonateľný.

Podľa Záhoru⁷ príkazy, ktoré sa používajú v trestnom konaní, by sa dali zoradiť do troch základných skupín:

1. príkazy, realizáciou ktorých sa zasahuje najmä do osobnej slobody, domovej slobody a súkromia osoby,
2. príkazy, realizáciou ktorých sa zasahuje do vlastníckeho práva,
3. príkazy, ktorými sa nariaďuje použitie informačno-technologických prostriedkov a prostriedkov operatívno-pátracej činnosti.

Príkaz na odpočúvanie a záznam telekomunikačnej prevádzky podľa § 115 Trestného poriadku Záhora zaraďuje do tretej skupiny. Realizáciou týchto úkonov sa tiež zasahuje do súkromia osoby a tieto inštitúty by mohli byť zaradené aj do prvej skupiny. Do tejto skupiny ich zaraďujeme pre ich špecifický charakter a osobitný režim ich vykonávania. Tieto úkony sa vykonávajú utajene a v záujme naplnenia ich účelu sa vyžaduje, aby dotknutá osoba o ich realizácii nevedela.⁸

Zákonné podmienky na vydanie príkazu na odpočúvanie a záznam telekomunikačnej prevádzky upravuje ustanovenie § 115 odsek 1 Trestného poriadku nasledovne: „v trestnom konaní o zločine, korupcii, trestných činoch extrémizmu, trestnom čine zneužívania právomoci verejného činiteľa, trestnom čine legalizácie príjmu z trestnej činnosti alebo pre iný úmyselný trestný čin, o ktorom na konanie zaväzuje medzinárodná zmluva, možno vydať príkaz na odpočúvanie

⁶ NOVOTNÁ, J. K některým otázkám dokazování odposlechem a záznamem telekomunikačního provozu. In *Trestněprávní revue*. 2003. č. 10. s. 291.

⁷ ZÁHORA, J. Príkaz v trestnom konaní. In *Justičná revue*. 2004. roč. 56, č. 5. s. 539.

⁸ IVOR, J. a kolektív. *Trestné právo procesné, druhé doplnené a prepracované vydanie*. Bratislava. IURA EDITION. 2010. s. 538.

a záznam telekomunikačnej prevádzky, ak možno dôvodne predpokladať, že budú zistené skutočnosti významné pre trestné konanie.“

Analýzou predmetného ustanovenia dospejeme ku kumulatívnym podmienkam, ktoré zákonodarca predpokladá a stanovuje pre vydanie príkazu na odpočúvanie a záznam telekomunikačnej činnosti a to:

1. existencia trestného konania,
2. existencia taxatívne určeného trestného činu,
3. dôvodný predpoklad zistenia skutočností významných pre trestné konanie.⁹
4. nemožnosť dosiahnuť sledovaný účel inak alebo ak by bolo jeho dosiahnutie iným spôsobom podstatne sťažené.

Zákonodarca v ustanovení § 115 odsek 5 Trestného poriadku zakotvil výnimku z odseku 1 a to splnením nasledovných kumulatívnych podmienok:

1. existencia trestného konania,
2. existencia úmyselného trestného činu,
3. dôvodný predpoklad zistenia skutočností významných pre trestné konanie,
4. súhlas užívateľa odpočúvaného alebo zaznamenávaného telekomunikačného zariadenia.

Podľa Čentéša možno považovať za citlivé najmä odpočúvanie pred začatím trestného stíhania (§ 196–198 Trestného poriadku). Dávame do pozornosti, že trestné konanie v zmysle § 10 odsek 15 Trestného poriadku je „konanie podľa tohto zákona, trestné stíhanie úsek od začatia trestného stíhania až do právoplatnosti rozsudku, prípadne iného rozhodnutia orgánu činného v trestnom konaní alebo súdu vo veci samej a prípravným konaním sa rozumie úsek od začatia trestného stíhania do podania obžaloby, návrhu na schválenie dohody o uznaní viny a prijatí trestu (ďalej len „dohoda o vine a treste“) alebo právoplatnosti rozhodnutia orgánu činného v trestnom konaní vo veci samej.“ Otáznikom je preto v tomto prípade (pred začatím trestného stíhania) formálna existencia skutku, ktorý naplňa znaky niektorého z trestných činov uvedených v § 115 odsek 1 Trestného poriadku. S prihliadnutím na zákonné podmienky tohto inštitútu možno dôvodne predpokladať, že v rámci tohto štádia trestného konania sa spravidla vyžaduje podanie trestného oznámenia a existencia informácií, z ktorých vyplýva podozrenie zo spáchania trestného činu uvedeného v § 115 odsek 1 Trestného poriadku. Len trestné oznámenie samo osebe, ak nie je doložené aspoň indíciami, z ktorých možno dôvodné podozrenie vyvodzovať, a ktoré sa opiera len o špekulatívnu úvahu, nestačí na nariadenie odpočúvania.¹⁰

Dokazovanie pred začatím trestného konania je špecifické v tom, že nie je možno vykonať dôkazy typické pre prípravné konanie. Podľa Javorského sa všeobecne uznáva, že pri skúmaní dôvodov pre rozhodnutie o trestnom oznámení možno zohľadniť aj skutočnosti vyplývajúce z listín, na ktoré by vo vyšetrovaní, alebo v skrátenom vyšetrovaní nebolo možné prihliadnuť. Formou ako sa informácie o podozrení z trestnej činnosti dostanú do sféry poznania orgánov činných v trestnom konaní zákon neupravuje, preto z pohľadu zákonnosti takto získaného poznatku, zásadne nemôže nastať nepoužiteľnosť dôkazu prameniaceho z takýchto informácií.¹¹

Už pri podávaní návrhu na vydanie príkazu na odpočúvanie a záznam telekomunikačnej prevádzky musia byť zákonom predpokladané podmienky splnené. Vydanie príkazu na odpočúvanie má totiž v praxi dva následky. Jednak ten, že je možné uskutočňovať hoc aj vo vymedzenom rozsahu odpočúvanie telefonických hovorov a jednak, že sa na základe príkazu získavajú dôkazy, ktoré sú potom v trestnom konaní použité na preukázanie rozhodujúcich skutočností rieše-

⁹ Bližšie pozri tiež ČENTĚŠ, J. a kol. Trestný poriadok. Žilina: Eurokódex – Poradca podnikateľa. 2006. s. 2015.

¹⁰ Bližšie pozri II. ÚS ČR 789/06.

¹¹ Bližšie pozri JAVORSKÝ, V. Zákonnosť procesu dokazovania pred začatím trestného stíhania. dostupné na http://www.ucps.sk/ZAKONNOST_PROCESU_DOKAZOVANIA_PRED_ZACATIM_TRESTNEHO_STIHANIA_.

ných v rámci trestného konania. Osoba, ktorej telefonický rozhovor bol odpočúvaný, musí mať možnosť obrany jednak voči samotnému faktu odpočúvania jeho rozhovoru, teda voči samotnému faktu zásahu do jeho práva na súkromie, ale aj proti použitiu odpočúvanej komunikácie ako dôkazu v trestnom konaní. Preskúmateľnosť dôvodnosti vydania príkazu na odpočúvanie si vyžaduje relevantnú konkrétnu vysvetľujúcu argumentáciu, akými skutočnosťami boli naplnené zákonom stanovené podmienky pre tento zásah do práva na súkromie. Bez takéhoto odôvodnenia opierajúceho sa o konkrétne skutočnosti je príkaz spravidla nepreskúmateľný. Námetka, že vzhľadom na utajený charakter odpočúvania by bolo kontraproduktívne uvádzať v odôvodnení konkrétne skutočnosti odôvodňujúce vydanie príkazu, lebo tieto by mohli zmariť účel, pre ktorý bol vydaný neobstoí, pretože práve vzhľadom na utajený charakter odpočúvania nič nebráni tomu, aby dôvody, ktoré viedli súd k vydaniu príkazu, boli konkrétne uvedené. Pri dodržaní režimu utajenia sa dotknuté osoby môžu o vydaní príkazu a o dôvodoch, ktoré k tomu viedli, dozvedieť len dodatočne, teda iba po realizácii odpočúvania.¹²

Ďalšou podmienkou na vydanie príkazu je existencia taxatívne vymedzeného trestného činu (zločin, korupcia, trestné činy extrémizmu, trestný čin zneužívania právomoci verejného činiteľa, trestný čin legalizácie príjmu z trestnej činnosti) alebo iný úmyselný trestný čin, o ktorom na konanie zaväzuje medzinárodná zmluva. Podľa Čentéša „iný úmyselný trestný čin, o ktorom na konanie zaväzuje medzinárodná zmluva“ nemožno vykladať tak, že ide len o trestné činy, na stíhanie ktorých zaväzuje priamo či bezprostredne medzinárodná zmluva, pretože v takom prípade by bol ich okruh veľmi obmedzený (napríklad genocídium), ale nepochybne ide o všetky trestné činy, ktoré majú podklad alebo nadväzujú na medzinárodné zmluvy, ktoré obsahujú záväzok pre štáty, ako ich zmluvné strany majú stíhať alebo postihovať, aj keď sa konkrétny vnútroštátny postih zásadne vykonáva podľa skutkových podstatí trestných činov, ktoré sú súčasťou vnútroštátneho právneho poriadku.¹³

Preto je dôležité skúmať, i keď ide o určitý všeobecný trestný čin, či na stíhanie nezaväzuje medzinárodná zmluva (napríklad Dohovor o právach dieťaťa, Dohovor Rady Európy číslo 141 o praní, vyhľadávaní, zbavovaní a konfiškácii výnosov z trestnej činnosti, Parížsky dohovor na ochranu priemyselného vlastníctva, Dohovor o medzinárodnom obchode s ohrozenými druhmi voľne žijúcich živočíchov a rastlín – CITES, a podobne). Keďže plynutím času dochádza k pridávaniu týchto trestných činov, v závislosti na uzatváraní a ratifikácii zmlúv, na ktorých Slovenská republika participuje, je potrebné vždy už pri podávaní návrhu na vydanie príkazu na záznam a odpočúvanie telekomunikačnej činnosti uvedené skúmať. Obdobne tak musí postupovať súd pri samotnom vydaní príkazu.

S vyššie uvedenými podmienkami na vydanie príkazu je úzko spätá i materiálna podmienka odpočúvania definovaná v ustanovení § 119 odsek 1 Trestného poriadku. Dôležité je preto skúmanie dôvodného predpokladu, že odpočúvaním telekomunikačnej prevádzky budú zistené skutočnosti významné pre trestné konanie, ktorými sú dokazované skutočnosti, či sa stal skutok a či má znaky trestného činu, kto tento skutok spáchal a za akých pohnútok a taktiež závažnosť činu a podmienok jeho spáchania.

Za každých okolností je potrebné, aby príslušné orgány skúmali nielen legalitu, legitimitu, proporcionalitu ale taktiež verejný záujem, rešpektujúc pritom základné práva a slobody jednotlivcov. Podľa Růžičku orgány činné v trestnom konaní (a súd) v okamihu nariadenia odpočúvania nemajú a ani nemôžu mať istotu, že skutočnosti dôležité pre trestné konanie, budú v bu-

¹² Bližšie pozri Uznesenie Najvyššieho súdu Slovenskej republiky spisová značka 1 To 4/2010.

¹³ ČENTÉŠ, J. Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. Bratislava: C. H. Beck. 2013. s. 100.

dúčnosti telekomunikačnou cestou zistené a oznámené. Pracujú len s predpokladom, ktorého dôvodnosť musí byť podložená doterajšími poznatkami.¹⁴

Dôvodnosť predpokladu o zistení skutočností významných pre trestné konanie je podstatná i pri preskúvaní zákonnosti a ústavnosti vydaného príkazu na odpočúvanie a záznam telekomunikačnej prevádzky zo strany osoby, ktorá sa domáha porušenia svojich práv.

Príkaz na odpočúvanie a záznam telekomunikačnej prevádzky vydáva predseda senátu a pred začatím trestného stíhania alebo v prípravnom konaní sudca pre prípravné konanie na návrh prokurátora. Zákon dáva možnosť výnimky z vyššie uvedeného a to na podklade existencie kumulatívnych podmienok a to, že existuje vec, ktorá neznesie odklad a príkaz sudcu pre prípravné konanie nemožno získať vopred. Vtedy je oprávnený na vydanie príkazu prokurátor, avšak taktiež len za predpokladu, že odpočúvanie a záznam telekomunikačnej prevádzky nie je spojené so vstupom do obydľia. Takýto krok však musí následne „odobriť“ v lehote najneskôr 24 hodín sudca pre prípravné konanie, inak takýto príkaz stráca platnosť a informácie takto získané nemožno použiť na účely trestného konania a musia sa predpísaným spôsobom bez meškania zničiť. Taktiež nemôže ísť o prípad podľa § 115 odsek 5 Trestného poriadku. Príkaz prokurátora ma teda predbežný charakter, pretože jeho platnosť je časovo obmedzená.

Na podklade uvedeného je potrebné opätovne zdôrazniť, že návrh prokurátora je jedným z predpokladov na vydanie príkazu a teda i tento musí spĺňať zákonom stanovené podmienky. Tieto sú ustanovené v § 115 odsek 3 Trestného poriadku nasledovne: „príkaz na odpočúvanie a záznam telekomunikačnej prevádzky musí vydať písomne a odôvodniť aj skutkovými okolnosťami, a to osobitne na každú účastnícku stanicu alebo zariadenie. V príkaze musí byť určená účastnícka stanica alebo zariadenie a osoba, ak je známa, ktorej sa odpočúvanie a záznam telekomunikačnej prevádzky týka, a čas, po ktorý sa bude odpočúvanie a záznam telekomunikačnej prevádzky vykonávať.“

Možno teda vysloviť, že bez takéhoto návrhu sudca pre prípravné konanie uvedené príkazy nie je oprávnený vydať. Súd preto i pri vyhodnocovaní použiteľnosti dôkazov musí skúmať i návrhy prokurátora na vydanie príkazu na záznam a odpočúvanie telekomunikačnej činnosti a v konaní pred súdom tieto oboznámiť na hlavnom pojednávaní a až po takto vykonanom dokazovaní následne hodnotiť ich zákonnosť a obsah.¹⁵

Čas odpočúvania a záznamu môže trvať najviac šesť mesiacov, pričom sudca pre prípravné konanie môže v prípravnom konaní na návrh prokurátora odpočúvanie predĺžiť vždy o ďalšie dva mesiace, a to aj opakovane. Počas tejto doby však policajt či príslušný útvar Policajného zboru sústavne skúma trvanie dôvodov, ktoré viedli k vydaniu príkazu. Ak tieto pominuli, musí byť bezodkladne odpočúvanie a záznam telekomunikačnej prevádzky skončené a to aj v prípade, že ešte neuplynula doba, na ktorú bol príkaz vydaný. O ukončení sa bez meškania písomne upovedomí ten, kto príkaz vydal a v prípravnom konaní aj prokurátor.

Nevyhnutnou náležitosťou príkazu na odpočúvanie a záznam telekomunikačnej prevádzky je určenie účastníckej stanice alebo zariadenia, a to osobitne pre každú stanicu alebo zariadenie. Spravidla ide o telefónne spojenie prostredníctvom pevnej siete alebo mobilné telefónne spojenie, fax, rádiostanicu a podobne. Ďalej o údaje prináležiace k účastníckej stanici alebo zariadeniu ako telefónne číslo, meno a adresa trvalého pobytu účastníka, obchodné meno, sídlo alebo miesto podnikania účastníka alebo registrovaného užívateľa, technické číslo (PUK, IMEI). Príkaz by mal byť individualizovaný vo vzťahu k osobe majiteľa, respektíve užívateľa účastníckej stanice alebo zariadenia. Musí byť z neho zrejmé, kto takéto zariadenie užíva alebo užíval

¹⁴ RŮŽIČKA, M. Odposlech a záznam telekomunikačního provozu v analytických materiálech státního zastupitelství. In Státní zastupitelství. 2008. číslo 3 s. 11.

¹⁵ Bližšie pozri Uznesenie Najvyššieho súdu Slovenskej republiky spisovej značky 4 To 3/2012.

a teda s tým súvisiaca pravdepodobnosť, že takéto zariadenie bude užívať i v budúcnosti. Vzhľadom na zákonodarcom predpokladanú skutočnosť, že predmetom odpočúvania môže byť aj neznáma osoba, je na podklade preverených skutočností potrebné túto bližšie špecifikovať. Ak ide o účastnícku stanicu evidovanú na inú osobu, nepostačuje formulka „operatívno-pátracou činnosťou bolo zistené, že účastnícku stanicu používa záujmová osoba...“, pretože je potrebné uviesť akou konkrétnou operatívno-pátracou činnosťou, kým a ako boli zistené uvedené skutočnosti. Jedná sa najmä o fiktívny telefonát, skutočnosti zistené legálnym spôsobom z iného odposluchu, a podobne. Obdobne v prípade účastníckej stanice vedenej na obchodnú spoločnosť je potrebné zistiť a uviesť vzťah záujmovej osôb k tejto spoločnosti, napríklad spoločník, konateľ, člen predstavenstva atď. V prípade účastníckej stanice, u ktorej nie je zrejmé, kto je majiteľom, je taktiež potrebné uviesť konkrétnu skutočnosť, ako bolo zistené, že číslo používa záujmová osoba.

Osobitnú pozornosť treba venovať i primeranému odôvodneniu vydaného príkazu. V praxi sa často stáva, že odôvodnenia obsiahnuté v príkazoch, ktoré sú súčasťou utajovanej prílohy spisu predloženého na rozhodnutie možno považovať len za formálne. Bez náležitého odôvodnenia opierajúceho sa o konkrétne skutočnosti je daný príkaz nepreskúmateľný, a tým aj arbitrárny (svojvoľný). K ďalším nedostatkom patrí absencia konkrétnych skutočností uvedených v odôvodnení, ktoré viedli k vydaniu príkazu. Taktiež v príkazoch, ktorými bola predlžovaná doba na odpočúvanie, keď už mohli byť známe aj konkrétne skutočnosti odôvodňujúce fakt, že sa má v odpočúvaní pokračovať, nie sú uvedené žiadne konkrétne skutočnosti, iba sa formálne konštatuje, že boli splnené všetky zákonom požadované podmienky pre predĺženie doby odpočúvania. Pritom stačí, ak odôvodnenie dá odpoveď na otázky, ktoré majú pre vec podstatný význam a dostatočne objasňuje skutkový a právny základ rozhodnutia.¹⁶

Ustanovenia odsekov 1 až 10 Trestného poriadku sa rovnako vzťahujú na údaje, ktoré sú v reálnom čase prenášané prostredníctvom počítačového systému.

3. Záznam telekomunikačnej prevádzky ako dôkaz v trestnom konaní

Ako sme už vyššie spomenuli, osobitne sa dbá na to, aby zásah do práva jednotlivca zo strany štátu bol primeraný a zákonný. Odpočúvanie a záznam telekomunikačnej prevádzky robí príslušný útvar Policajného zboru v režime utajenia.

V zmysle § 2 písmeno a) zákona číslo 215/2004 Z. z. o ochrane utajovaných skutočností i o zmene a doplnení niektorých zákonov v znení neskorších právnych predpisov utajovanou skutočnosťou „je informácia alebo vec určená pôvodcom utajovanej skutočnosti, ktorú vzhľadom na záujem Slovenskej republiky treba chrániť pred vyzradením, zneužitím, poškodením, neoprávneným rozmnožením, zničením, stratou alebo odcudzením (ďalej len „neoprávnená manipulácia“) a ktorá môže vznikať len v oblastiach, ktoré ustanoví vláda Slovenskej republiky svojím nariadením.“

Predpokladom použitia záznamu telekomunikačnej prevádzky ako dôkazu je:

1. doslovný prepis záznamu, ak to vyhotovený záznam umožňuje,
2. skončenie odpočúvania a záznamu telekomunikačnej prevádzky, a
3. zistenie skutočností dôležitých pre trestné konanie.

Podľa § 115 odsek 1 Trestného poriadku ak sa pri odpočúvaní a zaznamenávaní telekomunikačnej prevádzky zistí, že obvinený komunikuje so svojím obhajcom, takto získané informácie nemožno použiť na účely trestného konania a musia sa predpísaným spôsobom bez meškania

¹⁶ Rozhodnutie Ústavného súdu Slovenskej republiky I. ÚS 241/07.

zničiť; to neplatí, ak ide o informácie, ktoré sa vzťahujú na vec, v ktorej advokát nezastupuje obvineného ako obhajcu. Uvedené vyplýva zo špecifického vzťahu medzi obhajcom a obvineným založenom na vzájomnej dôvere. Dôvod je zrejмый. Pokiaľ by sa dohodnutá taktika obhajoby stala známou tretiemu subjektu (najmä orgánu činnému v trestnom konaní), išlo by o zásadný zásah do práv obvineného, najmä práva na obhajobu.¹⁷

Ak sa majú informácie zistené na základe príkazu použiť ako dôkaz, k záznamu sa musí v prípade, ak to vyhotovený záznam umožňuje, pripojiť doslovný prepis záznamu. Táto úloha pripadá príslušníkovi Policajného zboru vykonávajúcemu odpočúvanie a to v rozsahu zistených skutočností významných pre trestné konanie. Taxatívnymi náležitosťami sú ďalej údaje o mieste, čase, orgáne, ktorý záznam vykonal a zákonitosti odpočúvania. Záznam na elektronickom nosiči je súčasťou spisového materiálu. Prepis sa spravidla neutajuje, ak však obsahuje utajovanú skutočnosť, utajuje sa v zmysle zákona o utajovaných skutočnostiach.

V prípravnom konaní možno v prípade potreby predložiť súdu iba záznam telekomunikačnej prevádzky aj bez prepisu tohto záznamu pri splnení týchto podmienok:

- odôvodňujú to okolnosti prípadu, a zo sprievodnej správy vyplývajú údaje o mieste, čase a zákonnosti tohto úkonu a o osobách, ktorých sa záznam týka, a
- záznam je zrozumiteľný.

Keďže hodnovernosť prepisu posudzuje súd, je potrebné klásť zvýšené nároky na osobu príslušníka Policajného zboru. Ten musí nielen označiť tie rozhovory či ich pasáže, ktoré môžu byť významné ako dôkaz pre trestné konanie, ale je taktiež zodpovedný za to, že v súlade s ustanovením § 2 odsek 10 Trestného poriadku vyhodnotí rozhodujúce skutočnosti významné pre posúdenie trestnej činnosti konkrétnej osoby. Zabezpečuje, aby nedošlo k možnému skresľovaniu obsahu rozhovoru vytrhnutím rozhovoru z kontextu a teda zabezpečí spravidla celý rozhovor medzi účastníkmi telekomunikačnej prevádzky.¹⁸

Ústavný súd Českej republiky ako *obiter dictum* zaujal stanovisko, že štát musí preukázať, v prípade podozrenia manipulácie pri odpočúvaní, že k tomuto nedošlo. Podľa Ústavného súdu Českej republiky pritom nie je možné vylúčiť, že v priebehu trestného konania k určitej manipulácii s nahrávkami došlo, napríklad „ustrihnutím“ začiatku a konca rozhovorov osôb, ktoré sú predmetom záujmu. Je však úlohou obžaloby dokázať, že systém vyhotovenia odpočúvania neoprávnenú manipuláciu vylučuje alebo aspoň manipulovanie s nahrávkou eviduje. Pokiaľ toto nie je schopná, nemožno z toho vyvodiť záver, že sú nahrávky ako celok nepoužiteľné, je však potrebné sporné časti hodnotiť s prihliadnutím na zásadu *in dubio pro reo*.¹⁹

Ak je zaznamenaná komunikácia v cudzom jazyku, podmienkou použitia záznamu telekomunikačnej prevádzky v zmysle § 115 odsek 6 Trestného poriadku ako dôkazu je jeho doslovný prepis v cudzom jazyku, preložený do slovenského jazyka, ak to vyhotovený záznam umožňuje a pretlmočenie celého obsahu alebo príslušnej časti obsahu záznamu preloženého do slovenského jazyka (§ 28 Trestného poriadku) a jeho prepis do textovej podoby.²⁰

Najvyššie štátne zastupiteľstvo Českej republiky vydalo 13. 5. 2014 zjednocujúce stanovisko spisovej značky SL 750/2001 k použiteľnosti magnetofónového záznamu vyhotoveného súkromnou osobou utajeným spôsobom v trestnom konaní. V zásade je podľa neho neprípustné, aby súkromná osoba nahrávala utajeným spôsobom hlasový prejav iného s cieľom použiť ho ako dôkaz v trestnom či inom konaní. Pokiaľ má byť takto získaná informácia použitá ako dôkaz v trestnom konaní, musí byť tento postup odôvodnený zvláštnymi okolnosťami prípadu, kto-

¹⁷ JELÍNEK, J., UHLÍŘOVÁ, M.: Obhájce v trestním řízení. 1. vydání. Praha: Leges. 2011. s. 258.

¹⁸ Komentár k KO301_2005SK. Systém ASPI – stav k 13. 3. 2017 do čiastky 27/2017 z. z.

¹⁹ Pozri tiež Nález Ústavného súdu Českej republiky spisovej značky III. ÚS 2847/14.

²⁰ R 97/2014. Komentár k KO301_2005SK. ASPI – stav k 13. 3. 2017 do čiastky 27/2017.

ré odôvodňujú dôvodnosť porušenia práva na súkromie iného. Obdobne sám záujem získať informácie použiteľné v akoľvek konaní vrátane trestného nie je dostatočným záujmom odôvodňujúcim porušenia práva na súkromie. Absolútny zákaz použitia takto získaných informácií však neplatí a platiť ani nemôže. Tak ako v oblasti ochrany základných práv a slobôd pred neoprávnenými zásahmi orgánov verejnej moci, i tu platia výnimky, ktoré môžu takéto zásahy za určitých okolností odôvodniť. I v súkromnej sfére musí platiť, že existujú okolnosti, za ktorých je tento zásah dovolený, prípadne za ktorých je výsledok tohto (i nedovoleného) zásahu dovoľné využiť ako dôkaz.

Podľa § 115 odsek 7 Trestného poriadku v inej trestnej veci, ako je tá, v ktorej sa vykonávalo odpočúvanie a záznam telekomunikačnej činnosti, je možné záznam použiť len vtedy, ak sa súčasne aj v tejto veci vedie trestné konanie pre trestný čin uvedený v odseku 1 Trestného poriadku. Nielen medzi právnymi teoretikmi ale i medzi jednotlivými súdmi panuje názorový nesúlad ohľadne výkladu predmetného ustanovenia. Sporným je najmä slovo „súčasne“, ktoré sa vykladá rôznymi spôsobmi. Jedná sa najmä o posúdenie a príklon k vecnej či časovej súvislosti. Najvyšší súd Slovenskej republiky (ďalej len „Najvyšší súd“) v Uznesení z 21. 9. 2011 zaujal stanovisko, že slovo „súčasne“ je potrebné, na základe logického a gramatického výkladu, vzťahovať na okamih vyhotoveného záznamu pred orgánmi činnými v trestnom konaní a pred súdmi, a nie na okamih kedy sa odposluch vykonáva. Sporné ustanovenie upravuje iba použitie už existujúceho záznamu o telekomunikačnej prevádzke nie jeho vyhotovenie. Slovo „súčasne“ je preto potrebné v kontexte chápať tak, že súčasne v čase použitia záznamu musí byť vedené trestné konanie.²¹ Najvyšší súd v inej trestnej veci taktiež uviedol, že opačný výklad by bol v rozpore s argumentom *reductio ad absurdum*, keďže by viedol k záveru, ktorý nemá rozumný zmysel a v podstate by znamenal vylúčenie použitia tohto ustanovenia na rozhodujúcu väčšinu prípadov v praxi a znamenal by faktickú nemožnosť použitia predmetného ustanovenia.²² Naproti tomu v inej trestnej veci vyslovil opačný názor, pričom poukázal na časovú súvislosť.²³

Ivor prezentuje tri základné argumenty podporujúce záver o tzv. vecnej súvislosti:

1. ustanovenie § 115 odsek 7 Trestného poriadku treba rozdeliť na dve základné fázy upravennej činnosti. V prvej ide na základe logického a gramatického výkladu o vykonanie odpočúvania a vyhotovenie záznamu telekomunikačnej prevádzky, v druhej o použitie záznamu. Zákonodarcu mal jednoznačne úmysel slovo „súčasne“ vzťahovať na okamih použitia záznamu a nie jeho vyhotovenia,
2. zákon o ochrane pred odpočúvaním pripúšťa použiť informáciu získanú legálne a legitímne vedeným odpočúvaním ako dôkaz v trestnom konaní, pričom obdobne, ako je to v situácii podľa § 115 odsek 7 Trestného poriadku, ide o informáciu, pri ktorej v dobe získania ešte vôbec nebolo vedené trestné konanie, respektíve bola získaná mimo trestného konania,
3. obdobná úprava je aj v ustanovení § 88 odsek 6 českého Trestného poriadku, avšak bez slova „súčasne“.²⁴

Naproti tomu Perhács a Zajonc vyslovili názor, že slovo „súčasne“ sa vzťahuje len na také prípady, kedy sa už minimálne v dvoch veciach vedie trestné konanie a záznam ako dôkaz, ktorý sa má použiť v druhej (inej) veci, by bol zaznamenaný až potom, kedy by sa v inej veci viedlo mi-

²¹ <http://www.pravnelisty.sk/rozhodnutia/a128-k-moznostiam-pouzitia-zaznamu-telekomunikacnej-prevadzky-v-inej-trestnej-veci>.

²² Uznesenie Najvyššieho súdu Slovenskej republiky spisovej značky 1 To 4/2010.

²³ Bližšie pozri Rozsudok Najvyššieho súdu Slovenskej republiky spisovej značky 2 To 5/2010.

²⁴ IVOR, J. Využitie záznamu z odpočúvania ako dôkazu v trestnom konaní. In: Zborník príspevkov z medzinárodnej konferencie „Československé právnické dni“, 2. ročník. Omšenie. s. 209.

nimálne trestné konanie. Inými slovami, použiteľnosť záznamov by bola podmienená reálnou existenciou trestného konania v inej veci.²⁵

Stotožňujeme sa s názorom, že pri aplikácii sporného ustanovenia je potrebné prihliadnuť na vecnú súvislosť. Pričom v záujme právnej istoty by bolo žiaduce *de lege ferenda* vypustiť sporné slovo „súčasne“ z § 115 odsek 7 Trestného poriadku.

Opačným problémom sú dôkazy, z ktorých súd pri svojom rozhodovaní vychádzal, i keď nemal. Hanuš ich vymedzuje takto: „druhá kategória ústavnoprávne relevantných vád procesu dokazovania potom zahŕňa prípady vykazujúce také ústavne nesúladne deficity, keď dôkaz (informácia v ňom obsiahnutá) nie je získaný čo do jednotlivých fáz procesu dokazovania procesne prípustným spôsobom. Vychádza z toho, že proces dokazovania nie je možné chápať ako jednorázový akt, ale ako proces čiastkových skutkov, ktorého výsledkom v ich vzájomnej spojitosti a návaznosti je to, že súd dospeje k poznatku, ktorý je predmetom dokazovania. Z relevantnej vady či viacerých relevantných vád tohto procesu vyplýva, že takto získaný poznatok mal byť súdom pri vyvodení skutkových záverov vylúčený z predmetu úvah smerujúcich k ustáleniu (zisteniu) skutkového základu veci.“²⁶

4. Zničenie záznamu telekomunikačnej prevádzky

Ak sa pri odpočúvaní a zázname telekomunikačnej prevádzky nezistili skutočnosti významné pre trestné konanie, orgán činný v trestnom konaní alebo príslušný útvar Policajného zboru musí získaný záznam predpísaným spôsobom bezodkladne zničiť. O zničení záznamu sa spíše zápisnica, ktorá tvorí súčasť spisového materiálu. Je súčasťou originálu ako aj rovnopisu vyšetrovacieho spisu, a osoba, ktorá nemá možnosť nazerať do spisu, sa musí dodatočne oboznámiť, že jej telefonické hovory boli odpočúvané.²⁷

Podľa § 115 odsek 9 Trestného poriadku o zničení záznamu informuje osobu uvedenú v odseku 3, ak je známa, policajt alebo prokurátor, ktorého rozhodnutím sa vec právoplatne skončila, a v konaní pred súdom predseda senátu súdu prvého stupňa po právoplatnom skončení veci. Informácia obsahuje označenie súdu, ktorý vydal alebo potvrdil príkaz na odpočúvanie a záznam telekomunikačnej prevádzky, dĺžku odpočúvania a dátum jeho ukončenia. Súčasťou informácie je poučenie o práve podať v lehote dvoch mesiacov od jej doručenia návrh na preskúmanie zákonnosti príkazu na odpočúvanie a záznam telekomunikačnej prevádzky Najvyššiemu súdu. Informáciu podá orgán, ktorého rozhodnutím sa vec právoplatne skončila, a v konaní pred súdom predseda senátu súdu prvého stupňa do troch rokov od právoplatného skončenia trestného stíhania v danej veci.

Výnimkou z vyššie uvedeného je skutočnosť, ak ide o osobu, ktorá má možnosť nazerať do spisu podľa tohto zákona, alebo v konaní o obzvlášť závažnom zločine alebo zločine spáchanom organizovanou skupinou, zločineckou skupinou alebo teroristickou skupinou, alebo ak sa na trestnom čine podieľalo viac osôb a vo vzťahu aspoň k jednému z nich bolo trestné stíhanie právoplatne skončené, alebo ak by poskytnutím takej informácie mohol byť zmarený účel trestného konania.

²⁵ PERHÁCS, Z., ZAJONC, A. Poznámky k sledovaniu, priestorovému a telefonickému odposluchu. In Justičná revue. 2011. č. 8–9. s. 1140.

²⁶ HANUŠ, L.: Ústavnoprávny vady dôkazného procesu z pohľadu judikatury Ústavného soudu. In: Právní rozhledy. 2006. číslo 18. s. 650.

²⁷ PERHÁCS, Z.: O zničení záznamov získaných použitím informačno-technických prostriedkov. In: Justičná revue. 2007. číslo 5. s. 642.

5. Preskúmanie zákonnosti príkazu na odpočúvanie a záznam telekomunikačnej prevádzky

Ako vyplýva z medzinárodných dohovorov, ale najmä z judikatúry Európskeho súdu pre ľudské práva, vždy keď je to možno a neodporuje to zmyslu tajného odpočúvania, musí byť osoba dodatočne oboznámená s tým, že jej hovory boli odpočúvané, a musí mať k dispozícii účinný opravný prostriedok, ktorým môže namietat nezákonnosť alebo bezdôvodnosť odpočúvania (napríklad *Case of Segerstedt-Wiberg and Others v. Sweden*, 2006).²⁸

Ak chce štátny orgán alebo iný orgán verejnej moci vyhodnotiť dôkaz získaný použitím informačno-technických prostriedkov – ako dôkaz získaný zákonným spôsobom v zmysle a inenciách judikatúry Európskych orgánov ochrany práva, Ústavného súdu a Najvyššieho súdu – musí primárne skúmať štyri kumulatívne a zákonom striktne stanovené podmienky:

- 1) či podaný návrh spĺňa náležitosti stanovené Trestným poriadkom alebo zákonom o ochrane pred odpočúvaním (odôvodnenie, preskúmateľnosť, konkrétne zadefinovanie objektu používania informačno-technických prostriedkov),
- 2) či príkaz alebo súhlas na použitie informačno-technických prostriedkov je riadne odôvodnený, obsahuje všetky náležitosti a bol vydaný príslušným súdom a sudcom,
- 3) či použitie informačno-technických prostriedkov je riadne odôvodnené, obsahuje všetky stanovené náležitosti a bol vydaný príslušným súdom a sudcom,
- 4) či dôkaz získaný použitím informačno-technických prostriedkov je použiteľný v trestnom konaní z hľadiska kvality, obsahu a úplnosti.²⁹

Na to, aby mohol byť príkaz na odpočúvanie a záznam telekomunikačnej prevádzky vydaný účelu sledovanému zákonom, je potrebné, aby mu predchádzal taký návrh, ktorý svojím obsahom spĺňa náležitosti kladenému mu zákonom a bude obsahovať také konkrétne údaje o konkrétnom podozrení z konkrétnej trestnej činnosti so zadefinovaním konkrétneho objektu použitia ITP, že pri obstoí pri hodnotení súdu z hľadiska zákonnosti, ústavnosti, legality, legitimacy a proporcionality

Kto je oprávnený na vydanie príkazu na odpočúvanie a záznam telekomunikačnej činnosti je konkretizované v § 115 odsek 2 Trestného poriadku.

Sudcom pre prípravné konanie je v súlade s § 2 odsek 3 a § 10 odsek 3 Trestného poriadku sudca súdu prvého stupňa, rozvrhom práce poverený rozhodovať okrem iného o najzávažnejších procesných zásahoch do základných práv a slobôd pred začatím trestného stíhania a v prípravnom konaní. Pokiaľ ide o vydanie príkazu na odpočúvanie a záznam telekomunikačnej prevádzky v čase súdneho konania, predseda senátu (aj odvolacieho súdu), v súlade s § 2 odsek 11 prvá veta Trestného poriadku môže vykonať i dôkazy procesnými stranami nenavrhnuté.³⁰ Samozrejme nemožno opomenúť § 24 odsek 4 Trestného poriadku.

De lege ferenda by stálo za uváženie vypustenie oprávnenia prokurátora na vydanie príkazu na odpočúvanie a záznam telekomunikačnej prevádzky, najmä s poukazom na možné zneužitie tohto oprávnenia, respektíve doplnenie povinnosti informovať o takomto postupe v prípade, ak sa ešte pred uplynutím 24 hodinovej lehoty odpočúvanie ukončilo a príkaz prokurátora nebol potvrdený súdom.

²⁸ IVOR, J. a kolektív: Trestné právo procesné, druhé doplnené a prepracované vydanie. Bratislava. IURA EDITION. 2010. s. 406.

²⁹ PERHÁCS, Z., PERHÁCSOVÁ, A.: Právna úprava používania informačno-technických prostriedkov. 1. časť. In: Justičná revue. 2013. číslo 4. s. 542.

³⁰ KYJAC, Z.: Použitie informačno-technických prostriedkov v trestnom konaní, Odpočúvanie a záznam telekomunikačnej prevádzky, Bratislava, Wolters Kluwer. 2015, 144.

Na podklade vyššie uvedených skutočností môžeme vady odpočúvania a záznamu telekomunikačnej činnosti zhrnúť nasledovne:

- podaný návrh nespĺňa náležitosti stanovené Trestným poriadkom, resp. zákonom o ochrane pred odpočúvaním,
- vykonávanie odpočúvania bez príkazu oprávneného subjektu, respektíve vydané neoprávneným subjektom, respektíve bez potvrdenia vydaného príkazu príslušným orgánom,
- použitie odposluchu a záznamu nie v súlade s vydaným príkazom,
- vykonávanie odpočúvania za nedodržania materiálnych podmienok (absencia, respektíve iný trestný čin ako zákonom predpokladaný, absencia dôvodného predpokladu na zistenie skutočností významných pre trestné konanie, absencia odôvodnenia, písomného vyhotovenia, absencia náležitostí vyžadovaných zákonom atď.),
- odpočúvanie komunikácie medzi obvineným a obhajcom,
- odpočúvanie po uplynutí času uvedenému v príkaze, respektíve dlhšie ako ustanovuje zákon,
- bez súhlasu užívateľa odpočúvacieho zariadenia, respektíve po jeho odvolaní,
- technické problémy pri odposluchu, kvalita zvuku, neúplnosť alebo absencia rozhovoru, záznamu, prepisu,
- predkladané nekompletné spisové materiály,

Pri možnom predlžovaní vydaných príkazov sú tieto nedostatky:

- predpokladané nerelevantné podklady pre posúdenie dôvodnosti doposiaľ vykonaného odposluchu (absencia prepisu, len CD, resp. DVD, USB), nepreložený obsah hovoru,
- neskoré alebo naopak príliš skoré predkladané podnetov na vydanie návrhu na vydanie príkazu na odpočúvanie a záznam telekomunikačnej prevádzky a s tým súvisiaca nemožnosť riadne naštudovať súvisiaci spisový materiál,

V praxi sa taktiež stretáme s postupom, keď v prípade nevydania príkazu bez zmeny podmienok je podnet, respektíve návrh predkladaný inému službukonajúcemu prokurátorovi alebo sudcovi.

Príkaz na odpočúvanie a záznam telekomunikačnej prevádzky má povahu rozhodnutia sui generis (rozhodnutie svojho druhu), teda nejde o uznesenie. Z tohto dôvodu nie je proti nemu prípustný opravný prostriedok a dotknutá osoba nemá možnosť domáhať sa ochrany pred všeobecným súdom v súvislosti s faktom, že napríklad jej telefonický rozhovor bol odpočúvaný. Podľa názoru Ústavného súdu (I. ÚS 274/2005) oprávnenosť vydania právoplatného príkazu všeobecný súd nemôže preskúmať, a to práve preto, lebo príkaz je právoplatným rozhodnutím, ktorým je súd viazaný, resp. z ktorého musí vychádzať. Vztahuje sa to tak na trestné konanie, ako aj na prípadné občianskoprávne konanie na ochranu osobnosti (na ochranu súkromia). Príkaz na odpočúvanie a záznam telekomunikačnej prevádzky môže byť predmetom sťažnosti, o ktorej je oprávnený rozhodnúť Ústavný súd. Zároveň možno zdôrazniť, že odlišná situácia nastáva v prípade, ak záznam telekomunikačnej prevádzky sa má použiť ako dôkaz v trestnom konaní. V takomto prípade osoba, ktorej rozhovor bol odpočúvaný (spravidla obžalovaný), môže namietat zákonnosť tohto dôkazu a z toho vyplývajúcu jeho nepoužiteľnosť, avšak len pri súčasnom splnení dvoch podmienok, a to

- trestná vec musí dospieť do štádia súdneho konania,
- dotknutá osoba musí byť stranou v trestnom konaní (obžalovaný, poškodený).

Na základe uvedených skutočností Ústavný súd vyslovil názor, že ochrana zo strany trestného súdu vôbec neprichádza do úvahy v prípadoch, ktoré sa pred trestný súd vôbec nedostanú, ale ani v prípadoch takých dotknutých osôb, ktoré nie sú stranami v trestnom konaní.

Hoci ide o závažný zásah do základného práva, dotknuté osoby nemajú možnosť podať proti takému príkazu opravný prostriedok a o jeho vydaní sa dozvedia spravidla až dodatočne, keď už zásah do práva na súkromie bol realizovaný. Majú preto možnosť žiadať o jeho preskúmanie až dodatočne. Preskúmateľnosť dôvodnosti jeho vydania si vyžaduje relevantnú konkrétnu vysvetľujúcu argumentáciu, akými skutočnosťami boli naplnené zákonom ustanovené podmienky pre tento zásah do práva na súkromie. Bez takéhoto odôvodnenia opierajúceho sa o konkrétnu skutočnosť je daný príkaz spravidla nepreskúmateľný. Na prvý pohľad by sa mohlo zdať, že vzhľadom na utajený charakter odpočúvania by bolo neúnosné a kontraproduktívne uviesť v odôvodnení konkrétnu skutočnosť odôvodňujúce vydanie príkazu, lebo tieto by mohli jeho účel zmať. V skutočnosti je však opak pravdou. Práve vzhľadom na utajený charakter odpočúvania nič nebráni tomu, aby dôvody, ktoré viedli prokurátora k vydaniu príkazu, ktorým bolo nariadené odpočúvanie a záznam telekomunikačnej prevádzky podľa Trestného poriadku, boli konkrétne uvedené. Pri dodržaní režimu utajenia sa dotknuté osoby môžu o vydaní tohto rozhodnutia a o dôvodoch, ktoré k tomu viedli, dozvedieť len dodatočne (obdobne I. ÚS 274/05).³¹

S účinnosťou od 1. 1. 2016 (novelou zákona číslo 397/2015 Z. z.) sa do Trestného poriadku doplnila právna úprava, ktorá umožňuje osobe, ktorú príslušný orgán informuje o zničení záznamu podľa § 115 odsek 9 Trestného poriadku, podať návrh na preskúmanie zákonnosti príkazu na odpočúvanie a záznam telekomunikačnej prevádzky. Uvedené ustanovenie poskytuje širšiu ochranu súkromia zo strany orgánov verejnej moci.

Z povahy veci vyplýva, že nie je možné takýto návrh podať skôr, ako bola vec právoplatne skončená. Ak by teda napriek nesplneniu zákonných podmienok takýto návrh podaný bol, Najvyšší sud Slovenskej republiky (ďalej len „Najvyšší súd“) by nebol oprávnený začať konanie v zmysle § 362f Trestného poriadku.

Na návrh osoby uvedenej v § 115 odsek 9 Najvyšší súd na neverejnom zasadnutí preskúma zákonnosť príkazu na odpočúvanie a záznam telekomunikačnej prevádzky, pričom si pred rozhodnutím vyžiada stanovisko sudcu, ktorý rozhodol o vydaní alebo potvrdení príkazu podľa § 115 Trestného poriadku. Ak Najvyšší súd zistí, že príkaz na odpočúvanie a záznam telekomunikačnej prevádzky bol vydaný alebo vykonaný v rozpore so zákonom, vysloví uznesením porušenie zákona. Proti tomuto rozhodnutiu nie je prípustný opravný prostriedok. Z toho dôvodu sa v danom prípade neuplatňuje dvojinštancné konanie. Ak Najvyšší súd zistí, že príkaz na odpočúvanie a záznam telekomunikačnej prevádzky bol vydaný a vykonaný v súlade s podmienkami podľa § 115 odsek 1 Trestného poriadku (*lege artis*) vysloví uznesením, že zákon porušený nebol. Proti tomuto rozhodnutiu nie je taktiež prípustný opravný prostriedok.

Ústavný súd viackrát vyslovil, že povaha odôvodnenia je nedostatočná a formálna, pretože neodkryla súvislosti a okolnosti, na základe ktorých by bolo možné pochopiť odôvodnenosť tohto zásahu do práva na súkromie, a preto je takýto príkaz považovaný zo strany Ústavného súdu za nelegálny.³² V príkaze absentujú konkrétne odôvodnené skutočnosti, na základe, ktorých boli naplnené zákonné podmienky zásahu do práva na súkromie. V prípade strohej citácie príslušných zákonných ustanovení došlo len k formálnemu (všeobecnému) odôvodneniu príkazu, pričom takýto postup nie je možné akceptovať z hľadiska absencie splnenia materiálnych podmienok potrebných na nariadenie odpočúvania a záznamu telekomunikačnej prevádzky.

Aby bolo možné postup podľa § 115 Trestného poriadku označiť za ústavno konformný, musí obstať v tzv. teste proporcionality. Problém ústavnej konformity tohto postupu sa prejavuje v dvoch rovinách a to v prípustnosti takéhoto postupu s ohľadom na ochranu základných práv

³¹ Nález Ústavného súdu Slovenskej republiky spisovej značky III. ÚS 133/2010.

³² Pozri tiež Rozsudok Krajského súdu Trenčín spisová značka 6Co/84/2012.

a slobôd ako objektívnej hodnoty a posúdením prípustnosti vo vzťahu k subjektívnym základným právam a slobodám jednotlivca.

6. Európsky vyšetrovací príkaz v trestných veciach

V prvej polovici marca 2014 bol riadnym legislatívnym postupom Radou Európskej únie po prvom čítaní v Európskom parlamente prijatý návrh smernice z roku 2010 o európskom vyšetrovacom príkaze v trestných veciach (ďalej len „EVP“).³³ Po odobrení Radou Európskej únie majú členské štáty tri roky na jej transpozíciu do vlastných právnych systémov, pričom konečný dátum transpozície je 22. máj 2017. Do tohto dátumu musia členské štáty prijať opatrenia potrebné na dosiahnutie súladu s touto smernicou, pričom priamo v nich uvedú alebo pri ich úradnom uverejnení uverejnia odkaz na túto smernicu. K tomuto dátumu sa tiež viaže povinnosť členských štátov zaslať Komisii znenie ustanovení, ktorými do svojho vnútroštátneho práva transponujú povinnosti, ktoré im ukladá táto smernica (článok 36).

Pro futuro sa nás teda bude v súvislosti s našou témou týkať článok 30 a 31 predmetnej Smernice, v ktorom je upravené odpočúvanie telekomunikačnej prevádzky s technickou podporou iného členského štátu a informovanie členského štátu, v ktorom sa nachádza odpočúvaná osoba, a ktorého technická pomoc je potrebná.

Pre úplnosť uvádzame vyššie uvedené články v plnom znení:

Článok 30

Odpočúvanie telekomunikačnej prevádzky s technickou pomocou iného členského štátu

1. EVP sa môže vydať na účely odpočúvania telekomunikačnej prevádzky v členskom štáte, ktorého technická pomoc je potrebná.

2. Ak môže potrebnú technickú pomoc na rovnaké odpočúvanie telekomunikačnej prevádzky poskytnúť viac ako jeden členský štát, EVP sa zašle jednému z nich. Uprednostní sa vždy členský štát, v ktorom sa odpočúvaná osoba nachádza alebo sa bude nachádzať.

3. EVP uvedený v odseku 1 obsahuje aj tieto informácie:

- a) informácie na účely zistenia totožnosti odpočúvanej osoby;
- b) požadované trvanie odpočúvania a
- c) dostatočné technické údaje, najmä identifikátora cieľa, s cieľom zabezpečiť vykonanie EVP.

4. Vydávajúci orgán v EVP uvedie dôvody, prečo sa domnieva, že uvedené vyšetrovacie opatrenie je relevantné na účely príslušného trestného konania.

5. Okrem dôvodov neuznania alebo nevykonania uvedených v článku 11 možno odmietnuť vykonanie EVP uvedeného v odseku 1 aj vtedy, ak by sa dotknuté vyšetrovacie opatrenie nepovolilo v podobnom vnútroštátnom prípade. Vykonávajúci štát môže podmieniť svoj súhlas akýmkoľvek podmienkami, ktoré by sa museli splniť v podobnom vnútroštátnom prípade.

6. EVP uvedený v odseku 1 možno vykonať:

- a) bezodkladným zaslaním telekomunikačnej prevádzky vydávajúcemu štátu alebo
- b) odpočúvaním, záznamom a následným zaslaním výsledku odpočúvania telekomunikačnej prevádzky vydávajúcemu štátu.

Vydávajúci orgán a vykonávajúci orgán sa navzájom radia s cieľom dohodnúť sa na tom, či sa odpočúvanie vykoná v súlade s písmenom a), alebo b).

³³ Bližšie pozri Smernicu Európskeho parlamentu a rady 2014/41/EÚ z 3. apríla 2014 o európskom vyšetrovacom príkaze v trestných veciach.

7. Ak má na to vydávajúci orgán osobitný dôvod, môže pri vydávaní EVP uvedeného v odseku 1 alebo počas odpočúvania požiadať aj o prepis, dekódovanie alebo dešifrovanie záznamu, ak s tým vykonávajúci orgán súhlasí.

8. Náklady vyplývajúce z uplatňovania tohto článku sa znášajú v súlade s článkom 21, a to s výnimkou nákladov vyplývajúcich z prepisu, dekódovania a dešifrovania odpočúvanej telekomunikačnej prevádzky, ktoré znáša vydávajúci štát.

Článok 31

Informovanie členského štátu, v ktorom sa nachádza odpočúvaná osoba, a ktorého technická pomoc nie je potrebná

1. Ak na účely vykonania vyšetrovacieho opatrenia povolí príslušný orgán určitého členského štátu odpočúvanie telekomunikačnej prevádzky (ďalej len „odpočúvajúci členský štát“) a komunikačná adresa odpočúvanej osoby, určenej v príkaze na odpočúvanie, sa používa na území iného členského štátu (ďalej len „informovaný členský štát“), ktorého technická pomoc nie je potrebná na účely vykonania odpočúvania, odpočúvajúci členský štát informuje príslušný orgán informovaného členského štátu o odpočúvaní:

- a) pred odpočúvaním v prípadoch, keď je príslušnému orgánu odpočúvajúceho členského štátu pri nariadení odpočúvania známe, že odpočúvaná osoba sa nachádza alebo sa bude nachádzať na území informovaného členského štátu;
- b) počas odpočúvania alebo po jeho vykonaní, a to bezodkladne po tom, ako sa dozvie, že odpočúvaná osoba sa počas odpočúvania nachádza alebo nachádzala na území informovaného členského štátu.

2. Na informovanie uvedené v odseku 1 sa využije formulár uvedený v prílohe C.

3. Ak by sa odpočúvanie nepovolilo v podobnom vnútroštátnom prípade, príslušný orgán informovaných členských štátov môže bezodkladne a najneskôr do 96 hodín po informovaní uvedenom v odseku 1 informovať príslušný orgán odpočúvajúceho členského štátu o tom:

- a) že odpočúvanie sa nesmie vykonať alebo sa musí ukončiť a
- b) v prípade potreby sa žiadny materiál, ktorý sa získal odpočúvaním počas pobytu odpočúvanej osoby na jeho území nemôže použiť alebo sa môže použiť len za podmienok, ktoré určí. Príslušný orgán informovaného členského štátu informuje príslušný orgán odpočúvajúceho členského štátu o dôvodoch týchto podmienok.

4. Na informovanie uvedené v odseku 2 sa primerane uplatní článok 5 ods. 2.

Záver

Na záver treba uviesť, že odpočúvanie a záznam telekomunikačnej prevádzky má jednoznačný zmysel a význam a jeho využitie nie je možno spreneveriť na iný účel. Odpočúvanie a záznam telekomunikačnej činnosti je jedným z najzásadnejších zásahov do súkromia fyzickej osoby. Trestný poriadok ho upravuje kogentne a presne stanovuje limity jeho použitia. Nie je preto možné vykladať jeho použitie extenzívne, odvolávajúc sa na tzv. Radbruchovu formulu, ale výlučne restriktívne. Opačný, alternatívny výklad podľa prirodzeno-právnej koncepcie, by bol v rozpore s argumentom *reductio ad absurdum*. Bol by nezmyselný a mal by neprijateľný výsledok. Viedol by totiž k vylúčeniu použitia tohto ustanovenia, teda faktickej nemožnosti jeho použitia. Vykonanie tohto nezákonného dôkazu by bolo porušením povinnosti viesť trestné stíhanie výlučne zákonným spôsobom. Príkaz na odpočúvanie a záznam telekomunikačnej činnosti musí konkrétne odôvodňovať skutočnosti, na základe ktorých došlo k splneniu podmienky zásahu do

práva na súkromie a príslušné orgány zabezpečiť dodržiavanie limitov možných zásahov štátu do súkromnej sféry jednotlivca.

Použitá literatúra:

- Čentéš, J. a kol. Trestný poriadok s komentárom, Žilina: Eurokódex – Poradca podnikateľa, 2006.
- Čentéš, J. Odpočúvanie – procesnoprávne a hmotnoprávne aspekty, Bratislava: C. H. Beck, 2013.
- Kyjac, Z. Použitie informačno-technických prostriedkov v trestnom konaní, Odpočúvanie a záznam telekomunikačnej činnosti, Bratislava: Wolters Kluwer s. r. o., 2015.
- Ivor, J. a kol. Trestné právo procesné, druhé, doplnené a prepracované vydanie, Bratislava: Iura edition, 2010.
- Jelínek, J., Uhlířová, M. Obhájce v trestním řízení. 1. vydání. Praha: Leges. 2011.
- Molek, P. Právo na spravlivý proces, Praha: Wolters Kluwer, 2012.
- Samaš O. Stiffel H., Toman P., Trestný zákon stručný komentár, Bratislava: Iura edition 2006.
- Ivor, J. Využitie záznamu z odpočúvania ako dôkazu v trestnom konaní. In: Zborník príspevkov z medzinárodnej konferencie „Československé právnické dni“, 2. ročník. Omšenie.
- Čentéš, J., Lazareva, N. Legalita, legitimita a proporcionálnosť odpočúvania a zaznamenávania telekomunikačnej prevádzky, Zborník príspevkov z celoštátnej konferencie s medzinárodnou účasťou „Aktuálne otázky trestného zákonodarstva“ – pocta akademikovi, Dr. h. c. prof. JUDr. Milanovi Čičovi, DrSc., k 80. narodeninám, konanej 19. 1. 2012. Bratislava: Fakulta práva Paneurópskej vysokej školy, 2012.
- Novotná, J. K některým otázkám dokazování odposlechem a záznamem telekomunikačního provozu. In Trestněprávní revue. 2003. č. 10.
- Perhács, Z. Garancie ochrany pred svojvoľným použitím informačno-technických prostriedkov zločkami štátnej moci. In Justičná revue. 2013, roč. 65. č. 6–7
- Perhács, Z. Perhácsová, A. Právna úprava používania informačno-technických prostriedkov (1. časť). In Justičná revue. 2013, roč. 65. 2013, č. 4.
- Perhács, Z. Perhácsová, A. Právna úprava používania informačno-technických prostriedkov (2. časť). In Justičná revue. 2013, roč. 65. 2013, č. 5.
- Perhács, Z. O zničení záznamov, získaných použitím informačno-technických prostriedkov. In Justičná revue. 2007, roč. 59, č. 5.
- Perhács, Z., Zajonc, A. Poznámky k sledovaniu, priestorovému a telefonickému odposluchu. In Justičná revue. 2011, roč. 63, č. 8–9.
- Perhács, Z. O nevyhnutných atribútoch rozhodnutia sudcu na použitie informačno-technických prostriedkov, In Bulletin slovenskej advokácie, 2013, ročník XIV, 12.
- Růžička, M. Odposlech a záznam telekomunikačního provozu v analytických materiálech státního zastupitelství. In Státní zastupitelství. 2008. číslo 3.
- Záhora, J. Príkaz v trestnom konaní. In Justičná revue. 2004. roč. 56, č. 5.
- Zákon číslo 460/1992 Zb. Ústava Slovenskej republiky v znení neskorších právnych prepisov.
- Ústavný zákon číslo 23/1991 Zb., ktorým sa uvádza Listina základných práv a slobôd ako ústavný zákon Federálneho zhromaždenia Českej a Slovenskej Federatívnej Republiky.
- Zákon číslo 301/2005 Z. z. Trestný poriadok v znení neskorších právnych predpisov.
- Zákon číslo 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov v znení neskorších právnych predpisov.
- Zákon číslo 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších právnych predpisov.
- Nález Ústavného súdu Slovenskej republiky spisovej značky PL. ÚS 10/2014 z 29. 4. 2015.
- Nález Ústavného súdu Slovenskej republiky spisovej značky III. ÚS 133/2010 z 27. 9. 2011.
- Uznesenie Ústavného súdu Slovenskej republiky spisovej značky I. ÚS 604/2014 z 28. 10. 2014.

Uznesenie Ústavného súdu Slovenskej republiky I. ÚS 241/07 z 6. 3. 2007.

Uznesenie Najvyššieho súdu Slovenskej republiky spisovej značky 2 To 11/2014 z 27. 10. 2015.

Uznesenie Najvyššieho súdu Slovenskej republiky spisovej značky 1 To 4/2010 z 14. 11. 2011.

Uznesenie Najvyššieho súdu Slovenskej republiky spisovej značky 3 To 2/2011 z 21. 9. 2011.

Uznesenie Najvyššieho súdu Slovenskej republiky spisovej značky 4 To 3/2012 z 25. 6. 2013.

Rozsudok Krajského súdu Trenčín spisovej značky 6Co/84/2012 z 26. 11. 2013.

Rozhodnutie Európskeho súdu pre ľudské práva Sallinen c. Fínsko.

Rozhodnutie Európskeho súdu pre ľudské práva Case of Segerstedt-Wiberg and Others v. Sweden, 2006.

Rozhodnutie Európskeho súdu pre ľudské práva Marckx c. Belgicko z 13. júna 1979.

Smernica Európskeho parlamentu a Rady 2014/41/EÚ z 3. 4. 2014 o európskom vyšetrovacom príkaze v trestných veciach.

Nález Ústavného súdu Českej republiky spisovej značky III. ÚS 2847/14 z 3. 1. 2017.

Nález Ústavného súdu Českej republiky III. ÚS 501/04 z 3. 3. 2005.

ASPI – komentáre k zákonom a dôvodové správy.

<http://www.pravnelisty.sk/clanky/a544-vyhotovenie-nahravky-inej-osoby-utajovanim-sposobom>.

<http://www.pravnelisty.sk/rozhodnutia/a189-sukromna-diktafonova-nahravka-a-nezakonnost-dokazu>.

https://www.law.muni.cz/sborniky/cofola2011/files/normotvorba/Tothova_Marcela_5725.pdf.

http://www.ucps.sk/ZAKONNOST_PROCESU_DOKAZOVANIA_PRED_ZACATIM_TRESTNEHO_STIHANIA_.

Všeobecná deklarácia ľudských práv prijatá 10. Decembra 1948 Valným zhromaždením Organizácie spojených národov.

Charta základných práv Európskej únie.

Odpočúvanie a záznam telekomunikačnej prevádzky a oznámenie údajov o telekomunikačnej prevádzke¹

Interception and Recording of Telecommunications and Notification of Communication Data

Juraj Chylo²

Abstrakt: Témou príspevku je aktuálne vymedzenie informačno-technických prostriedkov z pohľadu odpočúvania a zaznamenávania telekomunikačnej prevádzky, ako i oznámenie údajov o telekomunikačnej prevádzke za účelom využitia informácií takto získaných ako dôkazu v trestnom konaní.

Abstract: The topic of the article is the current definition of the information and technical resources from the perspective of the interception and recording of telecommunications, as well as notification of communication data in order to use the information thus obtained as evidence in criminal proceedings.

Kľúčové slová: dôkazný prostriedok, dôkaz, informačno-technické prostriedky, odpočúvanie a zaznamenávanie telekomunikačnej prevádzky, oznámenie údajov o telekomunikačnej prevádzke.

Key words: means of evidence, evidence, information-technical means, interception and recording of telecommunications, notice of data communication traffic.

Informačno-technické prostriedky

Za dôkazný prostriedok sa podľa § 119 ods. 2 TP považujú aj informácie získané použitím informačno-technických prostriedkov alebo prostriedkov operatívno-pátracej činnosti.

Odhaľovanie a vyšetrovanie špecifických druhov trestných činov, najmä tých, pre ktoré je príznačná vysoká organizovanosť páchatelov ale i konšpiratívne metódy páchania trestnej činnosti vyžaduje pre naplnenie účelu trestného konania používanie špecifických prostriedkov získavania informácií pre trestné konanie využiteľné aj ako dôkazy. Ich použitie je spojené so zásahom do základných práv a slobôd, najmä práva na súkromie a rodinného života, domovej slobody, tajomstva dopravovaných správ, ochrany osobných údajov. Je preto nadmieru dôležité, aby v zmysle procesnej zásady primeranosti a zdržanlivosti nedochádzalo ich použitím k nepriemeraným zásahom do týchto práv, ale len v miere nevyhnutnej na dosiahnutie účelu trestného konania, pričom treba rešpektovať dôstojnosť osôb a ich súkromie nie len z pohľadu intenzity zásahu, ale aj časovej dĺžky zásahu.

Dotknuté práva osôb pri využívaní informačno-technických prostriedkov formálne vychádzajú ako z Ústavy SR, Listiny, tak i z Dohovoru, podľa ktorého každý má právo na rešpektovanie svojho súkromného a rodinného života, obdobia a korešpondencie, pričom štátny orgán nemôže do výkonu tohto práva zasahovať okrem prípadov, keď je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom a zločinnosti, ochrany zdravia alebo morálky alebo ochrany práv a slobôd iných.

¹ Táto práca bola podporovaná Agentúrou na podporu výskumu a vývoja na základe Zmluvy č. APVV-0356-12.

² JUDr. Juraj Chylo, PhD. Paneurópska vysoká škola, Fakulta práva, Tomášikova 20 Bratislava, prokurátor, Okresná prokuratúra Bratislava II, Kvetná 13 Bratislava.

Prostriedky tajného dohľadu nad občanmi sú typické pre policajný štát, avšak aj v demokratickej spoločnosti sú tolerovateľné na ochranu práva. Tolerovateľnosť zásahov do práva na súkromie sa podľa ustálenej judikatúry ESLP vykladajú podľa postupnosti a to, či je zásah považovaný za narušenie práva na súkromie, a ak áno, tak či je považovaný za

- **legálny** (tzn. zásah musí byť na základe zákona a v súlade so zákonom, ako i to, že zákon upravujúci štátom nariadené tajné sledovanie musí byť prístupný pre každého, aby mohol prispôbiť svoje správanie, pričom musí byť formulovaný dostatočne zrozumiteľne a určito aby bolo možné vymedziť osoby, ktoré môžu byť sledované, určiť podmienky použitia utajeného sledovania, ako i určiť štátne orgány oprávnené vykonávať, resp. nariadiť sledovanie),
- **legitímny** (teda keď je zásah vykonávaný v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom a zločinnosti, ochrany zdravia alebo morálky alebo ochrany práv a slobôd iných),
- **proporcionálny** (tzn. subsidiárny, nevyhnutný, kedy účel trestného konania nemožno dosiahnuť inou, miernejšou formou).

Tieto kritériá sa posudzujú v určitej postupnosti. Najskôr sa skúma, či bol zásah legálny, následne sa skúma, či bol legitímny a napokon, či bol proporcionálny. Ak sa dospeje k negatívnej odpovedi pri niektorej odpovedi pri niektorom z týchto kritérií, ďalej sa v skúmaní problematiky nepokračuje a konštatuje sa porušenie čl. 8 Dohovoru.³

S ochranou základných ľudských práv a slobôd je spojená aj súdna ochrana, kedy pri vydávaní príkazu na použitie informačno technických prostriedkov býva potrebný príkaz (súhlas) sudcu pre prípravné konanie v prípravnom konaní, resp. príkaz predsedu senátu v konaní pred súdom.

Informačno-technickými prostriedkami sa na účely TP rozumejú elektrotechnické, rádiotechnické, fototechnické, optické, mechanické, chemické a iné technické prostriedky a zariadenia alebo ich súbory použité utajovaným spôsobom pri odpočúvaní a zázname prevádzky v elektronických komunikačných sieťach (**odpočúvanie a záznam telekomunikačnej prevádzky**), **vyhotovovaní obrazových, zvukových alebo obrazovo-zvukových záznamov** alebo pri **vyhľadávaní, otváraní a skúmaní zásielok**, ak sa ich použitím zasahuje do základných ľudských práv a slobôd. (§ 10 ods. 21 TP).

Trestný poriadok upravuje aj vzťah k prevádzkovateľom verejných telefónnych sietí, poskytovateľom elektronických telekomunikačných sietí, poskytovateľom elektronických telekomunikačných služieb, poštovému podniku, dopravcom a iní zasielateľom a ich zamestnancom, kedy títo sú povinní poskytnúť nevyhnutnú súčinnosť pri použití informačno-technických prostriedkov, pričom sa nemôžu dovolávať povinnosti mlčanlivosti.

Aby bolo možné v súlade s ustanovením § 2 ods. 12 TP vyhodnotiť dôkaz získaný použitím informačno-technických prostriedkov ako dôkaz získaný zákonným spôsobom v zmysle a v intenciách judikatúry Európskych orgánov ochrany práva, Ústavného súdu Slovenskej republiky a Najvyššieho súdu Slovenskej republiky možno vo všeobecnosti zhrnúť, že je potrebné, aby boli splnené tieto základné podmienky:

- podaný návrh spĺňa náležitosti stanovené Trestným poriadkom alebo zákonom č. 166/2003 Z. z. o ochrane pred odpočúvaním;
- príkaz alebo súhlas na použitie informačno-technických prostriedkov je riadne odôvodnený, obsahuje všetky stanovené náležitosti a bol vydaný príslušným súdom a sudcom;

³ Záhora, J.: *Uchovanie počítačových údajov a ochrana súkromia*, In: Justičná revue, ročn. 2011, č. 6–7 s. 904.

- použitie informačno-technických prostriedkov bolo vykonané v súlade s vydaným príkazom;
- dôkaz získaný použitím informačno-technických prostriedkov je použiteľný v trestnom konaní z hľadiska kvality, obsahu a úplnosti.⁴

Odpočúvanie a záznam telekomunikačnej prevádzky

Odpočúvanie a záznam telekomunikačnej prevádzky je inštitútom zabezpečovania informácií v trestnom konaní za súčasného narušenia telekomunikačného tajomstva a odpočúvania, ako i zaznamenávania telekomunikačnej prevádzky telekomunikačného zariadenia a to v súčasnosti, alebo v budúcnosti, ktorý narušuje právo na súkromie. Ide o informačno technický prostriedok a dôkazným prostriedkom sú informácie získané jeho použitím. Odpočúvanie a záznam telekomunikačnej prevádzky robí príslušný útvar Policajného zboru.

Dôkaz použiteľný v trestnom konaní predstavuje záznam telekomunikačnej prevádzky s doslovným prepisom záznamu, ktorý vyhotoví príslušník Policajného zboru vykonávajúci odpočúvanie, v rozsahu zistených skutočností významných pre trestné konanie, s uvedením údajov o mieste, čase, orgáne, ktorý záznam vyhotovil, a zákonnosti vykonávania odpočúvania. V literatúre jemožné sa stretnúť aj s názorom, že prepis záznamu je nevyhnutný len v rozsahu nevyhnutnom pretrestné konanie. V praxi to znamená, že rozhovor trvajúci niekoľko desiatok minút nie je potrebné celý prepísať, ale doslovne len tie časti, ktoré sú z hľadiska trestného konania významné. Na rozdiel od prepisu musí byť kompletný záznam telekomunikačnej prevádzky v celosti uložený na nosiči, ktorý tvorí súčasť vyšetrovacieho spisu. Bez prepisu sa môže zrozumiteľný záznam telekomunikačnej prevádzky použiť v prípravnom konaní, len ak to okolnosti prípadu umožňujú a za účelom jeho predloženia súdu.⁵

Ak sa však pri odpočúvaní a zaznamenávaní telekomunikačnej prevádzky zistí, že obvinený komunikuje so svojím obhajcom, takto získané informácie nemožno použiť na účely trestného konania a musia sa predpísaným spôsobom bez meškania zničiť, to neplatí, ak ide o informácie, ktoré sa vzťahujú na vec, v ktorej advokát nezastupuje obvineného ako obhajcu. Uvedená zákonná úprava teda neposkytuje právnu ochranu komunikácii medzi advokátom a klientom vo všeobecnosti, ale len obvinenému a obhajcovi.

Odpočúvaním rozumieme utajené vnímanie komunikácie prostredníctvom telekomunikačných zariadení účastníkov telekomunikačnej prevádzky. **Záznamom** sa rozumie činnosť zaznamenania a uchovania prevádzky na príslušný nosič umožňujúci reprodukciu zaznamenananej komunikácie v budúcnosti.

Telekomunikačným tajomstvom sa podľa § 63 ods. 1 zákona č. 351/2011 Z. z. rozumie:

- a) obsah prenášaných správ,
- b) súvisiace údaje komunikujúcich strán, ktorými sú telefónne číslo, obchodné meno a sídlo právnickej osoby, alebo obchodné meno a miesto podnikania fyzickej osoby – podnikateľa alebo osobné údaje fyzickej osoby, ktorými sú meno, priezvisko, titul a adresa trvalého pobytu; predmetom telekomunikačného tajomstva nie sú údaje, ktoré sú zverejnené v telefónnom zozname,
- c) prevádzkové údaje a
- d) lokalizačné údaje.

⁴ Bližšie pozri Uznesenie NS SR 1 To 4/2010 z 14. 11. 2011.

⁵ ČENTĚŠ, J. a kol.: *Trestný poriadok – komentár*, Žilina: Eurokódex Poradca podnikateľa, 2014, s. 315.

V právnom poriadku SR je odpočúvania a záznam telekomunikačnej prevádzky vykonávaný na základe dvoch právnych noriem a to Trestného poriadku a zákona č. 166/2003 Z. z. zákona o ochrane pred odpočúvaním. Aplikácia konkrétnej normy závisí od účelu, ktorý chce príslušný štátny orgán dosiahnuť. Zákon o ochrane pred odpočúvaním upravuje podmienky odpočúvania pri spravodajskom rozpracovaní predmetu spravodajského záujmu a nie je ho možné aplikovať na odpočúvanie v trestnom konaní.

Uvedené však neplatí výnimočne, pretože je možné použiť ako dôkaz v trestnom konaní informácie získané použitím informačno-technických prostriedkov podľa zákona o ochrane pred odpočúvaním, pričom orgán štátu vyhotoví písomný záznam s uvedením údajov o mieste, čase a zákonnosti použitia informačno-technického prostriedku, taktiež k písomnému záznamu orgán štátu priloží záznam a jeho doslovný prepis. Informácie získané použitím informačno-technického prostriedku, ktoré sa nevzťahujú na dôvody jeho použitia uvedeného v žiadosti zákonnému sudcovi, ktorý udeľuje súhlas s použitím informačno-technických prostriedkov podľa zákona o ochrane pred odpočúvaním, sa môžu použiť ako dôkaz v trestnom konaní, len ak sa týkajú trestnej činnosti, v súvislosti s ktorou možno použiť informačno-technický prostriedok.⁶ Pokiaľ však orgány činné v trestnom konaní majú vedomosť, že vo veci, kde sa vykonáva odpočúvanie na základe zákona o ochrane pred odpočúvaním je páchaný trestný čin, je ich povinnosťou začať trestné konanie, resp. začať vykonávať odpočúvanie na základe Trestného poriadku.

Vykonávať odpočúvanie a záznam telekomunikačnej prevádzky v trestnom konaní je možné na základe príkazu predsedu senátu súdu a pred začatím trestného stíhania alebo v prípravnom konaní sudca pre prípravné konanie na návrh prokurátora. Je teda zrejmé, že predseda senátu má právomoc vydať príkaz ex officio aj bez návrhu prokurátora, pričom *conditio sine qua non* pre vydanie príkazu na odpočúvanie sudcom pre prípravné konanie predstavuje návrh prokurátora.

V prípade, ak ide o vec, ktorá neznesie odklad, a príkaz sudcu pre prípravné konanie nemožno získať vopred, môže príkaz na odpočúvanie a záznam telekomunikačnej prevádzky pred začatím trestného stíhania alebo v prípravnom konaní vydať prokurátor s platnosťou 24 hodín, ak odpočúvanie a záznam telekomunikačnej prevádzky nie je spojené so vstupom do obydľia. Do uplynutia lehoty 24 hodín však musí sudca pre prípravné konanie potvrdiť tento príkaz, inak stráca platnosť a takto získané informácie nemožno použiť na účely trestného konania a musia sa predpísaným spôsobom bez meškania zničiť.

Príkaz na odpočúvanie a záznam telekomunikačnej prevádzky sa musí vydať písomne a odôvodniť aj skutkovými okolnosťami odôvodňujúcimi potrebu vykonávať odpočúvanie a záznam telekomunikačnej prevádzky vždy pre každú jednu účastnícku stanicu alebo zariadenie.

Zákonnými náležitosťami príkazu je:

- individuálne určenie účastníckej stanice alebo zariadenia a zároveň aj určenie osoby, ak je známa, ktorej sa odpočúvanie a záznam telekomunikačnej prevádzky týka,
- čas, po ktorý sa bude odpočúvanie a záznam telekomunikačnej prevádzky vykonávať.

Čas odpočúvania a záznamu môže trvať najviac šesť mesiacov. Tento čas môže v prípravnom konaní na návrh prokurátora sudca pre prípravné konanie opakovane predĺžiť vždy o ďalšie dva mesiace a označenie orgánu, o ktorého rozhodnutie ide, dátum a miesto rozhodnutia, výrok príkazu s uvedením zákonných ustanovení, ktoré boli použité, skutok s uvedením právnej kvalifikácie trestného činu, ak z povahy veci nevyplýva niečo iné.

⁶ Bližšie pozri Aláč, M.: *Získavanie informácií na spravodajské účely a na účely trestného konania*, Bratislava: C. H. Beck, 2015, s. 65.

Príkaz na odpočúvanie možno vydať v trestnom konaní o zločine, korupcii, trestných činoch extrémizmu, trestnom čine zneužívania právomoci verejného činiteľa, trestnom čine legalizácie príjmu z trestnej činnosti alebo pre iný úmyselný trestný čin, o ktorom na konanie zaväzuje medzinárodná zmluva. Pre iný úmyselný trestný čin môže byť vydaný príkaz na odpočúvania a záznam telekomunikačnej prevádzky len so súhlasom užívateľa odpočúvaného, príp. zaznamenávaného zariadenia. Zároveň platí, že advokát nemôže súhlasiť s tým, aby si nechal odpočúvať svoj telefón, prostredníctvom ktorého komunikuje so svojimi klientami, čo súvisí s jeho povinnosťou zachovávať mlčanlivosť advokáta.

Ak sa pri odpočúvaní a zázname telekomunikačnej prevádzky nezistili skutočnosti významné pre trestné konanie, orgán činný v trestnom konaní alebo príslušný útvar Policajného zboru musí získaný záznam predpísaným spôsobom bezodkladne zničiť.

V minulosti vznikol aplikačný problém s využitím záznamu o telekomunikačnej prevádzke v inej trestnej veci, než v ktorej bol príkaz na odpočúvanie vydaný. Podľa § 115 ods. 7 TP v inej trestnej veci, ako je tá, v ktorej sa odpočúvanie a záznam telekomunikačnej prevádzky vykonal, možno záznam ako dôkaz použiť len vtedy, ak sa súčasne aj v tejto veci vedie trestné konanie pre príslušný trestný čin (podľa § 115 ods. 1 TP). Na jednej strane súdy zaujímali stanovisko, že treba toto ustanovenie vykladať doslovne, a to tak, že obligatórnou podmienkou použitia záznamu telekomunikačnej prevádzky v inej trestnej veci je vedenie tohto iného trestného konania pre trestné činy uvedené v § 115 ods. 1 TP súčasne s trestným konaním, kde sa záznam telekomunikačnej prevádzky vykonal.⁷ Na strane druhej a s tým súhlasíme, slovo „súčasne“ podľa § 115 ods. 7 TP je potrebné správne vzťahovať až k okamžiku použitia výsledkov odpočúvania a nie už k okamihu vykonávania odpočúvania. Bolo by nelogické, aby zákonným spôsobom vykonané odpočúvanie a záznam telekomunikačnej prevádzky, ktoré vo veci, v ktorej bolo nariadené mohlo byť vykonané aj pred začatím trestného stíhania, ale v inej veci by mohlo byť použité len v tom prípade, ak by už v dobe vykonávania tohto odpočúvania bolo v tejto inej veci vedené trestné stíhanie a nič by v tomto prípade nebránilo, aby bolo súčasne nariadené odpočúvanie aj v tejto veci, kde dokonca na rozdiel od tej prvej veci by obvinený už bol známy. Opačný výklad by bol v rozpore s argumentom *reductione ad absurdum*, nakoľko by viedol k záveru, ktorý nemá rozumný zmysel a v podstate by znamenal vylúčenie použitia tohto ustanovenia na rozhodujúcu väčšinu prípadov v praxi a znamenal by faktickú nemožnosť použitia predmetného ustanovenia.⁸

V súvislosti s odpočúvaním a záznamom telekomunikačnej prevádzky nemožno opomenúť ani inštitút oznámenia údajov o telekomunikačnej prevádzke podľa § 116 ods. 1 a 2 TP v trestnom konaní pre úmyselný trestný čin, za ktorý zákon ustanovuje trest odňatia slobody, ktorého horná hranica je najmenej tri roky, pre trestný čin ochrany súkromia v obydlí podľa § 194a, podvodu podľa § 221, nebezpečného vyhrážania podľa § 360, nebezpečného prenasledovania podľa § 360a, šírenia poplašnej správy podľa § 361, podnecovania podľa § 337, schvaľovania trestného činu podľa § 338, pre trestný čin, ktorým bola spôsobená ťažká ujma na zdraví alebo smrť alebo pre iný úmyselný trestný čin, pri ktorom na konanie zaväzuje medzinárodná zmluva, kedy sudca pre prípravné konanie (na návrh prokurátora), alebo predseda senátu môže vydať príkaz na zistenie a oznámenie údajov o telekomunikačnej prevádzke, ktoré sú predmetom telekomunikačného tajomstva, alebo na ktoré sa vzťahuje ochrana osobných údajov, ktoré sú nevyhnutné na objasnenie skutočností dôležitých pre trestné konanie. Príkaz možno vydať, ak nemožno sledovaný účel dosiahnuť inak alebo ak by bolo jeho dosiahnutie iným spôsobom podstatne sťaže-

⁷ Bližšie pozri napr. rozsudok Špecializovaného trestného súdu v Pezinku, sp. zn. PK 2T 21/2007 z 10. 12. 2009.

⁸ Bližšie pozri Uznesenie NS SR 1 To 4/2010 z 14. 11. 2011, Uznesenie NS SR 3 To 2/2011 z 21. 9. 2011.

né. Príkaz na zistenie a oznámenie údajov o telekomunikačnej prevádzke sa musí vydať písomne a odôvodniť; súčasťou príkazu je aj spôsob, rozsah a lehota oznámenia údajov.

Príkaz na zistenie a oznámenie údajov o telekomunikačnej prevádzke vydáva predseda senátu a pred začatím trestného stíhania alebo v prípravnom konaní sudca pre prípravné konanie na návrh prokurátora, ktorý musí byť písomný a odôvodnený aj skutkovými okolnosťami. Príkaz na zistenie a oznámenie údajov o telekomunikačnej prevádzke sa musí vydať písomne a odôvodniť, súčasťou príkazu je aj spôsob, rozsah a lehota oznámenia údajov. Ak sa príkaz týka konkrétneho používateľa, musí byť v ňom uvedená jeho totožnosť, ak je známa. Ak nejde o zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke, zisťovanie a oznamovanie týchto údajov môže trvať najviac šesť mesiacov; tento čas môže v prípravnom konaní na písomný a odôvodnený návrh prokurátora sudca pre prípravné konanie predĺžiť vždy o ďalšie dva mesiace, a to aj opakovane. Príkaz na zistenie a oznámenie údajov o telekomunikačnej prevádzke sa doručuje podniku poskytujúcemu verejné siete alebo služby. Ak údajom neboli zistené skutočnosti významné pre trestné konanie, orgán, ktorého rozhodnutím sa vec právoplatne skončila, údaj bezodkladne zničí, policajt údaj zničí po predchádzajúcom písomnom súhlase prokurátora.

Uvedené ustanovenia zakladajú orgánom činným v trestnom konaní oprávnenie, aby na účely objasnenia skutočností dôležitých pre trestné konanie získali od poskytovateľov elektronických komunikácií údaje o uskutočnenej telekomunikačnej prevádzke, ktoré sú inak predmetom telekomunikačného tajomstva alebo na ktoré sa vzťahuje ochrana osobných údajov.

V minulosti bola právna úprava zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke odlišná, kedy bolo možné vydať v trestnom konaní pre úmyselný trestný čin príkaz na zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke, ktoré sú predmetom telekomunikačného tajomstva alebo na ktoré sa vzťahuje ochrana osobných údajov, ktoré sú potrebné na objasnenie skutočností dôležitých pre trestné konanie. Sprísnenie prelomenia ochrany súkromia nastalo po vydaní nálezů Ústavného súdu SR, ktorým vyslovil o. i. aj nesúlady ustanovenia § 116 TP s čl. 13 ods. 4, čl. 16 ods. 1, čl. 19 ods. 2 a 3 a čl. 22 Ústavy SR, čl. 7 ods. 1, čl. 10 ods. 2 a 3 a čl. 13 Listiny základných práv a slobôd a čl. 8 Dohovoru o ochrane ľudských práv a základných slobôd. Ústavný súd SR k tomu uviedol, že zo znenia napadnutých ustanovení TP vyplýva, že oprávnenie orgánov činných v trestnom konaní požadovať od poskytovateľov elektronických komunikácií zistenie a oznámenie údajov o uskutočnenej elektronickej komunikácii je podmienené iba tým, že takéto opatrenie musí smerovať k objasneniu skutočností dôležitých pre trestné konanie v trestnom konaní pre úmyselný trestný čin. Oprávnenie orgánov činných v trestnom konaní požadovať zistenie a oznámenie údajov o elektronickej komunikácii sa teda netýka len určitej kategórie úmyselných trestných činov, a to tak, ako to ustanovuje § 58 ods. 7 zákona o elektronických komunikáciách, t. j. trestných činov súvisiacich s terorizmom, nedovoleným obchodovaním, organizovanou trestnou činnosťou, únikom a ohrozením utajovaných skutočností a trestných činov spáchaných nebezpečným zoskupením, ale akýchkoľvek úmyselných trestných činov, pričom podľa názoru ústavného súdu takto vymedzený okruh trestných činov, pre účely vyšetrovania, odhaľovania a stíhania ktorých možno zasiahnuť do základného práva na informačné sebaurčenie, upravuje medze tohto základného práva veľmi široko a neurčito. Umožňuje požiadať a použiť predmetné údaje zo strany orgánov činných v trestnom konaní stále, ak je možné nájsť určitú súvislosť s prebiehajúcim konaním o úmyselnom trestnom čine, resp. trestnom čine. Miera intenzity zásahu do práva na súkromie spôsobená uchovávaním a následným sprístupnením údajov o uskutočnenej elektronickej komunikácii orgánom činným v trestnom konaní však požaduje, aby oprávnenie orgánov činných v trestnom konaní požadovať zistenie a oznámenie údajov potrebných na objasnenie skutoč-

ností dôležitých pre trestné konanie sa vzťahovalo len na najzávažnejšie trestné činy. Oprávnenie orgánov činných v trestnom konaní požadovať zistenie a oznámenie údajov o uskutočnenej komunikačnej prevádzke nemôže byť vzhľadom na intenzitu, ktorou zasahuje do základného práva na súkromie, považované za obvyklý alebo rutinný prostriedok prevencie a odhaľovania trestnej činnosti. K použitiu tohto prostriedku boja proti trestnej činnosti môže dôjsť jedine vtedy, ak na dosiahnutie tohto cieľa neexistuje iný a vo vzťahu k základnému právu šetrnejší prostriedok. Ústavný súd SR preto dospel k záveru, že vtedajšie ustanovenia Trestného poriadku upravujúce oznámenie údajov o uskutočnenej telekomunikačnej prevádzke neobstoja v teste proporcionality, lebo nepodmieňovali zisťovanie údajov o uskutočnenej komunikačnej prevádzke zo strany orgánov činných v trestnom konaní požiadavkou nevyhnutnosti a pre ich aplikáciu neustanovovali účinné prostriedky kontroly, ktoré by umožňovali účinnú ochranu základného práva na informačné sebaurčenie dotknutých osôb v priebehu celého obdobia, počas ktorého tieto orgány disponujú predmetnými údajmi ako i to, že uvedené ustanovenia totiž neprikladajú žiaden význam povahe a závažnosti trestného činu, pre ktorý je trestné konanie vedené, a to i napriek tomu, že tieto skutočnosti sú už vo všeobecnej rovine významné pre výsledok pomeňovania v kolízii stojaceho základného práva na informačné sebaurčenie a verejného záujmu na predchádzaní a postihovaní trestných činov. Je úlohou zákonodarcu, aby presne určil, v prípade ktorých trestných činov tento verejný záujem prevažuje, pričom vo svojom rozhodnutí musí zohľadniť ich závažnosť.

Z rovnakých zásad vychádza aj obmedzenie možnosti vydať príkaz na odpočúvanie a záznam telekomunikačnej prevádzky podľa § 115 Trestného poriadku iba pre trestné konanie o zločine, korupcii, trestných činoch extrémizmu, trestnom čine zneužívania právomoci verejného činiteľa, trestnom čine legalizácie príjmu z trestnej činnosti alebo pre iný úmyselný trestný čin, o ktorom na konanie zaväzuje medzinárodná zmluva.⁹ Vzhľadom na skutočnosť, že Ústavný súd SR vyslovil nesúlad vtedajšieho ustanovenia § 116 TP, stratilo uvedené ustanovenie účinnosť a Národná rada SR prijala ustanovenie § 116 TP v súčasnom znení.

Záver

Vzhľadom na vyššie uvedené je možné vysloviť záver, že informačno-technické prostriedky sú prostriedkami tajného dohľadu štátu nad občanmi, ktoré zasahujú do základných práv občanov, najmä práva na súkromie, povinnosti zachovávať napr. telekomunikačné tajomstvo. Informácie získané použitím informačno-technických prostriedkov sú využiteľné ako dôkazy v trestnom konaní za vopred stanovených podmienok to, že musia byť legálne, legitímne a ich použitie musí byť nevyhnutelné (subsidiárne).

V právnom poriadku SR je odpočúvanie a záznam telekomunikačnej prevádzky vykonávaný na základe dvoch právnych noriem a to Trestného poriadku a zákona č. 166/2003 Z. z. zákona o ochrane pred odpočúvaním, pričom záleží na účele využitia odpočúvania a záznamov o telekomunikačnej prevádzke.

Vo vzťahu k využitiu záznamu o telekomunikačnej prevádzke v inej trestnej veci, než v ktorej bol príkaz na odpočúvanie vydaný sme toho názoru, že slovo „súčasne“ podľa § 115 ods. 7 TP je potrebné správne vzťahovať až k okamžiku použitia výsledkov odpočúvania a nie už k okamihu vykonávania odpočúvania. Zároveň sme toho názoru, že dôkaz získaný pri použití informačno-technických prostriedkov nemožno použiť v inom konaní (napríklad správnom konaní, civilnom konaní).

⁹ Nález ÚS SR zo dňa 29. apríla 2015 pod č. k. PL. ÚS 10/2014-78.

Vo vzťahu k oznámeniu údajov o telekomunikačnej prevádzke oprávnenie orgánov činných v trestnom konaní požadovať zistenie a oznámenie údajov o uskutočnenej komunikačnej prevádzke nemôže byť vzhľadom na intenzitu, ktorou zasahuje do základného práva na súkromie, považované za obvyklý alebo rutinný prostriedok prevencie a odhaľovania trestnej činnosti. Miera intenzity zásahu do práva na súkromie spôsobená uchovávaním a následným sprístupnením údajov o uskutočnenej elektronickej komunikácii orgánom činným v trestnom konaní však požaduje, aby oprávnenie orgánov činných v trestnom konaní požadovať zistenie a oznámenie údajov potrebných na objasnenie skutočností dôležitých pre trestné konanie sa vzťahovalo len na najzávažnejšie trestné činy. K použitiu tohto prostriedku boja proti trestnej činnosti môže dôjsť jedine vtedy, ak na dosiahnutie tohto cieľa neexistuje iný a vo vzťahu k základnému právu šetrnejší prostriedok, pričom predchádzajúca právna úprava umožňovala požiadať a použiť predmetné údaje zo strany orgánov činných v trestnom konaní stále, ak je možné nájsť určitú súvislosť s prebiehajúcim konaním o úmyselnom trestnom čine, resp. trestnom čine, preto bol spávy nálež Ústavného súdu SR pod č. k. PL. ÚS 10/2014-78, na základe ktorého Ústavný súd SR vyslovil nesúlad vtedajšieho ustanovenia § 116 TP, ktoré tým stratilo účinnosť a Národná rada SR prijala ustanovenie § 116 TP v súčasnom znení.

Zoznam použitej literatúry:

- Aláč, M.: Získavanie informácií na spravodajské účely a na účely trestného konania, Bratislava: C. H. Beck, 2015, s. 184, ISBN 978-80-89603-32-9,
- Čentéš, J.: Odpočúvanie – procesnoprávne a hmotnoprávne aspekty, Bratislava: C. H. Beck, 2013, 272 s. ISBN 978-80-89603-09-1,
- ČENTÉŠ, J. a kol.: Trestný poriadok – komentár, Žilina: Eurokódex Poradca podnikateľa, 2014, s. 944, ISBN 978-80-8155-0201-8,
- IVOR, J. a kol.: Trestné právo procesné, Druhé doplnené a prepracované vydanie, Bratislava: Iura Edition, 2010, s. 993, ISBN 80-8078-101-X,
- Záhora, J.: Uchovanie počítačových údajov a ochrana súkromia, In: Justičná revue, 2011, č. 6–7 s. 904–913, ISSN: 1335-6461,
- Nález ÚS SR zo dňa 29. apríla 2015 pod č. k. PL. ÚS 10/2014-78,
- Uznesenie NS SR 1 To 4/2010 z 14. 11. 2011,
- Uznesenie NS SR 3 To 2/2011 z 21. 9. 2011,
- Rozsudok Špecializovaného trestného súdu v Pezinku, sp. zn. PK 2T 21/2007 z 10. 12. 2009,
- Zákon č. 460/1992 Zb. Ústava SR,
- Zákon č. 301/2005 Z. z. Trestný poriadok,
- Zákon č. 166/2003 Z. z. zákona o ochrane pred odpočúvaním,
- Dohovor o ochrane ľudských práv a základných slobôd.

Využitie trestno-procesného inštitútu odpočúvanie a záznam telekomunikačnej prevádzky pri dokazovaní trestnej činnosti právnických osôb¹

The use of Wiretapping and Recording Telecommunications in Proving the Crime of Legal Entities

Barbora Tallová²

Abstrakt: Odpočúvanie a záznam telekomunikačnej prevádzky predstavuje dôležitý inštitút trestného práva procesného. Využíva sa pri odhaľovaní a dokazovaní najzávažnejších foriem trestnej činnosti. Témou predkladaného príspevku je využitie odpočúvania a záznamu telekomunikačnej prevádzky pri dokazovaní trestnej činnosti právnických osôb. Možnosť vyodenia trestnej zodpovednosti a s tým súvisiace odhaľovanie a dokazovanie ich trestnej činnosti priamo súvisí s prijatím zákona o trestnej zodpovednosti právnických osôb, ktorý bol s účinnosťou od 1. júla 2016 zavedený do nášho právneho poriadku.

Abstract: The wiretapping and recording of the telecommunications is an important institute of the criminal proceeding law. It is used for detecting and proving the most serious forms of crime. The topic of the present article is the use of wiretapping and recording telecommunications in proving the crime of legal entities. The possibility of detecting and proving of their criminal activity is directly related with the adoption of the Act of Criminal Responsibility of Legal Entities, which was effectively introduced to our law system from July 1st 2016.

Kľúčové slová: odpočúvanie, záznam telekomunikačnej prevádzky, trestná zodpovednosť právnických osôb.

Key words: wiretapping, the interception of telecommunications, criminal liability of legal entities.

Úvod

Odpočúvanie a záznam telekomunikačnej prevádzky je celosvetovo rozšíreným trestno-procesným inštitútom často využívaným v boji s kriminalitou. Slúži najmä na efektívne odhaľovanie závažnejších foriem trestnej činnosti. Problematika jeho použitia pri odhaľovaní a dokazovaní trestnej činnosti právnických osôb patrí k veľmi aktuálnym témam, ktoré priamo súvisia s prijatím nového zákona č. 91/2016 Z. z. o trestnej zodpovednosti právnických osôb, ktorý nadobudol účinnosť 1. 7. 2016. Zavedenie trestnej zodpovednosti právnických osôb do nášho právneho poriadku prinieslo množstvo otázok a doposiaľ nevyriešených problémov. Koncept trestnej zodpovednosti právnických osôb je nášmu trestnému právu cudzí a zásady na ktorých je vybudované trestné právo je možné realizovať v trestnom konaní proti právnickej osobe len veľmi ťažko. Narastajúca ekonomická sila právnických osôb je priamo úmerná vzrastajúcej kriminalite páchanej právnickými osobami. Trestnú činnosť páchajú stále viac sofistikovanejšie, vo väčšom rozsahu, s dôkladnejšou prípravou a premysleným postupom jej zakrytia. Postupom času sa odhaľovanie trestnej činnosti stáva stále viac obtiažnejšie. Páchatelia využívajú premyslené spôsoby utajova-

¹ Táto práca bola podporovaná Agentúrou na podporu výskumu a vývoja na základe Zmluvy č. APVV-15-0272./ This work was supported by the Slovak Research and Development Agency under the contract No. APVV-15-0272.

² Mgr. Barbora Tallová, Ústav verejného práva, Fakulta práva, Paneurópska vysoká škola, Bratislava, e-mail: xtallovab@is.paneurouni.com.

nia informácií ako napr. šifrovanie správ, používanie vlastného zakódovaného jazyka prípadne využívajú inú komunikáciu, ktorá sa nedá orgánmi činnými v trestnom konaní zachytiť. Napriek tomu inštitút odpočúvania a záznamu telekomunikačnej prevádzky v trestnom konaní stále plní nezastupiteľnú a dôležitú funkciu a výsledky jeho použitia sú veľmi významné pri odhaľovaní a dokazovaní trestnej činnosti. Doposiaľ patrí k najviac využívaným informačno-technickým prostriedkom v trestnom konaní. Využitie tohto inštitútu v trestnom konaní vedenom proti právnickej osobe je náročnejšie a komplikovanejšie ako v konaní proti fyzickej osobe. Viaceré možné aplikačné problémy vyplývajú z osobitého postavenia právnických osôb v našom právnom poriadku a ich odlišnej povahy v porovnaní s osobami fyzickými. Využitím daného trestno-procesného inštitútu sa závažným spôsobom zasahuje do práv všetkých dotknutých osôb, ktoré sú garantované nielen na vnútroštátnej ale i medzinárodnej úrovni. Preto aplikácia tohto inštitútu musí podliehať veľmi prísnyim podmienkam, aby práva všetkých zúčastnených osôb zostali zachované.

Zavedenie tzv. pravej trestnej zodpovednosti právnických osôb do nášho právneho poriadku

V úvodnej časti príspevku považujem za vhodné poukázať na základné zmeny týkajúce sa postavenia právnických osôb v trestnom práve, ktoré súvisia s prijatím nového zákona č. 91/2016 Z. z o trestnej zodpovednosti právnických osôb. Možnosť stíhania právnickej osoby v trestnom konaní a využitie inštitútu odpočúvania a záznamu telekomunikačnej prevádzky v trestnom konaní vedenom proti právnickej osobe sa priamo odvodzuje od prijatia predmetného zákona.

Zavedenie trestnej zodpovednosti právnických osôb predstavuje efektívny prostriedok v boji proti protiprávnym aktivitám právnických osôb. Koncept trestnej zodpovednosti právnických osôb má svoj pôvod v angloamerickej právnej kultúre, postupne sa pod vplyvom mnohých medzinárodných záväzkov zaviedol v rôznych modifikáciách vo všetkých štátoch Európskej Únie.³ Otázkami dôležitosti vyvodenia trestnej zodpovednosti právnických osôb sa právní teoretici zaoberali už v dávnej minulosti. Niektoré obchodné spoločnosti začali už vznikáť za účelom ich využívania a zakrývania trestnej činnosti fyzických osôb. „Obchodné spoločnosti vo svojich počiatkoch, prakticky od 15. storočia, boli zakladané s cieľom obmedziť zodpovednosť investora v prípade nezdarenia obchodu a z toho vyplývajúceho sa zadlženia tak, aby neohrozilo jeho osobu a jeho rodinu v súčasnosti a aj do budúcnosti.“⁴

Naše trestné právo patrí do kontinentálneho právneho systému a do 30. 6. 2016 bolo založené výhradne na zásade individuálnej trestnej zodpovednosti za zavinenie, t. j. zásade zodpovednosti konkrétnej fyzickej osoby za jej vlastné konanie, za spáchanie trestného činu. Neuplatňovala sa u nás zodpovednosť za cudziu vinu ani zodpovednosť subjektov tzv. kolektívnej povahy. Voči právnickým osobám sa od roku 2010 uplatňoval model tzv. nepriamej trestnej zodpovednosti. V určitých prípadoch bolo možné právnickej osobe uložiť dva druhy ochranných opatrení (zhabanie peňažnej čiastky a zhabanie majetku). Model nepriamej trestnej zodpovednosti právnických osôb nepredstavoval efektívny nástroj na boj proti protiprávnej činnosti páchanej právnickými osobami. Počas obdobia, kedy bola takáto úprava súčasťou nášho právneho poriadku, nebola týmto spôsobom sankcionovaná žiadna právnická osoba.

³ ZÁHORA, J., 2016. Otvorené otázky trestnej zodpovednosti právnických osôb. In: Justičná revue – časopis pre právnu prax. 2016. č. 5, s. 559–580.

⁴ HURDÍK, J., 2003. Právnické osoby a jejich typologie. 1. vyd. Praha: C. H. Beck, 2003. s. 71.

Až prijatím zákona č. 91/2016 Z. z. o trestnej zodpovednosti právnických osôb (ďalej len ako „TZPO“) s účinnosťou od 1. júla 2016 sa hlavná zásada trestného práva hmotného, zásada individuálnej trestnej zodpovednosti, sčasti prelomila a začala sa relativizovať. V zmysle nového zákona je právnická osoba už priamo zodpovedná za spáchanie trestného činu a je možné jej uložiť tresty, ktorých taxatívny výpočet je v predmetnom zákone uvedený. Prijatie TZPO súviselo najmä so splnením medzinárodných záväzkov Slovenskej republiky a so stále narastajúcou úlohou a vplyvom právnických osôb v spoločenskom živote a zvyšujúcim sa rozsahom škodlivých následkov vznikajúcich vo sfére pôsobnosti právnických osôb.⁵ V súčasnosti rastie vplyv nadnárodných korporácií na našom území a neprehľadnosť štruktúr niektorých právnických osôb neumožňuje vypátrať konkrétneho vinníka a presadiť voči nemu individuálnu trestnú zodpovednosť za spáchanie trestných činov. Nutnosť zavedenia efektívneho mechanizmu sankcionovania právnických osôb, ak došlo v súvislosti s ich činnosťou ku spáchaniu trestného činu vyplývalo z viac ako tridsiatich medzinárodných dokumentov. Uvedený zákon zaviedol do nášho právneho poriadku dovtedy neznámu kolektívnu zodpovednosť v trestných veciach. Sú v ňom upravené podmienky trestnej zodpovednosti právnických osôb, druhy trestov, ich ukládanie a taktiež ustanovenia o úprave trestného konania vedeného proti právnickej osobe.

Základom trestnej zodpovednosti právnických osôb je rovnako ako u fyzických osôb spáchanie trestného činu. „Právna teória pristupuje k právnickej osobe ako k organizácii osôb alebo majetku vytvorenej na určitý účel, ktorej právny poriadok priznáva vlastnú právnu subjektivitu.“⁶ Náš právny poriadok priznáva právnickým osobám tzv. neobmedzenú subjektivitu, spôsobilosť na práva a povinnosti aj spôsobilosť na právne úkony od okamihu jej vzniku. Trestná zodpovednosť právnických osôb je založená na teórii tzv. pričítateľnosti. Právnická osoba ako výtvor právneho poriadku, umelá právna konštrukcia nedokáže sama vlastným konaním spáchať trestný čin. Má zákonom presne stanovený mechanizmus konania, ktorý je zabezpečený a vykonávaný prostredníctvom fyzických osôb. Na rozdiel od fyzickej osoby právnická osoba nedokáže sama myslieť, konať a nemá ani slobodnú vôľu. Všetky úkony za ňu môže robiť len konkrétna fyzická osoba a prostredníctvom nej dochádza k prejavu vôle právnickej osoby, ktorá sa s konaním a myslením tejto osoby stotožňuje. Zákon presne stanovuje okruh subjektov, fyzických osôb, ktoré konajú v jej mene a takéto ich konanie sa považuje za konanie samotnej právnickej osoby. Páchateľom trestného činu teda môže byť právnická osoba, ak určitým zákonom nedovoleným spôsobom postupuje fyzická osoba v jej mene a právnickej osobe sa porušenie alebo ohrozenie záujmu chráneného Trestným zákonom pričíta. Osobou relevantne konajúcou za právnickú osobu môže byť štatutárny orgán alebo jeho člen, ktorý v právnickej osobe vykonáva dohľad (napr. člen dozornej rady), alebo iná osoba, ktorá je oprávnená zastupovať právnickú osobu alebo za ňu rozhodovať (napr. prokurista). Aby mohol byť trestný čin právnickej osobe pričítaný musí byť spáchaný niektorou z osôb uvedených v § 4 ods. 1 TZPO, ktorá takto konala v prospech právnickej osoby, v jej mene, v rámci jej činnosti alebo jej prostredníctvom. „Konceptia pričítateľnosti trestnej zodpovednosti právnických osôb nestojí na objektívnej trestnej zodpovednosti právnických osôb a je samozrejme odlišná od inštitútu zavinenia u fyzických osôb. Ide len o určitú fikciu zavinenia právnickej osoby.“⁷ Vyvodenie trestnej zodpovednosti právnickej osoby nie je podmienené zistením, ktorá konkrétna fyzická osoba takto protiprávne konala. Avšak TZPO, v prípade zistenia konkrétnej fyzickej osoby, ktorej prostredníctvom došlo

⁵ IVOR, J., POLÁK, P., ZÁHORA, J., 2016. Trestné právo hmotné. I. všeobecná časť. Bratislava: Wolters Kluwer. 2016. s. 31–32.

⁶ LAZAR, J., a kol., 2010. Občianske právo hmotné I, Bratislava: Iura Edition. 2010. s. 161.

⁷ IVOR, J., POLÁK, P., ZÁHORA, J., 2016. Trestné právo hmotné. I. všeobecná časť. Bratislava: Wolters Kluwer. 2016. s. 32.

k spáchaniu trestného činu umožňuje vykonať spoločné konanie voči právnickej osobe a fyzickej osobe, pričom trestná zodpovednosť sa v rámci spoločného konania posudzuje samostatne. Trestná zodpovednosť právnických osôb napriek tomu individuálnu trestnú zodpovednosť fyzických osôb nenahrádza. Prioritou v trestnom práve zostáva naďalej vyvodenie trestnej zodpovednosti voči fyzickým osobám. V súvislosti s uvedeným je vhodné pripomenúť, že na vyvodenie trestnej zodpovednosti fyzických osôb sa vyžaduje zavinenie, ktoré chápeme ako vnútorný psychický vzťah páchatela k zamýšľanému následku. Zavinenie môže mať dve formy, úmyselnú a nedbanlivostnú. Podstatným je konanie, ktoré viedlo k spôsobenému následku a v prípade fyzických osôb musí byť takéto konanie páchatelom zavinené. Následky, ktoré vyplynuli z konania fyzickej osoby jej možno pričítať, iba ak ich úmyselne zavinila.

„Trestná zodpovednosť právnických osôb má byť nápomocná tam, kde nie je možné vyvodit' individuálnu trestnú zodpovednosť a zároveň tam, kde je protiprávna činnosť realizovaná prostredníctvom právnickej osoby. Je potrebné odstrániť vákuum ktoré vznikalo v prípade protiprávnej činnosti realizovanej prostredníctvom právnických osôb, kedy sa konkrétne fyzické osoby zodpovedné za protiprávne konanie schovávali za zložité štruktúry právnických osôb.“⁸

V ustanovení § 1 ods. 2 TZPO je uvedené: „Ak tento zákon neustanovuje inak a ak to povaha veci nevyklučuje, na trestnú zodpovednosť právnickej osoby a tresty ukladané právnickej osobe sa vzťahuje Trestný zákon a na trestné konanie proti právnickej osobe sa vzťahuje Trestný poriadok.“ V predmetnom ustanovení je upravená subsidiarita použitia všeobecných trestnoprávných predpisov v prípadoch, ak TZPO konkrétnu právnu úpravu neobsahuje a povaha veci ich použitie nevyklučuje. V prípade, ak uvedený zákon neobsahuje osobitnú úpravu z oblasti hmotnoprávnej, použije sa podporne zákon č. 300/2005 Z. z. Trestný zákon a v prípade absencie procesnej úpravy, ktorá sa má týkať trestného konania vedeného proti právnickej osobe sa podporne bude aplikovať zákon č. 301/2005 Z. z. Trestný poriadok. Pri dokazovaní a odhaľovaní trestnej činnosti právnických osôb sa budú teda aplikovať a využívať procesné inštitúty upravené v Trestnom poriadku, samozrejme za predpokladu, ak to povaha veci nebude vylučovať, pretože TZPO osobitné ustanovenia ohľadne dokazovania v trestnom konaní neobsahuje.

Zásah do súkromia právnickej osoby prostredníctvom odpočúvania a záznamu telekomunikačnej prevádzky

V tejto časti príspevku je pozornosť zameraná na ochranu práva na súkromie, do ktorej možno zasiahnuť v trestnom konaní využitím informačno-technických prostriedkov. Zohrávajú nezasupiteľnú úlohu pri získavaní informácií v boji proti trestnej činnosti ale súčasne predstavujú výrazný zásah do súkromia osoby, proti ktorej sú použité. Dôležitá je precízna právna úprava podmienok ich použitia a nakladania s takto získanými informáciami. Medzi najviac využívané informačno-technické prostriedky v trestnom konaní patrí odpočúvanie a záznam telekomunikačnej prevádzky. Ako už bolo uvedené inštitút je možné použiť aj v trestnom konaní vedenom proti právnickej osobe. Predstavuje jeden z najintenzívnejších zásahov do základných ľudských práv a slobôd a na jeho použitie sa kladú vysoké právne nároky. Komunikácia prostredníctvom telekomunikačnej prevádzky, telefónnej a internetovej je jedným z hlavných prostriedkov medziľudskej výmeny informácií. Telefonovanie prostredníctvom mobilnej siete je možné v súčasnosti považovať za najrozšírenejší verbálny kontakt ľudí s okolitým svetom. Jeho prostredníctvom je možné zachytiť významné informácie, ktoré by sa iným spôsobom získať nedali, alebo by sa získavali len veľmi ťažko.

⁸ MEDELSKÝ, J., 2016. Trestná zodpovednosť právnických osôb. Plzeň: Aleš Čeněk. 2016. s. 185.

Právny rámec odpočúvania v Slovenskej republike tvorí najmä zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov a zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov v znení neskorších predpisov (ďalej iba „zákon o ochrane pred odpočúvaním“). Pre uvedené zákony je spoločné, že ide o uskutočňovanie odpočúvania verejnou mocou utajovaným spôsobom. Trestný poriadok upravuje použitie odpočúvania v trestnom konaní a zákon o ochrane pred odpočúvaním upravuje odpočúvanie mimo trestného konania. V trestnom konaní sa inštitút odpočúvania využíva ako efektívny nástroj na odhaľovanie niektorých závažnejších foriem kriminality. V súvislosti s jeho využitím v trestnom konaní vedenom proti právnickej osobe bude situácia o čosi komplikovanejšia. Z dôvodu, že TZPO neobsahuje osobitné ustanovenia o použití odpočúvania a záznamu telekomunikačnej prevádzky podporne sa na konanie vedené proti právnickým osobám použije všeobecná úprava uvedená v Trestnom poriadku.

Trestné konanie je síce vedené proti právnickej osobe, ale invazívny zásah do súkromia prostredníctvom odpočúvania je smerovaný voči konkrétnym fyzickým osobám. Preto aj pri využití inštitútu odpočúvania a záznamu telekomunikačnej prevádzky v trestnom konaní vedenom proti právnickej osobe treba striktnie dbať na dodržiavanie všetkých garantovaných ľudských práv a slobôd osôb, ktoré sú jeho použitím dotknuté.

Z existujúcej judikatúry Európskeho súdu pre ľudské práva (ďalej len „ESLP“) je nesporné, že odpočúvaním sa zasahuje do práva na súkromie. Pritom nejde iba o zásah do práva na súkromie užívateľa odpočúvanej stanice, ale právo na rešpektovanie súkromného života pri telefonickom odpočúvaní patrí aj ďalším na veci nezúčastneným osobám, ktoré s dotknutou osobou komunikujú, sú z linky volané, resp. na takúto odpočúvanú linku volajú. Právo na súkromie je v demokratickej spoločnosti garantované na vnútroštátnej aj medzinárodnej úrovni. Ústava SR⁹ garantuje v čl. 22 ods. 1 ochranu listového tajomstva, tajomstva dopravovaných správ, a iných písomností a ochranu osobných údajov, v čl. 22 ods. 2 je uvedené, že nikto nesmie porušiť listové tajomstvo ani tajomstvo iných písomností a záznamov, či už uchovávaných v súkromí, alebo zasielaných poštou, alebo iným spôsobom, výnimkou sú prípady, ktoré ustanoví zákon. Rovnako sa zaručuje tajomstvo správ podávaných telefónom, telegrafom alebo iným podobným zariadením. Významným prameňom ochrany ľudských práv je Európsky dohovor o ochrane ľudských práv a základných slobôd (ďalej len Dohovor). Podľa čl. 8 ods. 1 Dohovoru, každý má právo na rešpektovanie svojho súkromného a rodinného života, obdobia a korešpondencie. Štátny orgán nemôže do práva na súkromie zasahovať okrem prípadov, keď je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom a zločinnosti, ochrany zdravia alebo morálky alebo ochrany práv a slobôd iných. Touto ochranou sa právo na súkromný a rodinný život priznáva vo väčšom rozsahu ako podľa Ústavy SR, ktorá chráni súkromie, iba dokiaľ ho neobmedzí zákon. Dohovor umožňuje obmedziť súkromie iba z niektorého výslovne určeného dôvodu legitímneho záujmu. Odpočúvanie telefonických hovorov predstavuje v zmysle ustálenej judikatúry ESLP vážny zásah do práva na rešpektovanie súkromného života, ako aj práva na rešpektovanie korešpondencie. Ochrana súkromia zaručená Dohovorom sa vzťahuje nielen na záznam takejto odpočúvanej komunikácie, ale aj na nakladanie so získanými dátami a neskôr aj ich prípadné zničenie. „Súd nerobí rozdiely medzi súkromnými telefonátmi a pracovnými telefonátmi. Sú teda rovnako chránené aj rozhovory uskutočnené na linke zamestnávateľa,

⁹ Zákon č. 460/1992 Zb. Ústava Slovenskej republiky.

na služobných telefónnych linkách, na interných telefónnych okruhoch v úradoch, podnikoch a pod.“¹⁰

Právo na rešpektovanie súkromného života pri telefonickom odpočúvaní patrí každému účastníkovi telefonického rozhovoru rovnako tomu ktorého telefónna stanica je odpočúvaná, aj tomu kto je z tejto stanice volaný, alebo na ňu volá.¹¹

Dohovor priznáva práva a poskytuje ochranu každému, kto podlieha jurisdikcii vysokých zmluvných strán, nerozlišuje medzi fyzickými a právnickými osobami a práva, ktoré obsahuje priznáva všetkým. Jedinou výnimkou je, ak z povahy konkrétneho práva nevyplýva, že môžu byť priznané len fyzickej osobe. „Podľa kolektívu autorov“¹² nebolo úmyslom obmedziť možnosť dovolávať sa práv a slobôd podľa Dohovoru len pre fyzické osoby. Je však samozrejmosťou, že právnické osoby sa nemôžu dovolávať takých práv, ako je právo na život alebo právo na zdravie. Sťažovať sa nemôžu právnické osoby, ktoré nie sú dostatočne nezávislé od štátu.“¹³ Z uvedeného je nesporné, že ochrana práv Dohovorom sa priznáva za určitých okolností aj právnickým osobám. V nadväznosti na článok 8 ods. 1 je možné skonštatovať, že právo na rešpektovanie súkromia a korešpondencie sa právnickej osobe nepochybne priznáva. Pri odpočúvaní právnickej osoby sa ochrana súkromia poskytuje každému účastníkovi telefonického rozhovoru, bez ohľadu na to, či používa vlastnú (súkromnú) alebo cudziu (služobnú) telefónnu linku.

Niektoré právnické osoby v súvislosti s výkonom ich činnosti disponujú osobnými údajmi a informáciami o konkrétnych fyzických osobách. Všetky informácie, ktorými disponuje právnická osoba tvoria súčasť jej súkromia. Orgány verejnej moci musia pri každom úkone postupovať iba na základe zákona a zákonným spôsobom. Pri zásahu do práva na súkromie právnickej osoby prostredníctvom odpočúvania musia štátne orgány nakladať so získanými informáciami v súlade so zákonom a neustále dbať aby nedochádzalo k neoprávnenému zásahu do práv všetkých dotknutých fyzických osôb. Ako príklad možno uviesť advokátske kancelárie disponujúce rôznymi údajmi a informáciami o svojich klientoch, prípadne súkromné zdravotnícke zariadenia, ktoré držia zdravotnú dokumentáciu svojich pacientov. Ochrana osobných údajov tvorí neoddeliteľnú súčasť práva na rešpektovanie súkromia patriaceho medzi základné práva a slobody fyzických osôb garantované Ústavou SR, podľa ktorej „Každý má právo na ochranu pred neoprávneným zasahovaním do súkromného a rodinného života.“ a „Každý má právo na ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe.“ Osobnými údajmi vo všeobecnosti možno vnímať všetky údaje, informácie a charakteristické znaky, ktoré sú spôsobilé človeka identifikovať. Identitu človeka tak možno vnímať ako hodnotu, ktorá nás po celý život sprevádza na každom kroku, či už v súkromnom alebo pracovnom živote, vo vzťahu k orgánom verejnej správy alebo tretiemu sektoru.

Právo na súkromie nie je právom absolútnej povahy, je možné ho obmedziť za určitých podmienok. K obmedzeniu zo strany štátneho orgánu môže dôjsť iba na základe zákona, pokiaľ ide o zásah nevyhnutný v demokratickej spoločnosti a smerujúci k uskutočneniu legitímneho cieľa, a súčasne musí byť primeraný. Pri uskutočňovaní odpočúvania v trestnom konaní sú postavené proti sebe dve práva, právo jednotlivca príp. právnickej osoby na ochranu jeho súkromia na

¹⁰ KYJAC, Z., 2015. Použitie informačno-technických prostriedkov v trestnom konaní. Odpočúvanie a záznam telekomunikačnej prevádzky. Bratislava: Wolters Kluwer. 2015. s. 42.

¹¹ Rozsudok ESEP vo veci Huvig vs. Francúzsko z 24. apríla 1990, č. 11105/84.

¹² KMEC, J., KOSÁŘ, D., KRATOCHVÍL, J., BOBEK, M., 2012. Evropská úmluva o lidských právech. Komentář. 1. vyd. Praha: C. H. Beck. 2012.

¹³ MEZEI, M., 2015. Odpočúvanie právnickej osoby. In: Zborník z medzinárodnej vedeckej konferencie doktorandov a mladých vedeckých pracovníkov organizovanej Univerzitou Komenského v Bratislave, Právnickou fakultou, v dňoch 19.–21. 3. 2015 v priestoroch ÚZ NR SR Častá-Papiernička. Mílniky práva v stredoeurópskom priestore 2015. Bratislava: Univerzita Komenského, Právnická fakulta. 2015. s. 344.

jednej strane a záujem spoločnosti na ochrane pred trestnou činnosťou na strane druhej. Zasahovanie štátu do práv osôb musí vždy rešpektovať spravodlivú rovnováhu medzi verejným záujmom a ochranou práv jednotlivca.

Na účely ochrany práva na súkromný život ESLP zdôraznil, že právna úprava každého štátu musí vymedziť jasné a podrobné pravidlá upravujúce rozsah a použitie opatrení zasahujúcich do práva na súkromie, určiť minimálne požiadavky na ich dĺžku, spôsob uloženia takto získaných informácií a údajov, ich použitie, prístup tretích osôb k nim ako aj úpravu procedúry ich zničenia, a to spôsobom, aby jednotlivci disponovali dostatočnými zárukami proti riziku ich zneužitia a svojvoľe. ESLP určil minimálne záruky, ktoré by mali byť stanovené vo vnútroštátnom predpise, aby sa zamedzilo možnosti zneužitia právomoci príslušného orgánu. „Ide o podmienku definície osôb, ktorých telefón môže byť odpočúvaný na základe súdneho príkazu, druh trestného činu, ktorý môže dať podnet k takému príkazu, časové obmedzenie telefónneho odpočúvania, postup pre spísanie súhrnnej správy obsahujúcej odpočúvané hovory, opatrenia, ktoré je potrebné urobiť, aby prenos kaziet zostal neporušený a kompletný pre prípadné preskúmanie sudcom a obhajobou a tiež okolnosti, za ktorých môžu, ale nemusia byť nahrávky vymazané alebo pásky zničené, najmä vtedy, ak bol obvinený zbavený obžaloby vyšetrojúcim sudcom alebo súdom.“¹⁴

Z hľadiska zásahov do práva na súkromie je veľmi dôležitá rozhodovacia činnosť Európskeho súdu pre ľudské práva a Ústavného súdu Slovenskej republiky. Pri zásahoch do práva na súkromie sa predovšetkým skúma, či daný skutkový stav možno *ratione materiae* považovať za súčasť práva na súkromie. Po kladnej odpovedi na túto otázku treba skúmať či zásah bol legálny, legitímny a proporcionálny. Kritériá sa posudzujú v určitej postupnosti. Najskôr sa skúma, či zásah bol legálny. Kritérium legality znamená posúdenie, či zásah orgánu verejnej moci do práva bol vykonaný na základe zákona a v súlade so zákonom. Vyžaduje sa určitá kvalita zákona. Zákon musí byť dostupný, presný a dostatočne jasný dotknutej osobe. Dôležitá je požiadavka na predvídateľnosť zákona, ktorý by mal poskytovať osobám zodpovedajúce údaje o okolnostiach a podmienkach, za ktorých sú orgány verejnej moci oprávnené použiť takýto zásah.¹⁵ V súvislosti s uvedeným je vhodné uviesť rozhodnutie Ústavného súdu SR, v ktorom je upravené kritérium legality: „Štát môže zasiahnuť do práva na súkromie len vtedy, ak takýto zásah zákon pripúšťa a právna norma ho upravuje dostatočne jasne na to, aby bol za ustanovených podmienok predvídateľný.“¹⁶ Ako ďalšie sa skúma kritérium legitimacy zásahu do práva na súkromie. Jeho predmetom je posúdenie, či opatrenie umožňujúce zásah verejnej moci do tohto práva je v súlade s cieľmi taxatívne uvedenými v Dohovore v čl. 8 ods. 2. Zásah do práva na súkromie je prípustný len v prípadoch, ak je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom a zločinnosti, ochrany zdravia alebo morálky, alebo ochrany práv a slobôd iných. Nakoniec sa skúma, či zásah do práva na súkromie bol proporcionálny. Takým je zásah iba vtedy, ak je v demokratickej spoločnosti nevyhnutný a sledovaný cieľ nemožno dosiahnuť miernejšími prostriedkami. „Súd skúma, či sú zákonné opatrenia štátu prijímané z dôvodu ochrany jeho legitímnych záujmov primerané sledovanému cieľu. Proportionalita musí byť dodržaná vo vzťahu medzi právom na súkromie jednotlivca a výberom prostriedkov, ktorý-

¹⁴ STRÁŽNICKÁ, V., a kol., 2013. Medzinárodná a európska ochrana ľudských práv. Bratislava: Eurokódex. 2013. s. 400.

¹⁵ ČENTĚŠ, J., LAZAREVA, N., 2012. Legalita, legitimita a proportionalita odpočúvania a zaznamenávania telekomunikačnej prevádzky. In: *Magister Officiorum* (odborný časopis Učenej právnickej spoločnosti), roč. II, č. 2/2012. s. 17.

¹⁶ Rozhodnutie Ústavného súdu, II. ÚS 280/09.

mi štát disponuje pri plnení legitímneho cieľa.¹⁷ Základným kritériom proporcionality teda je nevyhnutnosť takéhoto zásahu v demokratickej spoločnosti. Ak na niektoré z uvedených kritérií je odpoveď záporná, ďalej sa v skúmaní problematiky nepokračuje a konštatuje sa porušenie článku 8 Dohovoru, t. j. práva na rešpektovanie súkromného života.

„Odpočúvanie verejnou mocou je vážnym obmedzením základných práv, najmä práva na súkromie. Pokiaľ právny poriadok pripúšťa zásah do týchto práv, deje sa tak v záujme ochrany spoločnosti, prípadne v záujme ústavne zaručených základných práv iných osôb. Prípustný je iba taký zásah do základných práv, ktorý je nevyhnutný, daný verejným (všeobecným) záujmom na ochrane spoločnosti pred trestnými činmi, ako aj tým, aby takéto činy boli zistené a aby ich páchatelia boli spravodlivo potrestaní; prípadne zásah zabezpečujúci bezpečnosť štátu, obranu štátu, predchádzanie a objasňovanie trestnej činnosti, ochranu práv a slobôd iných.“¹⁸

Vykonávanie odpočúvania a záznamu telekomunikačnej prevádzky pri dokazovaní trestnej činnosti právnických osôb

Ako sme už v predchádzajúcich častiach uviedli, z dôvodu absencie špeciálnej úpravy v TZPO, právnym predpisom upravujúcim vymedzenie, podmienky, subjekt a spôsob odpočúvania a záznamu telekomunikačnej prevádzky pri dokazovaní trestnej činnosti právnickej osoby bude Trestný poriadok.

„Odpočúvanie a záznam telekomunikačnej prevádzky je trestno-procesný inštitút umožňujúci zaznamenávať telefonické hovory a iné skutočnosti oznamované prostredníctvom elektronickej komunikačnej siete, ak sú svojim obsahom významné pre trestné konanie.“¹⁹ Je zameraný na zachytávanie, zisťovanie a dokumentovanie komunikácie realizovanej prostredníctvom elektronických komunikačných sietí. Obsahom komunikácie je prenos alebo vymieňanie informácií medzi rôznymi subjektmi. Ide o komunikáciu fyzických osôb, ich telefonické rozhovory prostredníctvom mobilnej alebo pevnej telekomunikačnej siete, telefonovanie cez internet, textové správy, elektronickú poštu, faxovú komunikáciu, rádiokomunikáciu a akúkoľvek dátovú komunikáciu. Podstatou tohto inštitútu je účelové vnímanie a zaznamenávanie aktuálne prebiehajúcej komunikácie účastníkov telekomunikačnej prevádzky tretím subjektom, ktoré je sprostredkované telekomunikačným zariadením.²⁰ V prípade jeho použitia štátny orgán získava informácie z elektronickej telekomunikačnej siete alebo elektronickej komunikačnej služby a nie z technického prostriedku, ktorý bol použitý na vytvorenie alebo prijatie informácie. Ak dotknutá osoba informáciu iba vytvorila a nikam nedistribuovala, v trestnom konaní by sa takéto informácie získavali prostredníctvom inštitútu uchovanie a vydanie počítačových údajov podľa § 90 TP.

Záznamom telekomunikačnej prevádzky sa rozumie jednak zaznamenávanie takto vnímanej komunikácie prebiehajúcej v telekomunikačnej prevádzke na dátový nosič, ktorý umožní uchovanie komunikácie a reprodukciu zachytenej komunikácie v budúcnosti, a jednak to, čo nosič obsahuje.²¹

¹⁷ STRÁŽNICKÁ, V., a kol., 2013. Medzinárodná a európska ochrana ľudských práv. Bratislava: Eurokódex. 2013. s. 372–373.

¹⁸ ČENTĚŠ, J., 2013. Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. Bratislava: C. H. Beck. 2013. s. 36.

¹⁹ IVOR, J., a kol., 2010. Trestné právo procesné. Druhé doplnené a prepracované vydanie. Bratislava: Iura Edition. 2010. s. 403.

²⁰ ČENTĚŠ, J., LAZAREVA, N., 2012. Legalita, legitimita a proporcionality odpočúvania a zaznamenávania telekomunikačnej prevádzky. In: Magister Officiorum (odborný časopis Učenej právnickej spoločnosti), roč. II, č. 2/2012. s. 19.

²¹ NOVOTNÁ, J., 2003. K některým otázkám dokazování odposlechem a záznamem telekomunikačního provozu, In: Trestněprávní revue, 2003, č. 10, s. 291.

„Odpočúvanie a záznam telekomunikačnej prevádzky vykonáva utajeným spôsobom príslušný útvar PZ a to za použitia technických na tieto účely určených prostriedkov a zariadení.“²²

Ustanovenie § 115 TP stanovuje podmienky a pravidlá využitia tohto inštitútu, definovaný je tu okruh trestných činov pri ktorých je možné odpočúvanie použiť. Zákonné podmienky na využitie odpočúvanie a záznamu telekomunikačnej prevádzky sú v zmysle § 115 ods. 1 TP nasledovné:

- existencia trestného konania – konania podľa Trestného poriadku (§ 10 ods. 15 TP)
- existencia taxatívne uvedeného trestného činu ako predmetu trestného konania. Musí ísť o zločin, korupciu, trestné činy extrémizmu, zneužívanie právomoci verejného činiteľa, legalizáciu príjmu z trestnej činnosti alebo pre iný úmyselný trestný čin, o ktorom na konanie zaväzuje medzinárodná zmluva.
- dôvodný predpoklad, že budú zistené skutočnosti významné pre trestné konanie.
- ak nemožno sledovaný účel dosiahnuť inak alebo ak by bolo jeho dosiahnutie iným spôsobom podstatne sťažené.
- predmetom odpočúvania nesmie byť komunikácia medzi obvineným a advokátom, ak ho zastupuje v konkrétnej trestnej veci ako jeho obhajca.²³

Drvivá väčšina odpočúvaní, vzhľadom aj na jeho charakter prebieha v predsúdnej časti konania, v postupe pred začatím trestného stíhania a v prípravnom konaní. Pre odhaľovanie trestnej činnosti právnických osôb bude pravdepodobne veľmi často odpočúvanie využívané pred začatím trestného stíhania, v takomto prípade bude dôležité preukázanie dôvodného podozrenia, že bol spáchaný jeden z uvedených trestných činov. „S prihliadnutím na zákoné podmienky tohto inštitútu možno dôvodne predpokladať, že v rámci tohto štádia trestného konania sa spravidla vyžaduje podanie trestného oznámenia a existencia informácií, z ktorých vyplýva podozrenie zo spáchania trestného činu uvedeného v § 115 ods. 1 TP.“²⁴ Je neprípustné využívať takýto prostriedok na dodatočné zabezpečovanie podkladov na dôvodnosť podozrenia zo spáchaného trestného činu. Začatím vykonávania odpočúvania pred začatím trestného stíhania sa začína trestné stíhanie, orgán činný v trestnom konaní vydá ihneď uznesenie o začatí trestného stíhania s uvedením úkonu, ktorým sa trestné stíhanie začalo.

Právnická osoba, ktorá má byť obvinená z niektorého z okruhu uvedených trestných činov sa stáva subjektom trestno-procesných vzťahov a nadobúda rozsah trestno-procesných práv a povinností.

Odpočúvanie a záznam telekomunikačnej prevádzky je možné vykonávať výhradne iba na základe príkazu vydaného príslušným orgánom. Kto je oprávnený vydať takýto príkaz je priamo závislé od štádia trestného konania v ktorom sa trestná vec nachádza.

V postupe pred začatím trestného stíhania a v prípravnom konaní je na vydanie príkazu oprávnený:

- sudca pre prípravné konanie len na návrh prokurátora,
- prokurátor iba v prípadoch, ak ide o vec, ktorá neznesie odklad a príkaz sudcu pre prípravné konanie nemožno získať vopred. Príkaz vydaný na odpočúvanie a záznam telekomunikačnej prevádzky vydaný prokurátorom nesmie byť spojený so vstupom do obydľia. Takýto príkaz má predbežný charakter, musí ho do 24 hodín od jeho vydania potvrdiť sudca pre prípravné konanie, inak stráca platnosť a informácie ním získané nemožno použiť v trestnom konaní ako dôkaz a musia byť zničené bez meškania predpísaným postupom.

²² ZÁHORA, J., a kol., 2013. Dokazovanie v trestnom konaní. Praha: LEGES, 2013. s. 256.

²³ ČENTĚŠ, J., a kol., 2015. Trestný poriadok. Veľký komentár. 2. aktualizované vydanie. Bratislava: EUROKÓDEX. 2015. s. 316.

²⁴ ČENTĚŠ, J., 2013. Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. Bratislava: C. H. Beck. 2013. s. 99.

V konaní pred súdom príkaz vydáva predseda senátu, ktorý má právomoc ho vydať z úradnej povinnosti, bez návrhu prokurátora.²⁵

V súvislosti s oprávnením prokurátora vydať príkaz na odpočúvanie pred začatím trestného stíhania a v prípravnom konaní, iba za predpokladu, ak sa nejedná o úkon spojený so vstupom do obydlija je vhodné poznamenať, že právnická osoba obydlie ako také nemá. Definíciu pojmu obydlie môžeme nájsť v ustanovení § 99 ods. 1 TP „Domovú prehliadku možno vykonať, ak je dôvodné podozrenie, že v byte alebo inom priestore slúžiacom na bývanie alebo v priestoroch k nim patriaci (ďalej len ‚obydlie‘) je vec dôležitá pre trestné konanie alebo, že sa tam skrýva osoba podozrivá zo spáchania trestného činu...“. Obydlie je definované tiež v ustanovení § 122 ods. 5 TZ: „Trestný čin je spáchaný v obydlí, ak je spáchaný v dome alebo byte iného alebo v iných priestoroch slúžiacich na bývanie, vrátane priestorov a pozemkov k nim patriacich, ak sú ako súčasť obydlija uzavreté.“ Zásah do domovej slobody právnickej osoby neprichádza do úvahy, nakoľko právnická osoba obydlie nemá. Právnická osoba môže disponovať a vlastníť určitý majetok. V prípade nutnosti prehliadky priestorov, ktoré právnická osoba vlastní sa postupuje nasledovne. V prípade prehliadky priestorov, ktoré neslúžia na bývanie, ide najmä o kancelárie právnickej osoby, sklady prípadne motorové vozidlá právnickej osoby sa postupuje podľa § 101 TP, vydáva sa príkaz na prehliadku iných priestorov a pozemkov. V prípade, ak právnická osoba vlastní priestory slúžiace na bývanie, je nutné vydať klasický príkaz na domovú prehliadku podľa § 100 TP, ktorý bude smerovať voči osobe, ktorá dom alebo byt užíva a to bez ohľadu na to, že vlastníkom bytu alebo domu je právnická osoba.²⁶

Trestný poriadok v ustanovení § 115 ods. 3 stanovuje, že príkaz na odpočúvanie a záznam telekomunikačnej prevádzky sa musí vydať písomne a odôvodniť aj skutkovými okolnosťami, a to osobitne pre každú účastnícku stanicu alebo zariadenie. V prípade trestného stíhania právnických osôb je situácia komplikovanejšia. Niektoré právnické osoby disponujú veľkým počtom účastníckych staníc. V určitých prípadoch ide o desiatky príp. aj stovky účastníckych staníc, ktoré využívajú jednotliví zamestnanci právnickej osoby. Príkaz na odpočúvanie musí byť vydaný pre každú účastnícku stanicu alebo zariadenie osobitne a musí obsahovať okrem všeobecných náležitostí upravených v § 181 ods. 1 TP aj nasledovné špecifické náležitosti podľa § 115 ods. 3 TP:

- a.) určenie účastníckej stanice alebo zariadenia, najčastejšie telefónnym číslom
- b.) určenie osoby, ak je známa, ktorej sa odpočúvanie a záznam telekomunikačnej prevádzky týka. „Príkaz by mal byť v zásade individualizovaný vo vzťahu ku konkrétnej osobe, ktorá je buď majiteľom, resp. užívateľom účastníckej stanice alebo zariadenia.“²⁷
- c.) určenie času vykonávania odpočúvania
- d.) odôvodnenie, a to aj skutkovými okolnosťami.²⁸ Odôvodnenie by malo byť konkrétne, jasné a presné, aby nepripúšťalo žiadne pochybnosti a aby takéto rozhodnutie a následne aj využitie tohto inštitútu mohlo byť preskúmateľné z hľadiska zákonnosti.

V súvislosti s vydaním príkazu na odpočúvanie právnickej osoby narážame na viaceré problémy. Je neprijateľné a dovoľím si tvrdiť, že v praxi aj nereálne, aby v prípade vydania príkazu na odpočúvanie právnickej osoby boli odpočúvané paušálne t. j. všetky účastnícke stanice registro-

²⁵ ČENTĚŠ, J., a kol., 2015. Trestný poriadok. Veľký komentár. 2. aktualizované vydanie. Bratislava: EUROKÓDEX. 2015. s. 317.

²⁶ ŠAMKO, P., 2016. Niekoľko poznámok k trestnej zodpovednosti právnických osôb. Dostupné na internete: <http://www.pravnelisty.sk/clanky/a466-poznamky-k-zakonu-o-trestnej-zodpovednosti-pravnickych-osob-2016>.

²⁷ KYJAC, Z., 2015. Použitie informačno-technických prostriedkov v trestnom konaní. Odpočúvanie a záznam telekomunikačnej prevádzky. Bratislava: Wolters Kluwer. 2015. s. 150.

²⁸ ČENTĚŠ, J., a kol., 2015. Trestný poriadok. Veľký komentár. 2. aktualizované vydanie. Bratislava: EUROKÓDEX. 2015. s. 317.

vané na právnickú osobu, z dôvodu podozrenia zo spáchania trestného činu právnickou osobou. V takomto prípade by nepochybne išlo o neprimerané zasahovanie do práva na súkromie všetkých zúčastnených osôb a z toho vyplývajúce porušenie čl. 8 Dohovoru. Pre každú odpočúvanú stanicu musí existovať konkrétny dôvod na použitie tohoto inštitútu.

Pred vydaním príkazu na odpočúvanie právnickej osoby je potrebné zbieranie informácií o právnickej osobe za účelom zistenia okruhu osôb, ktorých konanie by mohlo byť právnickej osobe pričítané. V zmysle § 4 ods. 1 TZPO je trestný čin spáchaný právnickou osobou, ak je spáchaný v jej prospech, v jej mene, v rámci jej činnosti alebo jej prostredníctvom, ak konal:

- a.) štatutárny orgán alebo člen štatutárneho orgánu
- b.) ten, kto vykonáva kontrolnú činnosť alebo dohľad v rámci právnickej osoby, alebo
- c.) iná osoba, ktorá je oprávnená zastupovať právnickú osobu alebo za ňu rozhodovať.

Trestný čin je spáchaný právnickou osobou aj vtedy, ak jedna z vyššie uvedených osôb nedostatočným dohľadom alebo kontrolou, ktoré boli jej povinnosťou, hoci z nedbanlivosti umožnila spáchať trestný čin osobou, ktorá konala v rámci oprávnení, ktoré jej boli zverené právnickou osobou. Len konanie tu uvedených osôb sa považuje za konanie samotnej právnickej osoby a je relevantné ohľadne vyvedenia trestnej zodpovednosti právnickej osoby. Z uvedeného dôvodu je dôležitý príkaz na odpočúvanie a záznam telekomunikačnej prevádzky obmedziť najmä na okruh osôb, ktoré tvoria vôľu samotnej právnickej osoby a na osoby u ktorých je dôvodný predpoklad, že ich odpočúvaním je možné získať informácie dôležité pre trestné konanie. Predpokladáme, že takéto operatívne zisťovanie a identifikácia takýchto osôb bude dosť v praxi dosť komplikovaná. Odpočúvaním príliš širokého okruhu osôb a s ním spojeného získania nadmerného množstva informácií, ktoré neobsahujú relevantné informácie o trestnom čine by bolo neúčelné a v praxi iba veľmi ťažko realizovateľné. V právnických osobách je tiež bežné, že určité telefónne číslo využívajú viacerí zamestnanci, mobilný telefón, príp. aj pevná linka nie je pridelená konkrétnemu zamestnancovi, ale tomu, kto vykonáva v tom čase službu, preto treba dôsledne dbať, aby nedochádzalo k neprimeranému zásahu do práva na súkromie vysokému počtu osôb a zvážiť či by sa informácie nedali zistiť iným menej invazívnym spôsobom.

Príslušníci Policajného zboru by mali operatívnou činnosťou postupne zistiť, ktoré konkrétne telefónne čísla používajú osoby, ktoré tvoria vôľu právnickej osoby a postupne zúžiť okruh len na tie účastnícke stanice alebo zariadenia osôb, u ktorých je dôvodný predpoklad, že páchajú trestnú činnosť v mene právnickej osoby.

Označenie osoby, ktorá má byť odpočúvaná pritom predpokladá uvedenie jej mena, priezviska, adresy bydliska, prípadne aj zamestnania a ďalších potrebných identifikačných údajov.²⁹

Pri odpočúvaní pevných liniek právnickej osoby je situácia zložitejšia. Pevné linky právnickej osoby bývajú veľmi často zabezpečené tak, že právnická osoba má pridelené iba jedno konkrétne telefónne číslo a ostatné zariadenia majú iba vlastnú klapku.³⁰ Ak by bolo potrebné odpočúvať takúto linku, museli by sa odpočúvať všetky zariadenia naraz, čo je taktiež v rozpore so zásadou primeranosti a zdržanlivosti a nepochybne by došlo k zásahu do súkromia veľkého počtu osôb. A nemožno opomenúť ani fakt, že odpočúvanie je vykonávané špeciálnym technickým automatickým zariadením, ktoré komunikáciu účastníkov telekomunikačnej prevádzky zaznamenáva. Komunikáciu začne nahrávať v okamihu, keď sa v účastníckej stanici začne hovoriť.³¹ V takýchto

²⁹ Nález Ústavného súdu ČR z 23. mája 2007, sp. zn. II. ÚS 615/06.

³⁰ MEZEI, M., 2015. Odpočúvanie právnickej osoby. In: Zborník z medzinárodnej vedeckej konferencie doktorandov a mladých vedeckých pracovníkov organizovanej Univerzitou Komenského v Bratislave, Právnickou fakultou, v dňoch 19.–21. 3. 2015 v priestoroch ÚZ NR SR Častá-Papiernička. Mílniky práva v stredoeurópskom priestore 2015. Bratislava: Univerzita Komenského, Právnická fakulta. 2015. s. 349.

³¹ ČENTĚŠ, J., 2013. Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. Bratislava: C. H. Beck. 2013. s. 105.

prípadoch by bol objem zaznamenaných informácií veľmi veľký. Nahrať záznam je až následne vypočítaný príslušníkmi Policajného zboru a vyhodnotený. Takáto činnosť zaberie množstvo času a je náročná nielen na personálne, ale aj na technické zabezpečenie. Je ťažké si čo i len predstaviť, aké by muselo byť odôvodnenie príkazu na odpočúvanie takejto linky, aby sudca pre prípravné konanie alebo predseda senátu jeho využitie schválil.

V súvislosti s nutnosťou riadneho odôvodnenia príkazu na odpočúvanie je vhodné spomenúť rozhodovaciu činnosť Ústavného súdu, ktorý vo svojich rozhodnutiach poukázal na jeho dôležitosť v súvislosti so základným právom na súdnu ochranu podľa čl. 46 ods. 1 Ústavy SR a s právom na spravodlivé súdne konanie podľa čl. 6 ods. 1 Dohovoru, ktorých obsahom je: „Právo účastníka konania, procesnej strany v konaní alebo právo inej zainteresovanej osoby na rozhodnutie, ktorého dôvody vydania sú zjavné a zreteľné, pretože práve odôvodnenie rozhodnutia je zárukou toho, že výkon spravodlivosti nebude arbitrárny.“³²

V ustanovení § 115 ods. 5 TP je uvedená možnosť využiť odpočúvanie a záznam telekomunikačnej prevádzky aj pre iný úmyselný trestný čin ako je uvedený v ods. 1. V takomto prípade je jeho využitie možné iba v prípade, ak užívateľ odpočúvaného alebo zaznamenávaného zariadenia dá na jeho použitie súhlas. Tu sa dostávame k ďalšej spornej otázke, kto v prípade odpočúvania právnickej osoby by mal takýto súhlas udeliť, ak je jedna účastnícka stanica alebo zariadenie využívané väčším množstvom zamestnancov právnickej osoby. Ktorá osoba bude kompetentná a oprávnená takýto súhlas vydať? Štatutárny orgán právnickej osoby určite nie. Vydanie súhlasu iba jedného užívateľa stanice, ktorú na pracovisku užívajú viacerí zamestnanci by bolo tiež v rozpore s týmto ustanovením. Aby bolo možné postupovať podľa § 115 ods. 5 TP je nutné zistiť všetkých užívateľov konkrétnej stanice, ktorá má byť takýmto spôsobom odpočúvaná a vyžiadať si ich súhlas. Predpokladáme, že v praxi takýto prípad nebude častý.

Snahou napomôcť dokazovaniu a objasňovaniu najzávažnejšej trestnej činnosti je zakotvenie možnosti použitia záznamu z odpočúvania ako dôkazu v trestnom konaní v inej trestnej veci, ako tej v ktorej bolo zákonným spôsobom nariadené a vykonané odpočúvanie. V zmysle § 115 ods. 7 TP takto získané dôkazy je možné v inej trestnej veci použiť len vtedy, ak sa súčasne aj v tejto trestnej veci vedie trestné konanie pre trestný čin uvedený v ods. 1. Predmetné ustanovenie spôsobuje nemalé ťažkosti v aplikačnej praxi aj z dôvodu nejednotného výkladu tohto ustanovenia Najvyšším súdom SR. Sporným je najmä vykládanie požiadavky súčasného vedenia trestného stíhania v inej trestnej veci. V odborných publikáciách autori zaujímajú tiež odlišné stanoviská k uvedenej problematike. Prvým z názorov je, že možnosť použitia záznamu ako dôkazu v inom trestnom konaní sa nevzťahuje k okamihu vykonávania odpočúvania (samotné technické prevádzkanie), ale až na okamih využitia jeho výsledku ako dôkazu v trestnom konaní, pretože ak by sa ustanovenie vykládalo opačne znamenalo by to vylúčenie použitia tohto ustanovenia na rozhodujúcu väčšinu závažných trestných vecí v praxi a pri mnohých prípadoch závažnej trestnej činnosti by sa takýto záznam nedal využiť ako dôkaz. Opačný názor oponuje, že príslušný orgán pri odpočúvaní by už mal disponovať určitým poznatkom o trestnej činnosti. Ak by tak nebolo mohlo by dôjsť k nekontrolovateľnému a hromadnému odpočúvaniu občanov.

V súvislosti s odpočúvaním právnických osôb je dôležité pripomenúť, že vyvodenie trestnej zodpovednosti právnickej osobe nie je závislé ani podmienené vyvodením trestnej zodpovednosti konkrétnej fyzickej osobe. V prípade, ale ak sa zistí konkrétna fyzická osoba, ktorá sa dopustila protiprávneho konania, ktoré môže byť právnickej osobe pričítané, trestné stíhanie sa bude viesť súbežne proti právnickej aj proti fyzickej osobe.

³² Nález Ústavného súdu zo 4. februára 2009, sp. zn. I. ÚS 117/07.

Ak sa odpočúvaním právnickej osoby zistia skutočnosti odôvodňujúce vzniesť obvinenie fyzickej osobe, takéto výsledky odpočúvania môžu byť použiteľné na vznesenie obvinenia konkrétnej fyzickej osobe. Bude sa tak postupovať v situáciách, ak pôjde o tú istú trestnú vec, v ktorej je vedené trestné stíhanie vo veci podozrenia zo spáchania trestného činu právnickou osobou a pri jej odpočúvaní sa zistí protiprávne konanie konkrétneho štatutárneho orgánu, ktorý sa dopúšťa trestného činu v mene právnickej osoby, v jej prospech, v jej záujme alebo jej prostredníctvom. V takomto prípade nič nebude brániť tomu, aby sa výsledky odpočúvania použili na vznesenie obvinenia nielen právnickej osobe, ale aj konkrétnej fyzickej osobe. Ak pôjde o zhodne skutkovo vymedzenú vec a trestné stíhanie sa bude viesť oddelene, t. j. v samostatných konaniach, výsledky odpočúvania budú využiteľné v oboch paralelne vedených trestných stíhaniach.³³

Záver

Prijatím zákona č. 91/2016 Z. z. sa do nášho právneho poriadku zaviedla možnosť vyvodenia trestnej zodpovednosti právnických osôb a s tým súvisiace priame sankcionovanie právnických osôb prostriedkami trestného práva. Prijatie zákona súviselo najmä s prijatím medzinárodných záväzkov a so zvyšujúcou sa kriminalitou páchanou právnickými osobami. Ich trestná činnosť je veľmi často vykonaná premysleným a ťažko odhaliteľným spôsobom. Keďže zákon o trestnej zodpovednosti žiadne osobitné ustanovenia o dokazovaní neobsahuje, na odhaľovanie a dokazovanie trestnej činnosti právnických osôb sa budú využívať procesné inštitúty upravené Trestným poriadkom. Odhaľovanie a dokazovanie trestnej činnosti právnických osôb bude dosť komplikované. Nápomocný môže byť aj inštitút odpočúvania a záznamu telekomunikačnej prevádzky, využívaný na odhaľovanie najzávažnejších foriem trestnej činnosti. Právnická osoba je umelý subjekt práva, výtvor právneho poriadku, preto aj v prípade vydania príkazu na odpočúvanie v trestnom konaní vedenom proti právnickej osobe zásah do práv je smerovaný voči konkrétnym fyzickým osobám. Väčšina právnických osôb disponuje pomerne veľkým množstvom telefónnych liniek, preto bude potrebné ešte pred vydaním príkazu na odpočúvanie náročné operatívne zisťovanie a stotožňovanie osôb, ktoré užívajú konkrétnu účastnícku stanicu a postupne vyselektovanie okruhu osôb, u ktorých existuje dôvodný predpoklad, že by odpočúvaním ich komunikácie mohli byť zistené skutočnosti významné pre trestné konanie. V prípade vyvodenia trestnej zodpovednosti právnickej osoby musí ísť o konanie osôb, ktoré tvoria vôľu právnickej osoby a takéto ich protiprávne konanie by mohlo byť právnickej osobe pričítané.

Aby sa predišlo komplikáciám súvisiacim s využitím tohto inštitútu v trestnom konaní, je potrebné dôsledne rešpektovať zákonné ustanovenia a splniť všetky zákonné podmienky, ktorých naplnenie je na použitie tohto inštitútu naviazané. Za dodržania zákonných podmienok pri súčasnom rešpektovaní ľudských práv všetkých dotknutých osôb by mohlo využitie inštitútu odpočúvania a záznam telekomunikačnej prevádzky významne napomôcť pri odhaľovaní a dokazovaní trestnej činnosti právnických osôb.

Zoznam použitej literatúry:

ČENTÉŠ, J., 2013. Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. Bratislava: C. H. Beck. 2013. s. 272. ISBN 978-80-89603-09-1

³³ ŠAMKO, P., 2016. Niekoľko poznámok k trestnej zodpovednosti právnických osôb. Dostupné na internete: <http://www.pravnelisty.sk/clanky/a466-poznamky-k-zakonu-o-trestnej-zodpovednosti-pravnickych-osob> 2016.

- ČENTĚŠ, J., a kol., 2015. Trestný poriadok. Veľký komentár. 2. aktualizované vydanie. Bratislava: EUKODEX. 2015. s. 955. ISBN 978-80-8155-057-7
- ČENTĚŠ, J., LAZAREVA, N., 2012. Legalita, legitimita a proporcionalita odpočúvania a zaznamenávania telekomunikačnej prevádzky. In: *Magister Officiorum* (odborný časopis Učenej právnickej spoločnosti), roč. II, č. 2/2012. ISSN 1338-5569
- HURDÍK, J., 2003. Právnické osoby a jejich typologie. 1. vyd. Praha: C. H. Beck, 2003. s. 107. ISBN 80-7179-790-1
- IVOR, J., a kol., 2010. Trestné právo procesné. Druhé doplnené a prepracované vydanie. Bratislava: Iura Edition. 2010. s. 1049. ISBN 978-80-8078-309-9
- IVOR, J., POLÁK, P., ZÁHORA, J., 2016. Trestné právo hmotné. I. všeobecná časť. Bratislava: Wolters Kluwer. 2016. s. 555. ISBN 978-80-8168-509-5
- KMEC, J., KOSÁŘ, D., KRATOCHVÍL, J., BOBEK, M., 2012. Evropská úmluva o lidských právech. Komentář. 1. vyd. Praha: C. H. Beck. 2012. s. 1687. ISBN 978-80-7400-365-3
- KYJAC, Z., 2015. Použitie informačno-technických prostriedkov v trestnom konaní. Odpočúvanie a záznam telekomunikačnej prevádzky. Bratislava: Wolters Kluwer. 2015. s. 307. ISBN 978-80-8168-266-7
- LAZAR, J., a kol., 2010. Občianske právo hmotné I, Bratislava: Iura Edition. 2010. s. 715. ISBN 978-80-8078-346-4
- MEDELSKÝ, J., 2016. Trestná zodpovednosť právnických osôb. Plzeň: Aleš Čeněk. 2016. s. 202. ISBN 978-80-7380-608-8
- MEZEI, M., 2015. Odpočúvanie právnickej osoby. In: Zborník z medzinárodnej vedeckej konferencie doktorandov a mladých vedeckých pracovníkov organizovanej Univerzitou Komenského v Bratislave, Právnickou fakultou, v dňoch 19.–21. 3. 2015 v priestoroch ÚZ NR SR Častá-Papiernička. Mílniky práva v stredoeurópskom priestore 2015. Bratislava: Univerzita Komenského, Právnická fakulta. 2015. s. 679. ISBN 978-80-7160-394-8
- NOVOTNÁ, J., 2003. K některým otázkám dokazování odposlechem a záznamem telekomunikačního provozu, In: *Trestněprávní revue*, 2003, č. 10, s. 291
- STRÁŽNICKÁ, V., a kol., 2013. Medzinárodná a európska ochrana ľudských práv. Bratislava: Eurokódex. 2013. s. 560. ISBN 978-80-8944-795-4
- ŠAMKO, P., 2016. Niekoľko poznámok k trestnej zodpovednosti právnických osôb. Dostupné na internete: <http://www.pravnelisty.sk/clanky/a466-poznamky-k-zakonu-o-trestnej-zodpovednosti-pravnickych-osob> 2016.
- ZÁHORA, J., a kol., 2013. Dokazovanie v trestnom konaní. Praha: LEGES, 2013. s. 320. ISBN 978-80-87576-76-2
- ZÁHORA, J., 2016. Otvorené otázky trestnej zodpovednosti právnických osôb. In: *Justičná revue – časopis pre právnu prax*. 2016. č. 5. ISSN: 1335-6461
- ZÁHORA, J., ŠIMOVICEK, I. Zákon o trestnej zodpovednosti právnických osôb: komentár, Bratislava: Wolters Kluwer, 2016. 342 s. ISBN 978-80-8168-413-5.

Aktuálne problémy vyhotovovania obrazových, zvukových alebo obrazovo-zvukových záznamov v trestnom konaní¹

Actual Problems of Making Video, Audio or Video-audio Recordings in Criminal Proceedings

Monika Širilová²

Abstrakt: Tento príspevok rozoberá problematiku inštitútu vyhotovovania obrazových, zvukových a obrazovo-zvukových záznamov, a to konkrétne možnosti využitia „odposluchu na telo“ v súvislosti s osobou v procesnom postavení svedka a agenta. Príspevok sa rovnako venuje podmienkam použitia záznamov získaných v súvislosti s monitorovaním priestorov prístupných verejnosti v trestnom konaní.

Abstract: This article discusses problematic of the institute of making video, audio and video-audio recordings, and namely the possibility of using “wiretapping on body” in relation to the person in procedural status of witness or agent. Article also devotes to conditions of using records obtained in relation to monitoring publicly accessible premises in criminal proceedings.

Kľúčové slová: informačno-technický prostriedok; obrazový, zvukový a obrazovo-zvukový záznam; svedok, agent, trestné konanie.

Key words: information-technical mean; video, audio or video-audio recordings; witness, agent, criminal proceedings.

Úvod

Problematika získavania informácií a dôkazov v trestnom konaní prostredníctvom informačno-technických prostriedkov vždy bola a v súčasnosti nepochybne stále je veľmi aktuálnou a diskutovanou témou.

Hneď v úvode uvádzam do pozornosti skutočnosť, že pre odhaľovanie a vyšetrovanie najzávažnejších foriem trestnej činnosti sú „klasické“ dôkazné prostriedky, medzi ktoré možno zaradiť najmä výsluchy, znaleckú činnosť či rôzne prehliadky, nedostačujúce, v dôsledku čoho, sa „čoraz intenzívnejšie presadzuje v trestnom konaní dokazovanie za pomoci využívania najrôznejších foriem informačno-technických prostriedkov.“³

Samotný pojem informačno-technické prostriedky je definovaný v § 10 ods. 21 Trestného poriadku,⁴ v zmysle ktorého sa informačno-technickými prostriedkami rozumejú elektro-technické, rádiotechnické, fototechnické, optické, mechanické, chemické a iné technické prostriedky a zariadenia alebo ich súbory použité utajovaným spôsobom pri odpočúvaní a zázname prevádzky v elektronických komunikačných sieťach (ďalej len „odpočúvanie a záznam telekomunikačnej prevádzky“), obrazových, zvukových alebo obrazovo-zvukových záznamov alebo

¹ Táto práca bola podporovaná Agentúrou na podporu výskumu a vývoja na základe Zmluvy č. APVV-15-0272.

² Mgr. Monika Širilová, MLA, Ústav verejného práva, Fakulta práva, Paneurópska vysoká škola, Bratislava, e-mail: sirilova@nitschneider.com.

³ IVOR, J.: Monitorovanie osôb ako dôkazný prostriedok v trestnom konaní. In: Karlovarská právnická revue. Roč. 3, č. 4 (2007), s. 1–5.

⁴ Zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov.

pri vyhľadávaní, otváraní a skúmaní zásielok, ak sa ich použitím zasahuje do základných ľudských práv a slobôd. Na spracúvanie informácií získaných použitím informačno-technických prostriedkov, ich evidenciu, dokumentáciu, ukladanie a vyraďovanie sa vzťahujú osobitné predpisy, ak tento zákon neustanovuje inak. Prevádzkovatelia verejných telefónnych sietí, poskytovatelia elektronických telekomunikačných sietí, poskytovatelia elektronických telekomunikačných služieb, poštový podnik, dopravcovia a iní zasielateľia a ich zamestnanci sú povinní poskytnúť nevyhnutnú súčinnosť pri použití informačno-technických prostriedkov; pritom sa nemôžu dovolávať povinnosti mlčanlivosti podľa osobitných zákonov.

Ako to už vyplýva zo samotného názvu môjho príspevku, svoju pozornosť upriamim na inštitút vyhotovovania obrazových, zvukových a obrazovo-zvukových záznamov, pričom konkrétne sa budem venovať možnostiam použitia tzv. „odposluchov na telo“ pri osobách v procesnom postavení svedka a agenta pri získavaní dôkazov v súvislosti s najzávažnejšou trestnou činnosťou, s výnimkou trestných činov korupcie a terorizmu a následne sa budem venovať problematike, ktorá priamo nesúvisí s vyhotovovaním obrazových, zvukových a obrazovo-zvukových záznamov podľa § 114 Trestného poriadku, a to konkrétne použitiu záznamov získaných v súvislosti s monitorovaním priestorov prístupných verejnosti, nakoľko je daná problematika podľa môjho názoru značne dôležitá v súvislosti so získavaním dôkazov v trestnom konaní.

Nakoľko samotné použitie informačno-technických prostriedkov ako takých predstavuje významný zásah do ľudských práv, považujem za nevyhnutné spomenúť, že tieto prostriedky nie je možné používať svojvoľne a rovnako nie je možné a ani žiadúce ich zneužívanie. Podmienky ich použitia sú predmetom nie len vnútroštátnej právnej úpravy, ale rovnako aj „medzinárodných dohovorov o ľudských právach, ktorými sa priznáva ochrana osobám, proti ktorým smeruje použitie informačno-technických prostriedkov.“⁵

V zmysle článku 8 Dohovoru o ochrane ľudských práv a základných slobôd:

- 1.) *Každý má právo na rešpektovanie svojho súkromného a rodinného života, obydlia a korešpondencie.*
- 2.) *Štátny orgán nemôže do výkonu tohto práva zasahovať, okrem prípadov, keď je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojov a zločinnosti, ochrany zdravia alebo morálky alebo ochrany práv a slobôd iných.*

V súvislosti s vnútroštátnou právnou úpravou uvádzam do pozornosti Ústavu SR,⁶ ktorá v článku 1 prehlasuje Slovenskú republiku za zvrchovaný, demokratický a právny štát, pričom z ďalších článkov vyplýva, že ide o štát založený na úcte k právam a slobodám človeka a občana. Zásahy do osobnostných práv sú v zmysle čl. 13 Ústavy SR možné výlučne na základe zákona. V predmetnej súvislosti rovnako poukazujem na občianskoprávnu ochranu osobnosti, konkrétne na § 12 Občianskeho zákonníka,⁷ v zmysle ktorého písomnosti osobnej povahy, podobizne, obrazové snímky a obrazové a zvukové záznamy týkajúce sa fyzickej osoby alebo jej prejavov osobnej povahy sa smú vyhotoviť alebo použiť len s jej privolením, a zároveň pripúšťa výnimku v podobe vyhotovovania takýchto záznamov bez privolenia dotknutej osoby na úradné účely na základe zákona.

⁵ DRGONEC, J.: Ústavný a zákonný rámec použitia informačno-technických prostriedkov štátnymi orgánmi. In: Justičná revue. Roč. 53, č. 10 (2001), s. 1009–1024.

⁶ Zákon č. 460/1992 Zb. Ústava SR v znení neskorších predpisov.

⁷ Zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov.

Možnosti využitia „odposluchu na telo“ v súvislosti s osobami v procesnom postavení svedka a agenta

V nasledujúcej časti môjho príspevku sa budem venovať problematike „odposluchov na telo“ a možnostiam ich využitia pri osobách v procesnom postavení svedka a agenta, pričom mojim cieľom bude poukázať na možnosti použitia tohto inštitútu, ako aj na jeho prínos pri získavaní dôkazov.

Pre správne pochopenie danej problematiky je na začiatok nevyhnutné oboznámiť sa so základnými pojmami.

Trestný poriadok neobsahuje legálnu definíciu pojmu svedok. Tento pojem však možno vyvodíť z ustanovenia § 127 Trestného poriadku, ktorý upravuje, kto má povinnosť svedčiť. Vychádzajúc z predmetného ustanovenia, svedkom je osoba (odlišná od obvineného), ktorá je povinná dostaviť sa na predvolanie orgánov činných v trestnom konaní alebo súdu, aby vypovedala ako svedok o tom, čo jej je známe o trestnom čine a o jeho páchatelovi alebo o okolnostiach dôležitých pre trestné konanie, teda o skutočnostiach, ktoré vnímala svojimi zmyslami, teda videla, počula a pod., pričom podať správu o tom, čo určitá osoba vnímala môže len takáto osoba.⁸ Keďže svedok vypovedá o skutočnostiach, ktoré vnímal vlastnými zmyslami (zrak, sluch, čuch, hmat, chuť), a tak získava poznatky o veci priamym a bezprostredným pozorovaním skutočnosti, je výpoveď svedka pre trestné konanie nenahraditeľná a nositeľ tejto výpovede nezastupiteľný.⁹

Agent je definovaný v § 10 ods. 20 Trestného poriadku ako príslušník Policajného zboru alebo príslušník polície iného štátu, ktorý na základe príkazu prokurátora alebo súdu prispieva k odhaľovaniu, zisťovaniu a usvedčovaniu páchatelov zločinu, trestných činov uvedených v treťom diele ôsmej hlavy osobitnej časti Trestného zákona (ďalej len „korupcia“), trestného činu zneužívania právomoci verejného činiteľa a trestného činu legalizácie príjmu z trestnej činnosti. Pri odhaľovaní, zisťovaní a usvedčovaní páchatelov korupcie alebo trestných činov terorizmu môže byť agentom aj iná osoba ako príslušník Policajného zboru ustanovená prokurátorom na návrh policajta alebo príslušníka Policajného zboru povereného ministrom vnútra Slovenskej republiky (ďalej len „minister vnútra“).

„Odposluch na telo“ nie je v právnej teórii nijako definovaný, ale pre účely môjho príspevku a jasné pochopenie mnou zvolenej témy ním možno rozumieť vyhotovovanie zvukových záznamov v zmysle § 114 Trestného poriadku, počas ktorého je zaznamenávacie zariadenie umiestnené na tele osoby, ktorá sa podieľa na získavaní dôkazov v konkrétnej trestnej veci (v našom prípade osoba svedka a agenta).

Ako príklad uvádzam modelovú situáciu kedy osoba A požiada osobu B, aby jej táto pomohla s vykonaním úkladnej vraždy osoby C, pričom osoba A má detailne vymyslený plán ako úkladnú vraždu zrealizovať a od osoby B potrebuje len to, aby táto plnila jej pokyny, ktoré jej vždy odovzdá na osobnom stretnutí, pričom miesto stretnutia bude vždy určené operatívne. Osoba B, v danom prípade svedok, sa ihneď rozhodne oznámiť tieto skutočnosti orgánom činným v trestnom konaní, nakoľko nemá v úmysle páchať, ani sa nijako inak podieľať na páchaní trestnej činnosti, v dôsledku čoho bude začaté trestné stíhanie vo veci trestného činu úkladnej vraždy v štádiu prípravy.

V predmetnom prípade je použitie informačno-technických prostriedkov nevyhnutnosťou, nakoľko získanie dôkazov iným spôsobom by bolo podstatným spôsobom sťažené. Zainteresovanie poškodeného, teda osoby C, je v danom prípade nelogické a neúčelné.

⁸ IVOR, J. a kol.: Trestné právo procesné, 2. vydanie. Bratislava: IURA EDITION. 2010. s. 465.

⁹ POLÁK, P.: Svedok v trestnom konaní. Bratislava: EUROKÓDEX, s. r. o., 2011, s. 75.

Najvhodnejším riešením by v danom prípade bolo využitie inštitútu „odposluchov na telo“ kedy by osoba B, na základe príkazu sudcu pre prípravné konanie v zmysle § 114 Trestného poriadku, mala na sebe počas stretnutí s osobou A nahrávacie zariadenie, ktorým by monitorovala celý priebeh stretnutia resp. stretnutí, pričom takto získané nahrávky by boli jasným dôkazom, či už v prospech alebo neprospech podozrivej osoby A.

Ako je zrejmé z modelovej situácie, použitie agenta – príslušníka Policajného zboru – by nebolo možné, nakoľko jeho „infiltrácia“ do prostredia by bola značne komplikovaná, a to najmä z dôvodu, že osoba A plne dôveruje a výlučne komunikuje len s osobou B, s ktorou už má vytvorený určitý vzťah.

V danej situácii sa vynára otázka, či je možné použiť „odposluch na telo“ u osoby B v procesnom postavení svedka potom, čo táto osoba už urobila oznámenie o konaní osoby A orgánom činným v trestnom konaní. Podotýkam, že čo sa týka súkromných nahrávok vyhotovených osobou B, v trestnom konaní môžu byť použité len tie, ktoré boli vyhotovené pre tým, než osoba B urobila oznámenie orgánom činným v trestnom konaní.

Odpoveď na položenú otázku nachádzame v rozhodnutí Najvyššieho súdu SR sp. zn. 2To 15/2015 zo dňa 25. októbra 2016, v ktorom súd konštatoval, že „osoba môže vystupovať v trestnom konaní v pozícii svedka podľa § 127 Trestného poriadku len dovtedy, pokiaľ neoznámi skutočnosti nasvedčujúce tomu, že má byť spáchaný trestný čin a nezačne byť riadená a ovplyvňovaná orgánmi činnými v trestnom konaní, pretože od tohto momentu koná v podstate v rovnakom faktickom postavení ako agent v zmysle § 117 Trestného poriadku – ako agent de facto, nie je však agentom de iure. Od tohto momentu má len formálne postavenie svedka, čo je však závažnejšie, na dôkaz získaný a predložený takýmto svedkom, či už v podobe výpovede alebo inej forme (predloženie vecného dôkazu, listín a podobne), nie je možné v ďalšom konaní prihliadať. Z uvedeného je zrejmé, že svedok sa nemôže nijako zúčastňovať na páchaní trestného činu v akejkolvek forme, podobe, či štádiu. Ak nemožno inými dôkaznými prostriedkami odhaliť, zistiť, či usvedčiť páchatela zločinu (a contrario § 117 ods. 1 veta druhá Trestného poriadku – len vtedy, ak odhaľovanie, zisťovanie a usvedčovanie páchatelov uvedených trestných činov by bolo iným spôsobom podstatne sťažené a získané poznatky odôvodňujú podozrenie, že bol spáchaný trestný čin alebo má byť spáchaný taký trestný čin), možno použiť agenta. Podľa § 117 ods. 2, veta prvá Trestného poriadku, konanie agenta musí byť v súlade s účelom tohto zákona a musí byť úmerné protiprávnosti konania, na odhaľovaní, zisťovaní alebo usvedčovaní ktorého sa zúčastňuje. Z uvedeného vyplýva, že procesné postavenie agenta (§ 117 Trestného poriadku) je oproti všeobecnému procesnému postaveniu svedka (§ 127 Trestného poriadku) osobitné, a to napriek okolnosti, že agent môže byť v trestnom konaní vypočutý ako svedok (§ 117 ods. 11 Trestného poriadku). Ak páchatel oznámi páchanie trestného činu v štádiu prípravy alebo pokusu políciou a nebol použitý ako agent na základe príkazu podľa § 117 ods. 5 až 7 Trestného poriadku (pričom okrem výnimky uvedenej v § 10 ods. 20 Trestného poriadku môže byť agentom len príslušník Policajného zboru), nemôže táto osoba, a to ani v rámci spolupráce s políciou, predstierať pokračovanie v páchaní trestného činu na účel usvedčenia ďalšieho páchatela, resp. spolupáchatela dotknutého činu. Ak k takému postupu došlo, nie je možné výpoveď svedka vo vzťahu k okolnostiam, ktoré nastali po oznámení trestného činu políciou, použiť v trestnom konaní ako dôkaz.“

S poukazom na vyššie uvedené rozhodnutie Najvyššieho súdu SR možno konštatovať, že získanie dôkazov v prípadoch, kedy by bolo nevyhnutné použiť svedka v de facto postavení agenta je prakticky vylúčené. Uvedené sa však nevzťahuje na trestné činy korupcie a terorizmu, pri vyšetrovaní ktorých Trestný poriadok umožňuje „postaviť“ do pozície agenta aj osobu, ktorá nie je príslušníkom Policajného zboru. Uvedená skutočnosť značne zvyhodňuje a uľahčuje vy-

šetrovanie trestných činov korupcie a terorizmu v porovnaní s vyšetrovaním ostatných druhov trestnej činnosti.

V nadväznosti na vyššie uvedené by bolo podľa môjho názoru vhodné, či dokonca priam žiaduce, aby bolo predmetné ustanovenie týkajúce sa agenta novelizované. Samozrejme, v prípade zmeny, je neprípustné, aby osoba konala ako „agent provokatér“. Teda agent v žiadnom prípade nesmie navádzať na páchanie trestnej činnosti a z jeho činnosti a komunikácie musí byť zjavné, že len pasívne participoval na príprave resp. plnil príkazy podozrivého pri samotnom pokuse o dokonanie trestného činu.

Použitie záznamov získaných v súvislosti s monitorovaním priestorov prístupných verejnosti v trestnom konaní

Záznamy získané v súvislosti s monitorovaním verejne prístupných priestorov v mnohých prípadoch slúžia ako priamy dôkaz prospeievajúci k usvedčeniu páchatelov trestných činov. Hoci predmetné záznamy nemožno zaradiť k inštitútu informačno-technických prostriedkov, považujem za potrebné venovať sa možnostiam ich použitia v trestnom konaní.

V prvom rade je potrebné definovať, čo môže byť v trestnom konaní považované za dôkaz. Túto otázku upravuje § 119 ods. 2 Trestného poriadku, v zmysle ktorého za dôkaz môže slúžiť všetko, čo môže prispieť na náležité objasnenie veci a čo sa získalo z dôkazných prostriedkov podľa tohto zákona alebo podľa osobitného zákona, pričom dôkaznými prostriedkami sú najmä výsluch obvineného, svedkov, znalcov, posudky a odborné vyjadrenia, previerka výpovede na mieste, rekognícia, rekonštrukcia, vyšetrovací pokus, obhliadka, veci a listiny dôležité pre trestné konanie, oznámenie, informácie získané použitím informačno-technických prostriedkov alebo prostriedkov operatívno-pátracej činnosti.

Z vyššie uvedeného nepochybne vyplýva, že záznam získaný monitorovaním priestorov verejne prístupných môže byť v trestnom konaní použitý ako dôkaz.

V predmetnej súvislosti je však potrebné sústrediť sa, okrem ustanovení Trestného poriadku, na zákon č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov, ktorého ustanovenia, konkrétne § 15 ods. 7 ustanovuje, že priestor prístupný verejnosti možno monitorovať len na účely ochrany verejného poriadku a bezpečnosti, odhaľovania kriminality, narušenia bezpečnosti štátu, ochrany majetku alebo zdravia, a to len vtedy, ak je priestor zreteľne označený ako monitorovaný; monitorovaný priestor je prevádzkovateľ povinný zreteľne označiť bez ohľadu na to, či sa snímaný obraz alebo zvuk zaznamenáva na nosič informácií. Označenie monitorovaného priestoru sa nevyžaduje, ak tak ustanovuje osobitný zákon. Vyhotovený záznam možno využiť len na účely trestného konania alebo konania o priestupkoch, ak osobitný zákon neustanovuje inak.

Monitorovanie verejne prístupných priestorov, najmä bánk, finančných ústavov, čerpacích staníc, hypermarketov, staníc resp. zastávok hromadnej dopravy, peších zón, ako aj iných miest, kde hrozí potenciálne narušenie verejného poriadku alebo zvýšené riziko páchania trestnej činnosti, so sebou prináša nové možnosti odhaľovania a následného dokazovania trestnej činnosti.

V súvislosti s danou problematikou uvádzam do pozornosti argument, ktorý je v priebehu trestného konania často používaný obvinenými resp. obhajcami a to, že monitorovaný priestor nie je zreteľne označený. „Nezreteľné označenie“ monitorovaného priestoru malo vo viacerých trestných veciach za následok skutočnosť, že kamerový záznam bol považovaný za nezákonne získaný dôkaz a nebolo možné naň prihliadať. S poukazom na vyššie uvedené uvádzam, že

z praktického hľadiska nie je možné a rovnako ani logické, aby bol každý verejne prístupný monitorovaný priestor označený tak, aby toto označenie bolo jasne viditeľné takpovediac „z každého uhla“ a to najmä v prípadoch, ak sú kamery jasne viditeľné a nie je možné ich prehliadnuť.

V nadväznosti na vyššie uvedené poukazujem na rozhodnutie Krajského súdu v Trnave pod sp. zn. 3To/58/2014, ktorý ako odvolací súd rozhodoval o odvolaní obžalovaného L. A. proti rozhodnutiu Okresného súdu v Galante, ktorým bol odsúdený za trestný čin marenia výkonu úradného rozhodnutia podľa § 348 ods. 1 písm. d) Trestného zákona. Predmetnom odvolania bola námietka proti použiteľnosti obrazového záznamu z čerpaciej stanice, nakoľko celý priestor nebol riadne označený ako monitorovaný.

Krajský súd v Trnave vo svojom rozhodnutí konštatuje, že „odvolacia námietka o nepoužiteľnosti obrazového záznamu z kamerového systému čerpaciej stanice bola odvolacím súdom vyhodnotená ako nedôvodná. Zákonná úprava, na ktorú odvolateľ v dôvodoch odvolania poukazuje, umožňuje priestor prístupný verejnosti monitorovať pomocou videozáznamu alebo audiozáznamu len pre účely verejného poriadku a bezpečnosti, odhaľovania kriminality alebo narušenia bezpečnosti štátu a to len vtedy, ak priestor je zreteľne označený a monitorovaný. Označenie monitorovaného priestoru sa nevyžaduje, ak tak ustanovuje osobitný zákon. Vyhodený záznam možno využiť len na účely trestného konania alebo konania o priestupkoch, ak osobitný zákon neustanovuje inak. Nie je sporné, že čerpacia stanica je priestor verejnosti prístupný, preto je tento možné monitorovať na účely vymedzené vyššie citovaným zákonným ustanovením. Aj keď zo zákona vyplýva povinnosť, aby takýto priestor bol zreteľne označený ako monitorovaný, nemožno od prevádzkovateľa vyžadovať, aby takto označil priestor po celom jeho obvode z dôvodu, aby bol viditeľný z každého uhla. Napokon je všeobecne známe, že takéto priestory sú vždy monitorované, a kamera, ktorá nasníma v kritickom čase obžalovaného a jeho vozidlo, bola na viditeľnom mieste. Možnosť využitia vyhotoveného záznamu kamerového systému pre účely trestného konania vyplýva priamo zo zákonnej úpravy.“¹⁰

Argumentácia „zreteľnosti, resp. nezreteľnosti označenia“ monitorovaného priestoru je teda vo väčšine prípadov len účelová s cieľom jednoznačne, aj keď nelogicky, spochybniť legálnosť získania takeéhoto dôkazu. V zmysle vyššie uvedených skutočností teda v centre pozornosti stojí potreba hodnotenia zákonnosti a prípustnosti kamerových záznamov získaných monitorovaním verejných priestranstiev na základe logiky, pričom pri hodnotení by mali vzaté do úvahy všetky skutočnosti, a nie len skutočnosť, či obvinený/obžalovaný mal možnosť všimnúť si nápis označujúci monitorovanie predmetného miesta. V predmetnej súvislosti by som rada zdôraznila potrebu logického a v daných prípadoch dokonca extenzívneho výkladu zákonných ustanovení, nakoľko daný postup môže v mnohých prípadoch výrazne prispieť k naplneniu účelu trestného konania.

Záver

Vzhľadom na limitovaný rozsah príspevku nie je možné venovať sa všetkým otázkam, ktoré považujem za aktuálne v súvislosti s vyhotovovaním obrazových, zvukových a obrazovo zvukových záznamov. Mojim hlavným cieľom bolo poukázať na tie z nich, ktoré sú podľa môjho názoru najzaujímavejšie a môžu predstavovať prínosný podnet pre odborné diskusie. Na záver by som chcela poukázať na vzájomnú prepojenosť a súvis medzi jednotlivými druhmi informačno-technických prostriedkov a prostriedkov operatívno-pátracej činnosti, ktorých praktic-

¹⁰ Rozhodnutie Krajského súdu v Trnave sp. zn. 3To/58/2014.

ké využívanie je v súčasnosti nevyhnutné pre zabezpečenie potrebného množstva relevantných dôkazov.

Zoznam použitej literatúry:

- ČENTĚŠ, J., a kol., 2015. Trestný poriadok. Veľký komentár. 2. aktualizované vydanie. Bratislava: EUKODEX. 2015. 955 s. ISBN 978-80-8155-057-7
- DRGONEC, J., 2001. Ústavný a zákonný rámec použitia informačno-technických prostriedkov štátnymi orgánmi, In: Justičná revue, 2001, Roč. 53, č. 10, s. 1009–1024
- IVOR, J., a kol., 2010. Trestné právo procesné. Druhé doplnené a prepracované vydanie. Bratislava: Iura Edition. 2010. 1049 s. ISBN 978-80-8078-309-9
- IVOR, J.: Monitorovanie osôb ako dôkazný prostriedok v trestnom konaní. In: Karlovarska právni revue. Roč. 3, č. 4 (2007), s. 1–5
- LAZAR, J., a kol., 2010. Občianske právo hmotné I., Bratislava: Iura Edition. 2010. 715 s. ISBN 978-80-8078-346-4
- POLÁK, Peter: Svedok v trestnom konaní. Bratislava: EUKODEX, s. r. o. 2011, 296 s. ISBN 978-80-89447-49-7
- ZÁHORA, J., a kol., 2013. Dokazovanie v trestnom konaní. Praha: LEGES. 2013. 320 s. ISBN 978-80-87576-76-2
- Rozhodnutie Krajského súdu v Trnave sp. zn. 3To/58/2014
- Rozhodnutie Najvyššieho súdu SR sp. zn. 2To 15/2015
- Zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov
- Zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov
- Zákon č. 460/1992 Zb. Ústava SR v znení neskorších predpisov

Osobitosti použitia ITP v pôsobnosti Slovenskej informačnej služby

Particularities of Use Information Technical Means within the Scope of the Slovak Intelligence Service

Michal Aláč¹

Abstrakt: Slovenská informačná služba bola zriadená zákonom Národnej rady Slovenskej republiky č. 46/1993 Z. z. o Slovenskej informačnej službe v znení neskorších predpisov ako integrovaná civilná spravodajská služba, t. j. ako služba plniaca úlohy na úseku vnútorného aj zahraničného spravodajstva. Keďže slovenská informačná služba plní špecifické úlohy, bolo nevyhnutné špecifickým spôsobom upraviť aj podmienky použitia osobitných prostriedkov, ktoré je oprávnená používať pri plnení svojich úloh. Jedným z týchto osobitných prostriedkov sú aj informačno-technické prostriedky, ktoré invazívnym spôsobom umožňujú Slovenskej informačnej službe získavať informácie a tým plniť zákonom ustanovené úlohy.

Abstract: Slovak Intelligence Service was established by the National Council of the Slovak Republic no. 46/1993 Coll. The Act on the Slovak Intelligence Service as an integrated civilian intelligence, i. e. as a service fulfilling tasks in the field of internal and even external intelligence. As the Slovak Information Service performs a specific task, it was necessary in a to modify in specific way conditions of using special equipment that is authorized to use in fulfilling its role. One of these special means are also technical-intelligence means by which in invasive way allows the Slovak Information Service to obtain information to perform the tasks laid down by law.

Kľúčové slová: spravodajská služba, informačno-technický prostriedok, odpočúvanie.

Key words: intelligence service, technical-intelligence means, interception.

I. Definícia informačno-technického prostriedku *in generalis*

Informačno-technický prostriedok je ako pojem „endemitom“ slovenského právneho poriadku. Jeho legálna definícia je ustanovená v § 10 ods. 21 zákona č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov (ďalej len „Trestný poriadok“) a v § 2 zákona č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) v znení neskorších predpisov (ďalej len „zákon č. 166/2003 Z. z.“).

Podľa Trestného poriadku sa informačno-technickými prostriedkami na účely tohto zákona rozumejú elektrotechnické, rádiotechnické, fototechnické, optické, mechanické, chemické a iné technické prostriedky a zariadenia alebo ich súbory použité utajovaným spôsobom pri odpočúvaní a zázname prevádzky v elektronických komunikačných sieťach (ďalej len „odpočúvanie a záznam telekomunikačnej prevádzky“), obrazových, zvukových alebo obrazovo-zvukových záznamov alebo pri vyhľadávaní, otváraní a skúmaní zásielok, ak sa ich použitím zasahuje do základných ľudských práv a slobôd.

Podľa zákona č. 166/2003 Z. z. sú informačno-technickými prostriedkami na účely cit. zákona najmä elektrotechnické, rádiotechnické, fototechnické, optické, mechanické, chemické a iné technické prostriedky a zariadenia alebo ich súbory používané utajovaným spôsobom pri

¹ JUDr. Michal Aláč, PhD., Trnavská univerzita v Trnave, Právnická fakulta.

- a) vyhľadávani, otváraní, skúmaní a vyhodnocovaní poštových zásielok a iných dopravovaných zásielok,
- b) získavaní obsahu správ prenášaných prostredníctvom elektronických komunikačných sietí vrátane odpočúvania telefónnej komunikácie,
- c) vyhotovovaní obrazových, zvukových, obrazovo-zvukových alebo iných záznamov.

Z dikcie citovaných ustanovení vyplýva, že zákonodarca pri kreovaní citovanej definície nezohľadňoval funkcionality, štruktúru alebo zloženie prostriedkov, t. j. nedefinoval prostriedky z technického hľadiska, ale ako definičný faktor zvolil iný atribút – to, či nejaký prostriedok možno považovať za informačno-technický prostriedok závisí od účelu a od spôsobu využitia jeho funkcionality alebo vlastností. *In generalis* za informačno-technický prostriedok možno považovať akýkoľvek prostriedok využívaný orgánmi štátnej moci na zasahovanie do práva na súkromie a vytvorenie výsledku, na ktorom budú zachytené informácie týkajúce sa súkromia dotknutej osoby. Napríklad len také použitie zariadenia na vyhotovovanie obrazových záznamov možno považovať za použitie informačno-technického prostriedku, ktoré je realizované utajovaným spôsobom orgánom štátnej moci a predmetným použitím dochádza k zásahu do súkromia dotknutej fyzickej osoby.

Uvedené legálne definície sú veľmi podobné, avšak je potrebné konštatovať, že definícia ustanovená Trestným poriadkom neobsahuje pojem „iný záznam“, čím zákonodarca značne obmedzil univerzálny charakter definície informačno-technického prostriedku. Ako už bolo uvedené, za informačno-technický prostriedok možno považovať akýkoľvek prostriedok, ak je používaný spôsobom anticipovaným zákonom o ochrane pred odpočúvaním, resp. Trestným poriadkom. Na túto skutočnosť reflektuje práve ust. § 2 ods. 1 písm. c) zákona č. 166/2003 Z. z. už uvedeným pojmom „iný záznam“. Práve výklad tohto pojmu v aplikačnej praxi spôsobuje problémy. V kontexte znenia uvedeného ustanovenia často dochádza k mylnému záveru, že pojem „iný záznam“ je ekvivalentom pre zvukovo-obrazový záznam. Tento záver má oporu v znení § 114 Trestného poriadku, v ktorom sa používa pojem „vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov“. Pod pojem „iný záznam“ je však nevyhnutné subsumovať akýkoľvek záznam vyhotovený pomocou informačno-technických prostriedkov. Môže ísť napríklad o vyhotovenie záznamu – kópie údajov nachádzajúcich sa v počítači záujmovej osoby alebo na pamäťovom médiu. Ide o obdobu inštitútu uchovania a vydania počítačových údajov podľa § 90 Trestného poriadku.

Zároveň však zákonodarca prezumoval záver, že použitím informačno-technického prostriedku sa vyhotoví iný záznam, avšak z pohľadu aplikačnej praxe by bol vhodnejší pojem použitý v ust. § 7 zákona č. 166/2003 Z. z., a to iný výsledok. Napr. pri použití chemického činidla ako informačno-technického prostriedku bude výsledkom nejaká zlúčenina, výsledkom je teda nejaký hmotný substrát, a preto by bol takýto výsledok výstižnejšie nazvať iný výsledok, než iný záznam.

Z definície pojmu informačno-technického prostriedku podľa Trestného poriadku, ako aj podľa zákona č. 166/2003 Z. z. zákonodarca vyňal použitie predmetného prostriedku pri zámene obsahu zásielok. Obsah zásielky však z technického hľadiska nemožno zameniť bez otvorenia zásielky, resp. bez narušenia jej vonkajšieho obalu. Bez narušenia vonkajšieho obalu možno zameniť obsah len takým spôsobom, že dôjde k použitiu inej, na tieto účely vytvorenej zásielky, ktorá bude mať požadovaný obsah a jej vonkajší vzhľad bude identický so zásielkou, ktorej obsah bolo potrebné zameniť.

II. Podmienky použitia informačno-technického prostriedku v podmienkach Slovenskej informačnej služby

Slovenská informačná služba bola zriadená zákonom Národnej rady Slovenskej republiky č. 46/1993 Z. z. o Slovenskej informačnej službe v znení neskorších predpisov (ďalej len „zákon o SIS“) ako integrovaná civilná spravodajská služba, t. j. ako služba plniaca úlohy na úseku vnútorného aj zahraničného spravodajstva. Mala tzv. „pure intelligence profile“, čiže bola spravodajskou službou bez výkonných právomocí a jej úlohou bolo získavať, sústreďovať a vyhodnocovať informácie o určenom okruhu hrozieb. Jej spravodajský charakter nebol *expressis verbis* vyjadrený v zákone o SIS, v ktorom bola definovaná ako štátny orgán, ale vyplýval z vymedzenia jej vecnej pôsobnosti. Podľa § 2 ods. 1 zákona o SIS bola Slovenská informačná služba v rozsahu svojej pôsobnosti oprávnená získavať, sústreďovať a vyhodnocovať informácie o

- a) činnosti ohrozujúcej ústavné zriadenie, územnú celistvosť a zvrchovanosť Slovenskej republiky,
- b) činnosti smerujúcej proti bezpečnosti Slovenskej republiky,
- c) aktivite cudzích spravodajských služieb,
- d) organizovanom terorizme,
- e) skutočnostiach spôsobilých vážne ohroziť alebo poškodiť hospodárske záujmy Slovenskej republiky,
- f) ohrození alebo úniku údajov obsahujúcich skutočnosti tvoriace predmet štátneho tajomstva.

Aktuálny spoločenský vývoj si vyžiadal, aby Slovenská informačná služba zamerala svoju činnosť na ďalšiu hrozbu. Touto hrozbou bol organizovaný zločin, ktorý začal prerastať do všetkých oblastí spoločenského života a bolo nevyhnutné jeho spravodajské rozpracovanie, a preto došlo k rozšíreniu vecnej pôsobnosti Slovenskej informačnej služby zákonom č. 256/1999 Z. z. ktorým sa mení a dopĺňa zákon č. 46/1993 Z. z. o Slovenskej informačnej službe v znení neskorších predpisov, ktorý medzi objekty jej spravodajského záujmu ustanovil aj organizovaný zločin.

Ďalšia výrazná zmena právneho postavenia a rozšírenie pôsobnosti Slovenskej informačnej služby bolo realizované v kontexte teroristických útokov, ku ktorým došlo v Európe v roku 2015. V rámci prijatia tzv. protiteroristického balíka zákonov bol zákonom č. 444/2015 Z. z., ktorým sa mení a dopĺňa zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony, a to konkrétne novelizačným článkom III, novelizovaný zákon o SIS. Uvedeným zákonom došlo k zmene samotnej podstaty Slovenskej informačnej služby. S účinnosťou zákona, t. j. od 1. 1. 2016, sa Slovenská informačná služba stala všeobecnou bezpečnostnou a spravodajskou službou Slovenskej republiky, čím došlo k zmene jej čisto spravodajského charakteru na službu, ktorá má špecifikovaný rozsah výkonných právomocí. Ide napríklad o oprávnenie zameniť vec za inú vec, ak je to nevyhnutné na účely získania informácie alebo zabránenia vzniku závažnej ujmy na bezpečnosti štátu, hospodárskych záujmoch štátu alebo ochrane utajovaných skutočností. Zámenu veci môže však Slovenská informačná služba vykonať len na základe predchádzajúceho písomného súhlasu sudcu súdu príslušného podľa osobitného predpisu. Týmto predpisom je zákon č. 166/2003 Z. z. Zároveň zákonodarca ustanovil podmienku proporcionality spočívajúcu v tom, že zámenou veci nesmie vzniknúť na týchto záujmoch väčšia ujma ako tá, ktorá by hrozila použitím zamieňanej veci. Ďalším novým oprávnením zvýrazňujúcim bezpečnostný charakter Slovenskej informačnej služby je predstieraný prevod veci. Predstieraným prevodom veci je podľa § 11 ods. 8 zákona o SIS predstieranie kúpy, predaja alebo iného spôsobu prevodu veci, na držanie ktorej sa vyžaduje osobitné povolenie alebo držanie ktorej je zakázané. Podľa cit. ustanovenia je možné vykonať predstieraný pre-

vod veci na základe predchádzajúceho písomného súhlasu sudcu súdu príslušného podľa zákona č. 166/2003 Z. z., ak je to potrebné na účely získania informácie alebo zabránenia vzniku závažnej ujmy na bezpečnosti štátu, hospodárskych záujmoch štátu alebo ochrane utajovaných skutočností. Zákomom č. 444/2015 Z. z. bol do zákona o SIS zavedený aj inštitút zamedzenia prevádzky webového sídla alebo prístupu na doménové meno, ak prevádzkou takéhoto webového sídla alebo doménového mena dochádza k šíreniu myšlienok podporujúcich alebo propagujúcich terorizmus, politický alebo náboženský extrémizmus, extrémizmus prejavujúci sa násilným spôsobom alebo škodlivé sektárske zoskupenia. Túto povinnosť má osoba, ktorá prevádzkuje webové sídlo alebo poskytuje doménové meno, a to na základe príkazu sudcu, ktorý príkaz vydáva na základe žiadosti Slovenskej informačnej služby. Posledným bezpečnostným oprávnením je oprávnenie Slovenskej informačnej služby realizovať primerané bezpečnostné opatrenia, ak je to potrebné na zabránenie aktivitám a ohrozeniam, ktoré spadajú do jej pôsobnosti alebo ak je to potrebné na realizáciu zahraničnopolitických záujmov Slovenskej republiky. Týmto oprávnením však Slovenská informačná služba disponuje od 1. 7. 2010, kedy bol zákon o SIS novelizovaný zákonom č. 151/2015 Z. z. o zahraničnej službe a o zmene a doplnení niektorých zákonov. Zákon neustanovuje definíciu pojmu primerané bezpečnostné opatrenia, a tak na základe výkladu môžeme konštatovať, že ide o akékoľvek opatrenie realizované Slovenskou informačnou službou, rešpektujúc podmienku proporcionality, ktoré je nevyhnutné realizovať na ochranu záujmov Slovenskej republiky.

Ako už bolo uvedené, zákonom č. 444/2015 Z. z. došlo k rozšíreniu, resp. špecifikácii vecnej pôsobnosti Slovenskej informačnej služby. S účinnosťou od 01. 01. 2016 Slovenská informačná služba v rozsahu svojej pôsobnosti získava, sústreďuje a vyhodnocuje informácie o

- a) činnosti ohrozujúcej ústavné zriadenie, územnú celistvosť a zvrchovanosť Slovenskej republiky,
- b) činnosti smerujúcej proti bezpečnosti Slovenskej republiky,
- c) aktivite cudzích spravodajských služieb,
- d) organizovanej trestnej činnosti,
- e) terorizme, vrátane informácií o účasti na terorizme, jeho financovaní alebo podporovaní,
- f) politickom a náboženskom extrémizme, extrémizme prejavujúcom sa násilným spôsobom a škodlivom sektárskom zoskupení,
- g) aktivitách a ohrozeniach v kybernetickom priestore, ak ohrozujú bezpečnosť štátu,
- h) nelegálnej medzinárodnej preprave osôb a migrácii osôb,
- i) skutočnostiach spôsobilých vážne ohroziť alebo poškodiť hospodárske záujmy Slovenskej republiky,
- j) ohrození alebo úniku informácií a vecí chránených podľa osobitného predpisu alebo medzinárodných zmlúv alebo medzinárodných protokolov.

Podľa § 2 ods. 4 zákona o SIS v znení neskorších predpisov plní Slovenská informačná služba v rozsahu svojej pôsobnosti ďalšie úlohy podľa osobitných zákonov a úlohy vyplývajúce z medzinárodných zmlúv a dohôd, ktorými je Slovenská republika viazaná a úlohy z dohôd o spolupráci s orgánmi iných štátov obdobného zamerania a pôsobnosti a medzinárodnými organizáciami.

Pri plnení svojich úloh je Slovenská informačná služba oprávnená používať osobitné prostriedky, ktorými sú

- a) informačno-operatívne prostriedky,
- b) informačno-technické prostriedky,
- c) technické prostriedky,
- d) osobitné finančné prostriedky.

Slovenská informačná služba je za dodržania podmienok ustanovených zákonom č. 166/2003 Z. z. oprávnená používať informačno-technické prostriedky na plnenie úloh v rozsahu celej svojej vecnej pôsobnosti ustanovenej v § 2 zákona o SIS. Ich použitie je podmienené len dodržaním zásad legality, legitimacy a proporcionality a samozrejme subsidiarity zásahu. Zásada proporcionality je vyjadrená v ust. § 3 ods. 1 zákona č. 166/2003 Z. z., podľa ktorého informačno-technický prostriedok možno použiť len vtedy, ak je to v demokratickej spoločnosti nevyhnutné na zabezpečenie ochrany ústavného zriadenia, vnútorného poriadku a zahraničnopolitických záujmov štátu, bezpečnosti a obrany štátu, získavanie informácií zo zahraničných zdrojov, predchádzanie a objasňovanie trestnej činnosti alebo na ochranu práv a slobôd iných a ak dosiahnutie tohto účelu inak by bolo neúčinné alebo podstatne sťažené. Použitím informačno-technického prostriedku sa môže základné právo alebo sloboda obmedziť len v nevyhnutnom rozsahu a nie dlhšie, ako je to nevyhnutné na dosiahnutie zákonom uznaného cieľa, na ktorý slúži. Dodržanie zásady subsidiarity, ktorá je doplnením princípu proporcionality nie je *expressis verbis* upravená ako povinnosť v žiadnom ustanovení zákona č. 166/2003 Z. z. a len konkludentne vyplýva z ust. § 4 ods. 3 písm. b) cit. zákona, podľa ktorého je žiadateľ o udelenie súhlasu, v tomto prípade Slovenská informačná služba, povinný uviesť informácie o predchádzajúcom neúčinnom alebo podstatne sťaženom odhaľovaní a dokumentovaní činnosti, pre ktorú sa podáva žiadosť. Možnosť použitia informačno-technických prostriedkov v pôsobnosti Slovenskej informačnej služby nie je podmienená *expressis verbis* žiadnou úrovňou poznatkov. Je však úlohou príslušného súdu, ako aj Slovenskej informačnej služby dbať na to, aby bola vždy dodržaná zásada legality, legitimacy a proporcionality zásahu do súkromia dotknutej osoby.

Ako už bolo uvedené, použitie informačno-technických prostriedkov v pôsobnosti Slovenskej informačnej služby je obmedzené len rozsahom jej pôsobnosti a nie je obmedzené skutkovými podstatami konkrétnych trestných činov, čo je dôsledkom toho, že Slovenská informačná služba neparticipuje na konaní a ani sa primárne nepodieľa na zisťovaní a odhaľovaní trestnej činnosti. Úlohou Slovenskej informačnej služby je získavanie informácií o hrozbách pre záujmy Slovenskej republiky a jej občanov, ktoré však nemusia bezpodmienečne naplňovať trestnoprávne znaky, resp. naplňovať znaky skutkovej podstaty niektorého trestného činu.

Z § 2 ods. 2 zákona o SIS vyplýva, že Slovenská informačná služba získava, sústreďuje a vyhodnocuje informácie aj o aktivitách, ktoré vznikajú v zahraničí a smerujú proti ústavnému zriadeniu a bezpečnosti Slovenskej republiky a informácie potrebné na realizáciu jej zahraničnopolitických záujmov. Na uvedenú úlohu Slovenskej informačnej služby reflektuje ust. § 3 zákona č. 166/2003 Z. z., ktoré ustanovuje, že informačno-technické prostriedky možno v pôsobnosti Slovenskej informačnej služby použiť aj mimo územia Slovenskej republiky v rozsahu úloh podľa osobitných predpisov.

Zároveň je potrebné na tomto mieste poukázať, že Slovenská informačná služba nie je oprávnená použiť informačno-technický prostriedok bez písomného súhlasu príslušného sudcu udeleného *ex ante*.

III. Výsledok použitia informačno-technického prostriedku

Zo zákonom zavedenej definície informačno-technických prostriedkov je zjavné, že ide o prostriedky a zariadenia alebo ich súbory, ktoré môžu viesť a často aj vedú, vzhľadom na svoju technickú špecifikáciu, k vytvoreniu odlišných výsledkov, avšak vždy vznikne hmotný výsledok. Ako už bolo uvedené, na univerzálny, možno až vágny, charakter definície informačno-technického prostriedku reflektuje § 2 ods. 1 písm. c) zákona č. 166/2003 Z. z., ktorého účelom je subsumovať

pod pojem „iný záznam“ všetky výsledky z použitia informačno-technického prostriedku, ktoré nemožno subsumovať pod obrazový alebo zvukový záznam.

Z pohľadu právnej teórie však možno *in generalis* konštatovať, že výsledkom použitia informačno-technického prostriedku je záznam alebo iný výsledok,² pretože nejde vždy o obrazový, zvukový alebo obrazovo-zvukový záznam. Napríklad pri použití informačno-technického prostriedku podľa § 2 ods. 1 písm. b) zákona č. 166/2003 Z. z. na zaznamenávanie elektronických textových správ, je výsledkom textový prepis znenia správ. Taktiež, ako už bolo uvedené, výsledkom použitia chemického prostriedku ako informačno-technického prostriedku je zlúčenina a nie vyhotovený obrazový záznam o priebehu použitia informačno-technického prostriedku.

Ústavný súd Slovenskej republiky v náleze sp. zn. III. ÚS 97/2012 vyslovil výkladové pravidlo pojmu „iný výsledok“, keď konštatoval, že nevidí príčinnú súvislosť medzi návrhom zničiť všetky písomnosti a predmetom konania, ako bol vymedzený uznesením o prijatí sťažnosti na ďalšie konanie. Ústavný súd Slovenskej republiky konštatoval, že písomnosti, ktoré sú súčasťou súdnych spisov, nevyplývajú z aktívnej činnosti krajského súdu a ani svojím obsahom nie sú výsledkom použitia informačno-technických prostriedkov. Z týchto dôvodov Ústavný súd Slovenskej republiky tomuto návrhu sťažovateľa nevyhovel. Z uvedeného dôvodu nemožno pod pojem „iný výsledok“ subsumovať písomnosti, ktoré sú výsledkom spravodajsko-analytickej činnosti, ale len priame výstupy z použitia informačno-technického prostriedku.

Zároveň je z pohľadu právnej teórie, ako aj praxe, možné rozdeliť výsledky použitia informačno-technických prostriedkov na originárne výsledky, tzv. primárne výsledky a odvodené informácie alebo výsledky, tzv. sekundárne výsledky. Primárnym výsledkom je priamy výstup získaný použitím informačno-technického prostriedku, t. j. v príslušnej technickej podobe prvotný produkt použitia konkrétneho druhu informačno-technického prostriedku. Za primárny výsledok použitia informačno-technického prostriedku je potrebné z dôvodu ochrany dotknutých osôb považovať aj kópiu záznamu alebo iného výsledku z použitia informačno-technického prostriedku a jeho doslovný prepis.

Za sekundárne výsledky z použitia informačno-technických prostriedkov možno považovať produkty spravodajsko-analytickej činnosti, ktoré môžu vychádzať z informácií obsiahnutých v primárnych výsledkoch z použitia informačno-technických prostriedkov a z informácií získaných použitím iných prostriedkov, napr. informačno-operatívnych prostriedkov alebo z inej činnosti spravodajskej služby.

IV. Nakladanie s výsledkami informačno-technického prostriedku³

Kópiu zvukového, obrazového alebo zvukovo-obrazového záznamu (ďalej len „záznam“), ktorý bol vyhotovený použitím informačno-technického prostriedku, možno postúpiť len vecne a miestne príslušnému štátnemu orgánu, ak záznam môže byť dôkazom v konaní vedenom pred príslušným štátnym orgánom v medziach jeho zákonom ustanovenej právomoci. Uvedený zákaz neplatí, ak ide o postúpenie záznamu alebo jeho kópie v rámci spolupráce spravodajských služieb s orgánmi iných štátov obdobného zamerania a pôsobnosti a medzinárodnými organizáciami podľa osobitného predpisu a tiež na účely jeho jazykového prekladu, odtajnenia vrátane jeho dešifrovania alebo dekodovania, ak osoba, ktorej sa má záznam alebo jeho kópia takto poskytnúť, podpíše vyhlásenie o mlčanlivosti. Vecne a miestne príslušný štátny orgán, ktorému bol

² Pozri nálež Ústavného súdu Slovenskej republiky sp. zn. III. ÚS 97/2012.

³ Pozri aj Deset, M.: Prostriedky zabezpečovania informácií dôležitých pre trestné konanie a právo na súkromie, Trnava: Typy Universitatis Tyrnaviensis, 2016.

záznam postúpený, nesmie vyhotoviť kópiu záznamu ani záznam alebo jeho prepis poskytnúť k nahliadnutiu či skopírovaniu inej osobe, inému štátnemu orgánu alebo orgánu územnej samosprávy alebo inej samosprávy. Uvedená výnimka zo zákazu postúpiť záznam bola do zákona č. 166/2003 Z. z. zapracovaná na základe požiadaviek aplikačnej praxe s účinnosťou od 1. 1. 2016 zákonom č. 404/2015 Z. z. ktorým sa mení a dopĺňa zákon o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) v znení neskorších predpisov. Najmä s výrazným nárastom hrozieb nadnárodného charakteru oprávnené orgány štátu, vrátane Slovenskej informačnej služby, získavali z použitia informačno-technických prostriedkov záznamy a iné výsledky, ktoré bolo nevyhnutné preložiť do úradného jazyka, resp. bolo potrebné vykonať iné odborné zásahy (napr. zašifrované informácie), aby bolo možné informácie zo záznamu, resp. iného výsledku spravodajsko-analyticky spracovať.

Považujeme však za dôležité poukázať na to, že cit. ustanovenie nereflektuje na skutočnosť, že z použitia informačno-technického prostriedku môže vzniknúť aj iný výsledok a z dikcie relevantných ustanovení nie je možné vyvodiť záver, či zákonodarca opomenul túto skutočnosť alebo chcel uvedený zákaz naviazať len na kópiu záznamu.

Po použití informačno-technického prostriedku, resp. po spravodajsko-analytickom spracovaní získaných informácií Slovenská informačná služba môže

- a) pokračovať v spravodajskej činnosti, ak je potrebné ďalej rozpracúvať hrozbu,
- b) postúpiť spravodajský produkt zákonným príjemcom, ak je to potrebné na ich rozhodovacie procesy, a naďalej pokračovať v spravodajskej činnosti alebo ju ukončiť, alebo
- c) ukončiť spravodajskú činnosť, ak sa hrozba nepotvrdila a záznamy alebo iné výsledky z použitia informačno-technických prostriedkov zničiť.

V aplikačnej praxi často vyvstáva otázka, či je možné záznamy alebo iné výsledky z použitia informačno-technických prostriedkov podľa zákona č. 166/2003 Z. z. použiť v trestnom konaní. Zastávame názor, že z legislatívneho hľadiska zákonodarca vytvoril podmienky na trestno-procesné využitie tzv. spravodajských záznamov alebo iných výsledkov z použitia informačno-technických prostriedkov. Trestný poriadok v ust. § 119 ods. 2 ustanovuje, že za dôkaz môže slúžiť všetko, čo môže prispieť na náležité objasnenie veci a čo sa získalo z dôkazných prostriedkov podľa tohto zákona alebo podľa osobitného zákona. Týmto osobitným predpisom je, okrem iných, práve zákon č. 166/2003 Z. z., ktorý túto možnosť *expressis verbis* ustanovuje v § 7 ods. 2, podľa ktorého, ak sa majú informácie získané použitím informačno-technického prostriedku použiť ako dôkaz v trestnom konaní, vyhotoví orgán štátu písomný záznam s uvedením údajov o mieste, čase a zákonnosti použitia informačno-technického prostriedku. K písomnému záznamu orgán štátu priloží záznam a jeho doslovný prepis. Informácie získané použitím informačno-technického prostriedku, ktoré sa nevzťahujú na dôvody jeho použitia uvedeného v žiadosti, sa môžu použiť ako dôkaz v trestnom konaní, len ak sa týkajú trestnej činnosti, v súvislosti s ktorou možno použiť informačno-technický prostriedok. Z citovaných ustanovení jednoznačne vyplýva vôľa zákonodarcu vytvoriť orgánom činným v trestnom konaní a spravodajským službám legislatívnu možnosť použiť informácie získané zákonným spôsobom podľa zákona č. 166/2003 Z. z. pri plnení zákonom ustanovených úloh na úseku ochrany ústavného zriadenia, vnútorného poriadku a bezpečnosti a na úseku boja proti zločinnosti. Je nepochybné, že oba dotknuté zákony, a to Trestný poriadok ako aj zákon č. 166/2003 Z. z., naplňajú požiadavku legality, legitimacy a proporcionality zásahu do súkromia s dôrazom na subsidiárny charakter tohto zásahu a na obligatórnu aprobáciu zásahu príslušným sudcom.

Pri možnosti využitia informácií získaných z použitia informačno-technických prostriedkov podľa zákona č. 166/2003 Z. z. v trestnom konaní je potrebné prihliadať aj na záujmy spoločnos-

ti a na úlohy trestného práva. Aj keď právo na súkromie je jedno z najdôležitejších práv osoby, nie je možné ho vykladať extenzívne a dogmaticky a nadradovať ho nad ostatné práva. Pri výklade cit. ustanovení Trestného poriadku a zákona č. 166/2003 Z. z. je dôležité prihliadať nie len na záujmy dotknutého jednotlivca, t. j. na právo na súkromie, ale aj na záujem verejnosti na zisťovaní a vyšetrovaní trestných činov a následnom zákonnom potrestaní ich páchatel'ov.

Ak sa nedosiahol zákonom ustanovený účel, t. j. použitím nezistili sa skutočnosti významné na dosiahnutie zákonom ustanoveného účelu použitia informačno-technického prostriedku, orgán štátu, ktorý záznam vyhotovil, je povinný bezodkladne záznam zničiť. Povinnosť zničiť záznam, resp. iný výsledok z použitia informačno-technického prostriedku má štátny orgán aj vtedy, ak sa informačno-technický prostriedok použil v rozpore so zákonom č. 166/2003 Z. z. (napr. bez súhlasu sudcu, použil sa informačno-technický prostriedok, ktorý nespĺňa podmienky podľa § 2 ods. 5 cit. zákona), a to do 24 hodín od protiprávneho použitia informačno-technického prostriedku. Pri ničení záznamu alebo iného výsledku z použitia informačno-technického poriadku je obligatórna prítomnosť príslušného sudcu. Keďže došlo k porušeniu zákonnosti použitia informačno-technického prostriedku, zákonodarca ustanovil povinnú účasť sudcu pri ničení záznamu, aby tým poskytol ochranu dotknutým osobám.

Je dôležité, že povinnosť zničiť sa viaže len na záznam a iný výsledok použitia informačno-technického prostriedku, t. j. primárny výsledok. Povinnosť zničiť sa nevzťahuje na sekundárne výsledky z použitia informačno-technického prostriedku, ktoré sú výsledkom spravodajsko-analytickej činnosti. S týmito sekundárnymi výsledkami z použitia informačno-technických prostriedkov je potrebné naložiť podľa § 17 ods. 6 zákona o SIS, podľa ktorého ak údaje uchovávané v evidenciách už nie sú na plnenie ustanovených úloh potrebné, alebo ak je na to iný zákonný dôvod, je Slovenská informačná služba oprávnená tieto údaje uložiť spôsobom, ktorý zabráni každému, okrem súdu, v prístupe k nim. Z cit. ustanovenia vyplýva pre Slovenskú informačnú službu zákaz akýmkoľvek iným spôsobom nakladať s údajmi obsiahnutými v evidenciách (a informačných systémoch), t. j. aj so sekundárnymi výsledkami z použitia informačno-technických prostriedkov. Slovenská informačná služba bola oprávnená údaje ničiť do 18. 10. 1999. Uvedené oprávnenie jej zaniklo s účinnosťou zákona č. 73/1998 Z. z. o štátnej službe príslušníkov Policajného zboru, Slovenskej informačnej služby, Zboru väzenskej a justičnej stráže Slovenskej republiky a Železničnej polície, ktorým sa zároveň menil zákon o SIS.

Zoznam použitej literatúry

1. Čentéš, J.: *Odpočúvanie – procesnoprávne a hmotnoprávne aspekty*, Praha: C. H. Beck, 2016, s. 250, ISBN: 978-80-8960-309-1
2. Deset, M.: *Prostriedky zabezpečovania informácií dôležitých pre trestné konanie a právo na súkromie*, Trnava: Typy Universitatis Tyrnaviensis, 2016, ISBN 978-80-8082-995-7
3. Kyjac, Z.: *Použitie informačno-technických prostriedkov v trestnom konaní, Odpočúvanie a záznam telekomunikačnej prevádzky*, Bratislava: Wolters Kluwer, 2015, s. 307, ISBN 978-80-8168-266-7

Využitie informácií získaných prostredníctvom ITP v „netrestnej veci“¹

Using of Information Obtained by Technical Means in a “Non-criminal Case”

Jozef Záhora²

Abstrakt: Použitím informačno-technických prostriedkov sa výrazne zasahuje do práva na súkromie. Právo na súkromný život v sebe zahŕňa aj právo na ochranu pred sledovaním zo strany verejnej moci. Autor poukazuje na niektoré problémy pri využívaní výsledkov získaných informačno-technickými prostriedkami podľa Trestného poriadku v konaní, ktoré nie je trestným činom.

Abstract: The use of means of information of technical resources significantly interferes with the right to privacy. The right of private life implies a right to protection against persecution on the public authorities by monitoring. The author focuses the problems using the results obtained by technical means of information according to the Criminal Procedure Code in “non-criminal case”.

Kľúčové slová: dôkaz, odpočúvanie telekomunikačnej prevádzky, obrazovo-zvukový záznam informačno-technické prostriedky, disciplinárne konanie.

Key words: Evidence, Interception of Communications, Video and Audio record, Means of Information of Technical Resources, Disciplinary Proceedings.

Úvod

Používaním informačno-technických prostriedkov sa vážne zasahuje do práva na súkromie. V zmysle ustálenej judikatúry Ústavného súdu Slovenskej republiky (*ďalej len „Ústavný súd“*) sa súkromím rozumie predovšetkým sféra života človeka, do ktorej nemožno zasahovať bez jeho súhlasu. Právom na súkromie sa zaručuje osobe možnosť rozhodovať samostatne o tých svojich záležitostiach, ktoré sa uznávajú za súkromie. Právo na ochranu pred neoprávneným zasahovaním do súkromnej sféry jednotlivca obsahuje nielen negatívnu povinnosť štátu zdržať sa mocenského zásahu, ale aj jeho pozitívny záväzok prijať účinné opatrenia na zabezpečenie jeho efektívnej ochrany.³ Právo na súkromný život tak v sebe zahŕňa i právo na ochranu pred sledovaním, striehnutím a prenasledovaním zo strany verejnej moci, a to i vo verejnom priestore či na verejne prístupných miestach. Európsky súd pre ľudské práva (*ďalej len „Európsky súd“*) vo svojej judikatúre k právu na rešpektovanie súkromného života podľa čl. 8 Dohovoru o ochrane ľudských práv a základných slobôd⁴ (*ďalej len „Európsky dohovor“*) označil za zásahy do súkromia jednotlivca intervencie v podobe kontroly dát, obsahu pošty či odpočúvaní telefónnych rozhovorov, zisťovanie telefónnych čísel telefonujúcich osôb, zisťovanie údajov o telefónnom spojení.⁵

¹ Táto práca bola podporovaná Agentúrou na podporu výskumu a vývoja na základe Zmluvy č. APVV-15-0272.

² Prof. JUDr. Jozef Záhora, PhD., Ústav verejného práva, Fakulta práva, Paneurópska vysoká škola, e-mail: jozef.zahora@paneurouni.com.

³ Napr. Uznesenie Ústavného súdu Slovenskej republiky, sp. zn. PL. ÚS 10/2014-29, z 29. apríla 2015, Uznesenie Ústavného súdu Slovenskej republiky sp. zn. PL. ÚS 40/2015-20, z 9. septembra 2015.

⁴ Dohovor o ochrane ľudských práv a základných slobôd a Protokolov na tento Dohovor nadväzujúcich, Oznámenie MZV č. 209/1992 Z. z. v znení oznámení č. 102/1999 Z. z., 143/2001 Z. z., 480/2005 Z. z., 208/2010 Z. z.

⁵ Nález Pléna Ústavného súdu Slovenskej republiky sp. z. PL. ÚS 10/2014 z 29. apríla 2015.

Ako aj iné dôkazy, aj dôkazy získané prostredníctvom informačno-technických prostriedkov podliehajú dôkladnému hodnoteniu. Dôkazy sa hodnotia na základe zásady voľného hodnotenia dôkazov, v zmysle ktorej „Orgány činné v trestnom konaní a súd hodnotia dôkazy získané zákonným spôsobom podľa svojho vnútorného presvedčenia založeného na starostlivom uvážení všetkých okolností prípadu jednotlivo i v ich súhrne nezávisle od toho, či ich obstaral súd, orgány činné v trestnom konaní alebo niektorá zo strán.“ Okrem legislatívneho vyjadrenia v § 2 ods. 4 Trestného poriadku č. 301/2005 Z. z. v znení neskorších predpisov (*ďalej len „Trestný poriadok“*), na rozdiel od iných zásad trestného konania, výslovné zakotvenie tejto zásady nenachádzame v ústavných predpisoch.⁶

Podstatou zásady voľného hodnotenia dôkazov je, že orgány činné v trestnom konaní a súd nemajú zákonom stanovené aké množstvo dôkazov a akých dôkazov je potrebné vykonať na preukázanie potrebných skutočností a v zásade neuvádzajú ani druhy dôkazných prostriedkov, ktoré sa majú použiť. Inak povedané, že ani jeden z dôkazov nemá dopredu určenú dôkaznú silu a hodnotu a zároveň Trestný poriadok nestanovuje ani potrebný počet dôkazov k preukázaniu skutkového stavu bez dôvodných pochybností.⁷

Aj napriek tomu, že pri utváraní vnútorného presvedčenia významnú úlohu zohráva subjektívny faktor, nemožno prehliadnuť skutočnosť, že obsahom hodnotenia sú objektívne zistiteľné kritériá, najmä:⁸

- otázka prípustnosti prameňa dôkazov zákonnosti procesného postupu pri dokazovaní,
- vzťah dôkaznej informácie k dokazovanej skutočnosti,
- či je dôkaz pravdivý, presvedčivý a vierohodný,
- dôkazný význam získanej informácie z hľadiska cieľa dokazovania,
- či dôkaz možno využiť pre získanie ďalších dôkazov v dokazovanej veci.

Ako už bolo uvedené, jedným zo základných objektívnych kritérií hodnotenia dôkazov je aj **prípustnosť dôkazu**, ktorá znamená, že určitý element dokazovania je spôsobilý na základe práva podporiť alebo vyvrátiť určité tvrdenia (nároky) a sudca ho nemôže a priori odmietnuť. Z predmetného výroku vyplýva skutočnosť, že Trestný poriadok v ustanovení § 119 ods. 2 nedovoľuje vylúčiť uplatnenie žiadneho dôkazného prostriedku získaného v súlade so zákonom,⁹ na druhej strane v niektorých prípadoch výslovne zakazuje použitie niektorých dôkazov. Vo vzťahu ku skúmanej problematike **informačno-technických prostriedkov** ide predovšetkým o nasledovné prípady:¹⁰

1. Využitie dôkazu získaného **vyhotovením obrazových, zvukových alebo obrazovo-zvukových záznamov v inej trestnej veci**. (*V inej trestnej veci, ako je tá, v ktorej boli vyhotovené obrazové, zvukové alebo obrazovo-zvukové záznamy, možno záznam ako dôkaz použiť len vtedy, ak sa súčasne aj v tejto veci vedie trestné konanie pre úmyselný trestný čin, na ktorý zákon ustanovuje trest odňatia slobody s hornou hranicou trestnej sadzby prevyšujúcou tri roky, korupciu, trestný čin zneužívania právomoci verejného činiteľa, trestný čin legalizácie*

⁶ Pozri JELÍNEK, J. a kol. *Trestní právo procesní*. Praha, Leges, 2010, s. 150.

⁷ Bližšie ŠÁMAL, P., NOVOTNÝ, F., RŮŽIČKA, M., VONDRUŠKA, F., NOVOTNÁ, J. *Přípravné řízení trestní*. 2. vyd. Praha: C. H. Beck, 2003. s. 69.

⁸ porovnaj napr. MATHERN, V. *Dokazovanie v československom trestnom procese*. Bratislava, Obzor, 1984, s. 102, IVOR, J., POLÁK, P., ZÁHORA, J. *Trestné právo procesné I*. Wolters Kluwer, Bratislava 2017, s. 420.

⁹ ŠÁMAL, P., NOVOTNÝ, F., RŮŽIČKA, M., VONDRUŠKA, F., NOVOTNÁ, J. *Přípravné řízení trestní*. 2. vyd. Praha: C. H. Beck, 2003. s. 800.

¹⁰ podľa ZÁHORA, J. *Nepřípustnost důkazu získaného donútením*. In. Teoretické a praktické problémy dokazovania – pocta prof. JUDr. Vladimírovi Mathernovi, DrSc. k 80. narodeninám. Zborník príspevkov z celoštátnej konferencie s medzinárodnou účasťou konanej dňa 15. decembra 2008, Bratislavská vysoká škola práva, Bratislava 2008, s. 291–302.

príjmu z trestnej činnosti alebo pre iný úmyselný trestný čin, o ktorom na konanie zaväzuje medzinárodná zmluva.)¹¹

2. Využitie dôkazu získaného pri odpočúvaní a zaznamenávaní telekomunikačnej prevádzky **v inej trestnej veci**. (*V inej trestnej veci, ako je tá, v ktorej sa odpočúvanie a záznam telekomunikačnej prevádzky vykonal, možno záznam ako dôkaz použiť len vtedy, ak sa súčasne aj v tejto veci vedie trestné konanie pre trestný čin uvedený v odseku 1.)¹²*

Zo znenia § 114 ods. 7 resp. § 115 ods. 7 Trestného poriadku vyplýva obmedzenie možnosti použitia záznamu ako dôkazu v inej trestnej veci len v **trestnom konaní**. Problematika využitia dôkazu „v inej trestnej veci“ je v praxi polemická a vyskytujú sa rôzne názory. V tejto súvislosti sa možno stretnúť s názorom, že slovo „súčasne“ sa vzťahuje až k okamihu použitia výsledku odpočúvania ako dôkazu v inej trestnej veci (a nie k okamihu vykonávania odpočúvania), pretože § 115 ods. 7 Trestného poriadku upravuje len použitie záznamu telekomunikačnej prevádzky a nie vykonanie odpočúvania. Pri tomto postupe sa vychádza z toho, že dôkaz zabezpečený na základe legálneho odpočúvania nemožno objektívne opakovať.¹³

Rozhodovacia činnosť slovenských súdov nie je v tomto smere jednoznačná. Podľa jedného rozhodnutia¹⁴ je potrebné slovo súčasne „vzťahovať až k okamžiku použitia výsledkov odposluchu a nie už k okamihu vykonávania odposluchu.“ **Opačný názor** vyslovil Najvyšší súd v publikovanom rozhodnutí,¹⁵ kde súd zdôrazňuje, že súčasným vedením trestného konania v inej trestnej veci v zmysle citovaného rozhodnutia sa rozumie úkon, rozhodnutie alebo iný postup, vykonaný na základe Trestného poriadku, ku ktorému v inej trestnej veci došlo **pred zabezpečením dotknutej dôkaznej informácie** vo veci, v ktorej bol tento postup nariadený (jej zabezpečením sledovaním osôb a vecí, vyhotovením obrazového, zvukového alebo obrazovo-zvukového záznamu, odpočúvaním a záznamom telekomunikačnej prevádzky, alebo porovnaním údajov v informačných systémoch). Inou trestnou vecou sa rozumie trestné konanie (aj pred začatím trestného stíhania) pre iný skutok, kvalifikovaný ako trestný čin.¹⁶

Táto nejednotnosť viedla k rozdielnemu výkladu ustanovenia § 115 ods. 7 Trestného poriadku v odlišných rozhodnutiach dvoch senátov trestnoprávneho kolégia Najvyššieho súdu Slovenskej republiky. Hoci v roku 2012 bol pripravený návrh zjednocujúceho stanoviska pod č. Tpj 34/2012, Trestnoprávne kolégium Najvyššieho súdu sa predmetnou problematikou zaoberalo na dvoch zasadnutiach 11. júna 2012 a 10. decembra 2012, k uvedenej problematike na žiadosť z týchto rokovaní nedokázalo prijať zjednocujúce stanovisko.¹⁷

Vzhľadom na to, že v odbornej literatúre sú jednotlivé argumenty dostatočne spracované,¹⁸ tejto problematike sa nebudem bližšie venovať, v ďalšom texte svoju pozornosť zameriam na

¹¹ § 114 ods. 7 Trestného poriadku.

¹² § 115 ods. 7 Trestného poriadku.

¹³ Bližšie IVOR, J. *Využitie záznamu z odpočúvania ako dôkaz v trestnom konaní*. In: *Dokazovanie v civilnom a trestnom konaní*. Pezinok: Justičná akadémia Slovenskej republiky, 2012, s. 208.

¹⁴ Uznesenie Najvyššieho súdu Slovenskej republiky sp. zn. 3To 2/2011 z 21. 9. 2011.

¹⁵ Rozsudok Najvyššieho súdu Slovenskej republiky sp. zn. 2To 5/2011 z 7. 2. 2012.

¹⁶ Bližšie ZÁHORA, J. *Použitie záznamu získaného odpočúvaním ako dôkazu v inej trestnej veci*. In: JELÍNEK, J. a kol. *Trestní právo procesní – minulost a budoucnost*. Praha: Leges, 2016, s. 167.

¹⁷ ČENTĚŠ J. *Odpočúvanie – procesnoprávne a hmotnoprávne aspekty*. Bratislava: C. H. Beck, 2013, s. 127.

¹⁸ Napr. ŠÁMAL, P. *Odposlech a záznam telekomunikačního provozu ve světle judikatury*. In: *Soudní rozhledy* č. 3/2000, s. 69 a nasl., KYBIC, P. *K otázce použití odposlechu a záznamu telekomunikačního provozu jako důkazu v jiné trestní věci*. In: *Trestněprávní revue* č. 4/2002, s. 114 a nasl., ČENTĚŠ, J. *Právna úprava odpočúvania a záznamu telekomunikačných činností po novele Trestného poriadku*. In: *Justičná revue* č. 2/2003, s. 172–178, PERHÁCS, Z. *O zničení záznamov získaných použitím informačno-technických prostriedkov*. In: *Justičná revue* č. 5/2007, s. 642 a nasl., ČENTĚŠ, J. *K odpočúvaniu a zaznamenávaniu telefonického rozhovoru*. In: *Justičná revue* č. 5/2009, s. 603 a nasl., PERHÁCS, Z., ZAJONC, A. *Poznámky k sledovaniu, priestorovému a telefonickému odposluchu*. In: *Justičná revue* č. 8–9/2011, s. 1138 a nasl., IVOR, J. *Využitie záznamu z odpočúvania ako dôkaz*

aplikačné problémy využitia dôkazu získaného prostredníctvom informačno-technických prostriedkov podľa Trestného poriadku v inom ako trestnom konaní, predovšetkým v konaní o prepustení príslušníka ozbrojeného zboru zo služobného pomeru.

Rozhodovacia činnosť slovenských súdov

Znenie ustanovení § 114 ods. 7 resp. § 115 ods. 7 Trestného poriadku „v inej trestnej veci“, rigorózne a obmedzuje, že záznamy nemožno použiť **v iných trestných veciach**, pokiaľ sa súčasne v týchto veciach nevedie trestné konanie. Z citovaných ustanovení Trestného poriadku vyplýva, že záznam sa môže prostredníctvom informačno-technických prostriedkov vyhotoviť v trestnom konaní iba pre účely trestného konania a len v prípadoch niektorých výslovne uvedených trestných činov (zločinov a ďalších vymenovaných trestných činov) pri súčasnom dodržaní predpísaných procesných podmienok. Argumentom *a contrario* možno dospieť k záveru, že použitie záznamu vyhotoveného v trestnom konaní za použitia informačno-technických prostriedkov **v inom ako trestnom konaní je vylúčené**. Právna úprava neumožňuje záznamy z legálneho odpočúvania použiť ako dôkaz v disciplinárnom konaní, napr. v súvislosti s prepustením zo služobného pomeru.¹⁹

Aj napriek tomu, v rozhodnutiach slovenských súdov sa vyskytujú aj rozhodnutia, ktoré posudzovali zákonnosť dôkazov, konkrétne informačno-technických prostriedkov vykonaných podľa Trestného poriadku v konaní v „netrestnej veci“, konkrétne v konaní o prepustení policajta resp. colníka zo služobného pomeru. Bolo vydané viacero rozhodnutí všeobecných súdov.²⁰

V rámci rozhodovacej činnosti²¹ sa Ústavný súd zaoberal prípustnosťou využitia získaného dôkazu vyhotovovaním obrazovo-zvukových záznamov a následnom využití takýchto záznamov vo veci prepustenie colníka zo služobného pomeru. Sťažovateľ bol prepustený zo služobného pomeru z dôvodu, že mal zvlášť hrubým spôsobom porušiť základné povinnosti colníka. Rozhodnutie colného úradu sa odvoláva na výpisky riaditeľa z obrazovo-zvukového záznamu, ktorý sprístupnil vyšetrovateľ inšpekcie v rámci trestného konania.

Ústavný súd zdôrazňuje, že procesné ustanovenie, podľa ktorého za dôkaz môžu slúžiť všetky prostriedky, ktorými možno zistiť a objasniť skutočný stav veci, pokiaľ sú v súlade s právnymi predpismi, treba z ústavnoprávneho hľadiska považovať za kolíziu verejného záujmu a ochrany práv. Ide totiž o stret medzi verejným záujmom na dôslednom objasnení rozhodujúcich skutočností potrebných na vydanie rozhodnutia v konaní a ochranou určitých práv, resp. oprávnených záujmov, ktoré bránia použitiu niektorého dôkazného prostriedku. Vo všeobecnej rovine možno konštatovať, že prednosť má verejný záujem na dôslednom objasnení rozhodujúcich skutočností potrebných na vydanie rozhodnutia, avšak za súčasného spolupôsobenia brzd daných s ohľadom na ochranu určitých práv, resp. oprávnených záujmov. Tým je dané, že nie všetky prostriedky, pomocou ktorých by objektívne bolo možné zistiť a objasniť skutočný stav veci, sa smú použiť v príslušnom konaní. Z ustanovenia § 114 ods. 7 Trestného poriadku vyplýva zásadný zákaz použitia obrazovo-zvukového záznamu získaného v rámci konkrétneho trest-

v trestnom konaní. In: Dokazovanie v civilnom a trestnom konaní: Pezinok: Justičná akadémia Slovenskej republiky, 2012, s. 204–214, ZÁHORA, J. Použitie záznamu získaného odpočúvaním ako dôkazu v inej trestnej veci. In: JELÍNEK, J. a kol. Trestní právo procesní – minulost a budoucnost. Praha: Leges, 2016, s. 162–174.

¹⁹ Porovnaj PERHÁCS, Z., ZAJONC, A. Poznámky k sledovaniu, priestorovému a telefonickému odposluchu. In: Justičná revue. č. 8–9/2011, s. 1140.

²⁰ Napr. Rozsudok Krajského súdu v Bratislave sp. zn. 4S/59/2009-105 zo dňa 14. mája 2010, Rozsudok Krajského súdu v Bratislave sp. zn. 3S 257/2011-100 zo dňa 13. novembra 2012.

²¹ Nález Ústavného súdu Slovenskej republiky z 15. decembra 2011, sp. zn. II. ÚS 5/2011.

ného konania v inom trestnom konaní, avšak s určitými taxatívne vymenovanými výnimkami. Trestný poriadok upravuje matériu získavania a použitia obrazovo-zvukových záznamov zhotovených informačno-technickými prostriedkami iba v rámci trestného konania. Naproti tomu získavanie a použitie obrazovo-zvukových záznamov zhotovených informačno-technickými prostriedkami v iných konaniach, resp. pre účely iných konaní upravuje zákon o ochrane pred odpočúvaním.²²

V náleze **IV. ÚS 519/2012** z 24. júla 2013 Ústavný súd opakuje vyššie uvedenú argumentáciu a dopĺňa ju. Ústavný súd konštatuje, že rozhodujúce sú námietky sťažovateľa, ktoré sa týkajú obrazovo-zvukového záznamu získaného v trestnom konaní a jeho použitia v správnom konaní. Uvedené námietky sú totiž logicky a vecne prepojené a je potrebné skúmať ich v poradí, ktoré rešpektuje ich vzájomný vzťah. Z tohto pohľadu je rozhodujúce skúmať v prvom rade námietku **použiteľnosti obrazovo-zvukového záznamu v správnom konaní**, teda námietku prípustnosti tohto dôkazu v namietanom správnom konaní. Až následne má zmysel skúmať, či **spôsob získania tohto dôkazu pre účely správneho konania bol v súlade s právnymi predpismi** (teda nahliadnutie riaditeľa colného úradu do trestného spisu, vyhotovenie úradného záznamu a pod.), a tiež, či tento dôkaz bol vykonaný v správnom konaní, prípadne krajským súdom a najvyšším súdom spôsobom, ktorý bol zákonný a ústavne udržateľný (či sťažovateľ bol oboznámený s predmetným dôkazom, či mal dostatočnú možnosť sa k tomuto dôkazu vyjadriť a pod.).

Ústavný súd je toho názoru, že záver o legalite zásahu možno urobiť až na základe dôsledného preskúmania vzájomného vzťahu § 227 ods. 1 zákona o štátnej službe colníkov na jednej strane a § 114 Trestného poriadku a príslušných ustanovení zákona o ochrane pred odpočúvaním na strane druhej, čo zásadne patrí do pôsobnosti všeobecných súdov. Formulovanie výslovného právneho názoru k tejto otázke považuje ústavný súd za zásadné pre ďalší postup najvyššieho súdu. Skúmanie legitimacy a proporcionality zásahu prichádza totiž do úvahy až po konštatovaní legality zásahu. Pretože táto otázka bola a aj je rozhodujúca nielen pre posúdenie zákonnosti použitia obrazovo-zvukového záznamu z trestného konania v správnom konaní, ale aj posúdenie, či ním mohlo dôjsť k porušeniu základných práv sťažovateľa, bolo povinnosťou najvyššieho súdu podať ústavne konformný výklad k aplikácii dvoch kolidujúcich právnych úprav rovnakého stupňa právnej sily. Bez neho je totiž rozsudok najvyššieho súdu nedostatočne odôvodnený, čo spôsobuje v konečnom dôsledku jeho nepreskúmatelnosť. Bez zaujatia stanoviska k tejto kľúčovej právnej otázke relevantnej pre posúdenie ústavnosti namietaného rozhodnutia takéto odôvodnenie neposkytuje ústavne udržateľný podklad pre namietaný rozsudok najvyššieho súdu v spojení s rozsudkom krajského súdu. Na tomto základe ústavný súd rozhodol, že namietaným rozsudkom najvyššieho súdu a postupom, ktorý predchádzal jeho vydaniu, bolo porušené základné právo sťažovateľa na súdnu ochranu podľa čl. 46 ods. 1 ústavy (bod 1 výroku tohto nálezu). Vychádzajúc z toho, že otázka prípustnosti obrazovo-zvukového záznamu z trestného konania v inom (správnom) konaní bola rozhodujúca, nebolo už potrebné osobitne sa zaoberať ďalšími námietkami sťažovateľa.

U vedených intenciách sú odôvodňované aj rozhodnutia všeobecných súdov napr. uznesenie Najvyššieho súdu²³ rozsudok Krajského súdu Košice.²⁴

Citované uznesenie Najvyššieho súdu 3 Sžo/10/2012 riešilo zásadnú otázku a to: „**či je právne prípustné pre účely zistenia porušenia služobnej disciplíny colníka alebo policajta, ktoré sa skutkovo prekrýva s dôvodným podozrením zo spáchania trestného činu, použiť v kona-**

²² Zákon č. 199/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním).

²³ Uznesenie Najvyššieho súdu Slovenskej republiky sp. zn. 3 Sžo/10/2012 z 5. júna 2012.

²⁴ Rozsudok Krajského súdu Košice, sp. zn. 6S/97/2009 zo dňa 28. 6. 2012.

ní o skončenie služobného pomeru obrazovo-zvukový záznam (ITP) získaný v jeho trestnej veci, v trestnom konaní z vyšetrovacieho spisu.“

Najvyšší súd dospel k záveru, že ustanovenie 114 ods. 7 Trestného poriadku, ktoré upravuje využitie dôkazu v inej trestnej veci uvedené ustanovenie nie je v rámci súdneho prieskumu zákonnosti relevantné a ani Trestný poriadok nie je prameňom správneho práva, pokiaľ niektorý z právnych predpisov, ktoré sú prameňom správneho práva na použitie Trestného poriadku neodkazuje. Ak ide o údaje získané v trestnom konaní je potrebné jednoznačne uviesť ustanovenia dotknutých právnych predpisov alebo iných prameňov práva, **ktoré bránia ich použitiu v konaní** o skončenie služobného pomeru colníka. Zákon o ochrane pred odpočúvaním je relevantným predpisom i pre správne konanie o skončenie služobného pomeru colníka. Najvyšší súd ďalej pokračuje, že zákon o ochrane pred odpočúvaním²⁵ v § 3 ods. 1 umožňuje použiť informačno-technický prostriedok iba vtedy, „ak je to v demokratickej spoločnosti nevyhnutné na zabezpečenie bezpečnosti štátu, obranu štátu, **predchádzanie a objasňovanie trestnej činnosti** ...“. Predchádzanie trestnej činnosti colníkov pri výkone ich služby a v mieste výkonu služby je relevantným dôvodom pre použitie informačno-technického prostriedku. Najvyšší súd vychádza zo skutočnosti, že nevyhnutnosť ich použitia vyplýva i z okolností tohto prípadu, na vonkajšej hranici colného územia EU s Ukrajinou.

Vo vzťahu k Trestnému poriadku Najvyšší súd **nezistil existenciu ustanovenia Trestného poriadku, ktoré by zakazovalo použitie obrazovo-zvukového záznamu v inom ako trestnom konaní**. Ustanovenie § 114 ods. 7 Trestného poriadku používa pojem „v inej trestnej veci“ a nie pojem v „inej veci“. To znamená, že použitie záznamu je obmedzené, ak vedie k trestnej zodpovednosti. Trestná zodpovednosť má však prísnejšie podmienky na uplatnenie ako disciplinárna zodpovednosť colníkov, ktorí podliehajú služobnej disciplíne.

Diskusia

S vyššie uvedeným závermi Najvyššieho súdu „**Najvyšší súd nezistil existenciu ustanovenia Trestného poriadku, ktoré by zakazovalo použitie obrazovo-zvukového záznamu v inom ako trestnom konaní.**“ nemožno v zásade súhlasiť.

Citované ustanovenie § 114 ods. 7 Trestného poriadku sa zaoberá problematikou využitia dôkazu v trestnej veci nie v konaní o prepustení policajta. Podľa § 238 zákona o štátnej službe príslušníkov Policajného zboru...²⁶ „*Za dôkaz môžu slúžiť všetky prostriedky, ktorými možno zistiť a objasniť skutočný stav veci a ktoré sú v súlade s právnymi predpismi.*“ Rovnako ako Trestný poriadok aj citovaná právna norma kladie dôraz na **zákonnosť dôkazu**.²⁷

Pri argumentácii si pomôžem aj stanoviskom českého Štátneho zastupiteľstva.²⁸ Orgány činné v trestnom konaní nemôžu údaje získané odpočúvaním a záznamom telekomunikačnej prevádzky pre účely trestného konania poskytovať iným orgánom pre iné účely, teda ani súdu pre účely civilného konania. Poskytovanie takýchto informácií iným osobám Trestný poriadok **neumožňuje**, čo možno to dovodiť z ustanovenia o nazeraní do spisu.

²⁵ Zákon č. 199/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním).

²⁶ Zákon č. 73/1998 Z. z. o štátnej službe príslušníkov Policajného zboru, Slovenskej informačnej služby, Zboru väzenskej a justičnej stráže Slovenskej republiky a Železničnej polície v z nej neskorších predpisov.

²⁷ MATHERN, V. *Dokazovanie v československom trestnom procese*. Bratislava: Obzor, 1984, s. 107.

²⁸ Stanovisko ke sjednocení výkladu zákonů a jiných právních předpisů k poskytování údajů z odposlechu a záznamu telekomunikačního provozu pořízených pro účely trestního řízení jiným orgánům Sběrka výkladových stanovisek nejvyššího státního zastupitelství 3/2006 zo dňa 11. decembra 2006.

Ak bol predmetný informačno-technický prostriedok vyhotovený pre účely trestného konania, nie je možné sa k takejto informácii dostať „legálnym spôsobom.“ Trestný poriadok v § 69 umožňuje nazerať do spisu nasledovným subjektom:²⁹

1. obvinený, jeho obhajca, poškodený a zúčastnená osoba, splnomocnenec, ustanovený opatrovník, v konaní pred súdom prokurátor, probačný a mediačný úradník, vyšší súdny úradník a súdny tajomník, asistent prokurátora, zákonný zástupca obvineného, poškodeného a zúčastnenej osoby, ak tieto osoby sú pozbavené spôsobilosti na právne úkony alebo ich spôsobilosť na právne úkony je obmedzená,
2. iné osoby iba so súhlasom predsedu senátu a v prípravnom konaní so súhlasom orgánu činného v trestnom konaní, len ak je to potrebné na uplatnenie ich práv. Do úvahy prichádzajú najmä osoby, ktoré môžu v prospech obvineného podať opravný prostriedok [napr. príbuzní obvineného v priamom rade, jeho súrodenec, osvojiteľ, manžel alebo druh (§ 186 ods. 2, § 308 ods. 2, § 369 ods. 5) Trestného poriadku],
3. znalec, znalcovi treba umožniť, aby sa v potrebnom rozsahu oboznámil s obsahom spisu, najmä s vykonanými dôkazmi (§ 145 ods. 1 Trestného poriadku),

Okrem týchto osôb, do trestných spisov môžu v zmysle § 69 ods. 4 Trestného poriadku nazerať aj štátne orgány s oprávnením podľa osobitného zákona v zmysle predovšetkým:

- verejný ochranca práv (§ 17 ods. 8 zákona č. 564/2001 Z. z. o verejnom ochrancovi práv v znení neskorších predpisov),
- nadriadený prokurátor (§ 55 zákona č. 153/2001 Z. z. o prokuratúre v znení neskorších predpisov),
- zamestnanci Ministerstva spravodlivosti SR pri preverovaní skutočností dôležitých pre rozhodnutie o podanej žiadosti o odškodnenie (§ 10 zákona č. 215/2006 Z. z. o odškodňovaní osôb poškodených násilnými trestnými činmi),
- národný člen Eurojustu [§ 4 ods. 1 písm. e) zákona č. 383/2011 Z. z. o zastúpení Slovenskej republiky v Eurojuste],
- Protimonopolný úrad Slovenskej republiky (§ 22 ods. 3 republiky zákona č. 136/2001 Z. z. o ochrane hospodárskej súťaže [...] v znení neskorších predpisov),
- členovia oddelení vnútornej revízie súdu (§ 56 zákona č. 757/2004 Z. z. o súdoch a o zmene a doplnení niektorých zákonov).

Žiadny z predpisov neumožňuje nadriadenému v konaní o prepustení policajta alebo colníka nahliadať do „živého“ trestného spisu. Nemožno súhlasiť s citovaným názorom Najvyššieho súdu *nezistil existenciu ustanovenia Trestného poriadku, ktoré by zakazovalo použitie obrazovo-zvukového záznamu v inom ako trestnom konaní*.

Je tu potrebné zdôrazniť, že z hľadiska zodpovednosti orgánov činných v trestnom konaní za dodržanie podmienok ochrany informácií, ktoré podliehajú zvýšenej ochrane a ktoré im boli zverené výlučne pre účely trestného konania, musí byť zaistená aj ich ochrana z hľadiska práva na súkromie. Znamená to, že orgány činné v trestnom konaní tieto informácie môžu poskytnúť výlučne na **základe zákonného zmocnenia**, t. j. ak je to zákonom výlučne dovolené. **Nie preto, že to nie je zákonom výslovne zakázané.**

Hoci vo vzťahu k fyzickým osobám platí pravidlo, že každý môže konať to, čo nie je zákonom zakázané, vo vzťahu k štátnym orgánom, kde nepochybne možno zaradiť aj nadriadeného v konaní o prepustení policajta z služobného pomeru, sa uplatňuje v zmysle čl. 2 ods. 2 Ústavy pravidlo, že môžu „**konať iba na základe ústavy, v jej medziach a v rozsahu a spôsobom, ktorý ustanoví zákon**“ resp. inými slovami iba to, čo im dovoľuje resp. prikazuje zákon.

²⁹ IVOR, J., POLÁK, P., ZÁHORA, J. *Trestné právo procesné I*. Wolters Kluwer, Bratislava 2017, s. 288 a nasl.

V zmysle § 115 ods. 6 Trestného poriadku ak sa majú záznamy použiť v trestnom konaní ako dôkaz, musí sa ukončiť odpočúvanie a príslušný útvar po požiadaní o odtajenie a tzv. sprocesenie záznamu vyhotoví doslovný prepis záznamu. Podľa súčasne platného právneho stavu až takýto záznam má povahu trestno-procesného dôkazu. Teda, ak by orgán prípravného konania poskytol neodtajnený záznam príslušnému nadriadenému s disciplinárnou a personálnou právomocou, tento by bol absolútne nepoužiteľný tak v disciplinárnom ako aj v trestnom konaní.³⁰

Citovaní autori pokračujú, že ak by orgán prípravného konania umožnil čo i len nahliadnuť do neodtajneného a nesprocesneného záznamu neoprávnenému subjektu, ktorým nadriadený s disciplinárnou a personálnou právomocou nepochybne je, nielenže by konal v rozpore s procesnými predpismi, ale za istých okolností by mohol naplniť pojmové znaky skutkovej podstaty zneužívania právomoci verejného činiteľa, prípadne iného trestného činu uvedeného v osobitnej časti Trestného zákona. Obdobne by to platilo aj v prípade, že by záznamy boli odtajnené a sprocesené, pretože nadriadený s disciplinárnou právomocou nie je oprávneným subjektom na oboznámenie sa s dôkazmi získanými použitím informačno-technických prostriedkov. Na dôvazok, nie je oprávneným subjektom ani na nazeranie do súvisiaceho vyšetrovacieho spisu a oboznamovanie sa s jeho obsahom, na vyhotovenie fotokópií spisov alebo jeho častí.

Záver

Záverom možno skonštatovať, že Trestný poriadok upravuje podmienky získavania a použitia obrazovo-zvukových záznamov zhotovených informačno-technickými prostriedkami iba v rámci trestného konania a pre účely trestného konania. Získavanie a použitie obrazovo-zvukových záznamov zhotovených informačno-technickými prostriedkami v iných konaniach, resp. pre účely iných konaní upravuje zákon o ochrane pred odpočúvaním.³¹ Zákon o ochrane pred odpočúvaním v § 3 ods. 1 umožňuje použiť informačno-technický prostriedok iba vtedy, „ak je to v demokratickej spoločnosti nevyhnutné na zabezpečenie bezpečnosti štátu, obranu štátu, **predchádzanie a objasňovanie trestnej činnosti** ...“. Predchádzanie trestnej činnosti colníkov pri výkone ich služby a v mieste výkonu služby je relevantným dôvodom pre použitie informačno-technického prostriedku. Najvyšší súd vychádza zo skutočnosti, že nevyhnutnosť ich použitia vyplýva i z okolností tohto prípadu, na vonkajšej hranici colného územia EU s Ukrajinou.³²

Ako možné riešenie prichádza do úvahy novelizácia príslušných zákonov upravujúcich služobný pomer priznať služobnému úradu pri rozhodovaní o prepustení policajta resp. colníka oprávnenie aké má Protimonopolný úrad „Pri plnení povinností podľa tohto zákona alebo osobitného predpisu je úrad oprávnený vyžiadať si od orgánov policajného zboru alebo od orgánov činných v trestnom konaní informácie získané podľa osobitných predpisov, predovšetkým je oprávnený nazeráť do spisov vedených v trestnom konaní, robiť si zo spisov výpisy a poznámky a zaobstaráť si na vlastné trovy kópie spisov a ich častí, a tie použiť na účely podľa tohto zákona.“³³

³⁰ Porovnaj PERHÁCS, Z., ZAJONC, A. *Poznámky k sledovaniu, priestorovému a telefonickému odposluchu*. In: Justičná revue. č. 8–9/2011, s. 1140.

³¹ Nález Ústavného súdu Slovenskej republiky z 15. decembra 2011, sp. zn. II. ÚS 5/2011.

³² Uznesenie Najvyššieho súdu Slovenskej republiky sp. zn. 3 Sžo/10/2012 z 5. júna 2012.

³³ § 22 ods. 3 zákona č. 136/2001 Z. z. o ochrane hospodárskej súťaže a o zmene a doplnení zákona Slovenskej národnej rady č. 347/1990 Zb. o organizácii ministerstiev a ostatných ústredných orgánov štátnej správy Slovenskej republiky v znení neskorších predpisov.

Literatúra

- ALÁČ, M. *Získavanie informácií na spravodajské účely a na účely trestného konania*. Bratislava: C. H. Beck 2015.
- ČENTĚŠ J. *Odpočúvanie – procesnoprávne a hmotnoprávne aspekty*. C. H. Beck: Bratislava, 2013.
- ČIČ, M. a kol. *Komentár k Ústave Slovenskej republiky*. Žilina: Eurokódex 2012.
- HARFIELD, C., HARFIELD, K. *Covert Investigation (Blackstone's Practical Policing)*. Oxford., Oxford University Press, 2016.
- IVOR, J. *Využitie záznamu z odpočúvania ako dôkaz v trestnom konaní*. In: *Dokazovanie v civilnom a trestnom konaní*. Pezinok: Justičná akadémia Slovenskej republiky, 2012. s. 204–214.
- IVOR, J., POLÁK, P., ZÁHORA, J. *Trestné právo procesné I*. Wolters Kluwer, Bratislava 2017.
- MATHERN, V. *Dokazovanie v československom trestnom procese*. Bratislava, Obzor, 1984.
- PERHÁCS, Z., ZAJONC, A. *Poznámky k sledovaniu, priestorovému a telefonickému odposluchu*. In: *Justičná revue*. č. 8–9/2011, s. 1138–1144.
- PŮRY, F. *Některé limity dokazování v trestním řízení České republiky*. In: *Dokazovanie v civilnom a trestnom konaní*. Pezinok: Justičná akadémia Slovenskej republiky, 2012. s. 195–203.
- SVÁK, J. *Ochrana ľudských práv v troch zväzkoch*. Žilina: Eurokódex, 2011.
- ŠÁMAL, P., NOVOTNÝ, F., RŮŽIČKA, M., VONDRUŠKA, F., NOVOTNÁ, J. *Přípravné řízení trestní*. Praha: C. H. Beck, 2003.
- ŠÁMAL, P. a kol. *Trestní řád*. Komentář. 7. vydání. Praha: C. H. Beck, 2013.
- ZÁHORA, J. *Dokazovanie v trestnom konaní*. Praha: Leges, 2013.
- ZÁHORA, J. *Použitie záznamu získaného odpočúvaním ako dôkazu v inej trestnej veci*. In: *JELÍNEK, J. a kol. Trestní právo procesní – minulost a budoucnost*. Praha: Leges, 2016, s. 162–174.

Nakladatelství Leges, s. r. o.
Lublaňská 61, Praha 2
www.knihyleges.cz

