Jozef Záhora (ed.)

Informačno-technické prostriedky v trestnom konaní – možnosti a perspektívy

Zborník príspevkov z vedeckej konferencie konanej dňa 4. apríla 2019

Leges

teoretik

INFORMAČNO-TECHNICKÉ PROSTRIEDKY V TRESTNOM KONANÍ – MOŽNOSTI A PERSPEKTÍVY

Jozef Záhora (ed.)

INFORMAČNO-TECHNICKÉ PROSTRIEDKY V TRESTNOM KONANÍ – MOŽNOSTI A PERSPEKTÍVY

Zborník príspevkov z vedeckej konferencie konanej dňa 4. apríla 2019

Leges

Vzor citácie:
Záhora, J. (ed.): Informačno-technické prostriedky v trestnom konaní – možnosti a perspektívy. Praha: Leges, 2019, 267 s.

Zostavil:
prof. JUDr. Jozef Záhora, PhD.

Recenzenti:
doc. JUDr. Sergej Romža, PhD.
doc. JUDr. Marek Fryšták, Ph.D.

Programový výbor:
prof. JUDr. Jozef Záhora, PhD.
Dr. h. c. prof. JUDr. Jaroslav Ivor, DrSc.
prof. JUDr. Jiří Jelínek, CSc.
prof. JUDr. Peter Polák, PhD.

KATALOGIZACE V KNIZE – NÁRODNÍ KNIHOVNA ČR

Informačno-technické prostriedky v trestnom konaní – možnosti a perspektívy (konference) (2019 : Bratislava, Slovensko)
Informačno-technické prostriedky v trestnom konaní – možnosti a perspektívy : zborník príspevkov z vedeckej konferencie konanej dňa 4. apríla 2019 / Jozef Záhora (ed.). – Vydání první. – Praha : Leges, 2019. – 267 stran
Částečně český text

ISBN 978-80-7502-363-6 (brožováno)

* 343.98.06 * 343.13 * (062.534)
– informačně technické prostředky
– trestní řízení
– 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

Za odbornú a jazykovú stránku príspevkov zodpovedajú autori.
Rukopis neprešiel jazykovou úpravou.
Vydalo Nakladatelství Leges, s. r. o., Lublaňská 4/61, Praha 2, v roce 2019
jako svou 564. publikaci.
Vydání první
Návrh obálky Michaela Vydrová
Sazba Gradis
Tisk PBtisk, a. s., Příbram
www.knihyleges.cz

© 2019, Paneurópska vysoká škola

ISBN 978-80-7502-363-6

Obsah

Obsah 5

Predhovor 9

Program 11

Miroslava Bálintová
Použitie informačno-technických prostriedkov z pohľadu Európskeho súdu pre ľudské práva 15

Jiří Jelínek
Prostorový odposlech a jeho právní (ne)úprava v České republice 28

Ivan Šimovček
Primeranosť využívania informačno-technických prostriedkov v trestnom konaní 36

Peter Polák, Marek Talapka
Limity uplatňovania informačno-technických prostriedkov vyplývajúce zo základných zásad trestného konania a z judikatúry Európskeho súdu pre ľudské práva 43

Marek Kordík
Informačno-technické prostriedky – vybrané aplikačné problémy v praxi 59

Ján Šanta
K praktickým poznatkom vyplývajúcim zo Zákona o ochrane pred odpočúvaním a Trestného poriadku 66

Jozef Čentéš
Posúdenie zásady proporcionality pri zaznamenaní telefonického hovoru 83

Jaroslav Ivor, Eduard Kolla
Záznam z autokamery ako dôkaz v trestnom konaní 92

Miloš Deset
Obrazovo-zvukové záznamy vyhotovované súkromnými osobami a ich prípustnosť v trestnom konaní 109

Peter Šamko
Skutočne možno použiť v trestnom konaní nezákonné dôkazy získané súkromnými osobami? 115

Miroslav Lisoň, Michal Marko
Koncepcie a funkcie používania ITP v procesoch kriminálno-policajného poznania 129

Ladislav Pokorný
K vybraným otázkám důkazního použití odposlechu pořízeného zpravodajskými službami 139

Miroslav Růžička
K některým otázkám týkajícím se odposlechu, zjišťování údajů z telekomunikačního provozu 149

Adrián Vaško
Perspektívy akceptácie informácie zabezpečených mimoprocesným použitím ITP 157

Michal Aláč
Použitie informačno-technických prostriedkov a nezodpovedané otázky 167

Marcela Tittlová
Povoľovací mechanizmus vo vzťahu k ITP 173

Jozef Medelský
Trestnoprávne prostriedky boja proti kybernetickým hrozbám 187

Dominik Vanek
Obrazový, zvukový alebo obrazovo-zvukový záznam ako informačno-technický prostriedok v trestnom konaní 196

Filip Korček
Odpočúvanie a záznam telekomunikačnej prevádzky v trestnom konaní 205

Monika Šebestová-Širilová
Oznámenie o odpočúvaní a zničenie záznamu telekomunikačnej prevádzky 211

Barbora Tallová
Preskúmanie zákonnosti vydaného príkazu na odpočúvanie a záznam telekomunikačnej prevádzky 225

Barbora Dorkinová
Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní 239

Jakub Jagnešák
Operatívno-pátracia činnosť *de lege lata* 248

Jozef Záhora
Vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov – úvahy *de lege ferenda* 259

Contents

Contents 7

Preface 9

Conference Programme 11

Miroslava Bálintová
Using Means of Secret Surveillance from the Perspective of the European Court of Human Rights 15

Jiří Jelínek
Surround Interception and Its Legal (Non)regulation in the Czech Republic 28

Ivan Šimovček
Relevance of the Use of Information Technology in Criminal Proceedings 36

Peter Polák, Marek Talapka
Limits on the Application of Information and Technology Resources Stemming from the Basic Principles of Criminal Proceedings and the Case Law of the European Court of Human Rights 43

Marek Kordík
Information-technical Tools – Selected Application Problems in Practice 59

Ján Šanta
Practical Knowledge Related to the Law about Protection from Interception and Code of Criminal Procedure 66

Jozef Čentéš
Assessment of the Proportionality Principle for Telephone Calling 83

Jaroslav Ivor, Eduard Kolla
Vehicle Camera Record as the Proof in Criminal Proceedings 92

Miloš Deset
Video and Audio Records Made by Private Persons and their Admissibility in the Criminal Proceedings 109

Peter Šamko
Is it Possible to use Unlawful Evidence Obtained by Private Individuals in Criminal Proceedings? 115

Miroslav Lisoň, Michal Marko
Concepts and Functions Use ITP in Criminal-police Knowledge 129

Ladislav Pokorný
Selected Problems of Intelligence Interception as an Evidence in Criminal Proceeding 139

Miroslav Růžička
Selected Questions Concerning Interception of Telecommunication, Ascertainment Data of Telecommunication 149

Adrián Vaško
Perspectives of Acceptance of Information Provided not Criminal Proceedings Use of Information and Technical Means 157

Michal Aláč
Using of Information Technical-intelligence Measures and Unanswered Questions 167

Marcela Tittlová
Authorization Mechanism in Relation to Information Technology Means 173

Jozef Medelský
Criminal Means against Cyber Threats 187

Dominik Vanek
Video, Audio or Video-sound Recording as Information and Technology in Criminal Proceedings 196

Filip Korček
Listening and Recording of Telecommunications Traffic in Criminal Proceedings 205

Monika Šebestová-Širilová
Notice of Interception and Destruction of Telecommunication Service Records 211

Barbora Tallová
The Reviewing the Legality of the Interception and Recording of the Telecommunications Order 225

Barbora Dorkinová
Theoretical and Practical Problems of Using Information and Technical Resources in Criminal Proceeding 239

Jakub Jagnešák
Operative-search Activity *de lege lata* 248

Jozef Záhora
Production Video, Audio or Video-audio Records – Consideration *de lege ferenda* 259

Predhovor

Preface

V posledných desaťročiach sa v súvislosti s páchaním kriminality začali objavovať úplne nové javy vyplývajúce z charakteru trestnej činnosti. Týmito javmi sú najmä kvalitatívne nové druhy trestnej činnosti, osobitne však organizovaná kriminalita. Organizovaná kriminalita vykazuje mimoriadne vysoký stupeň rezistencie voči policajným a justičným zásahom. Preto aj tradičné dôkazné prostriedky sa javia ako nedostatočne efektívne. V súvislosti s tým, vzniká potreba hľadať nové dôkazné prostriedky, ktoré sú spôsobilé odhaliť a preukázať aj tento druh trestnej činnosti.

Tieto „nové" dôkazné prostriedky predstavujú veľmi špecifické, ofenzívne a spravidla utajeným spôsobom vykonávané dôkazné postupy, pomocou ktorých je možné získavať informácie dôležité pre trestné konanie. Ich význam a nezastupiteľné miesto v trestnom konaní je podporené aj tým, že odhaľovanie a dokazovanie tých najzávažnejších druhov trestnej činnosti prostredníctvom klasických prostriedkov je iba málo efektívne, v niektorých prípadoch dokonca nemožné. Efektívne a účinné odhaľovanie a dokazovanie tých najzávažnejších druhov kriminality si tak vyžaduje využitie špecifických a zároveň silne ofenzívnych prostriedkov, ktoré umožňujú získavanie objektívnych a neskreslených informácií o kriminálnom správaní. Je potrebné uvedomiť si, že na jednej strane ide o efektívne a účinné prostriedky smerujúce k odhaľovaniu závažných druhov trestnej činnosti, no na strane druhej ide o prostriedky ofenzívne, ktoré vážne zasahujú do oblasti základných ľudských práv, predovšetkým do práva na súkromie, na čo poukázal niekoľkokrát vo svojej judikatúre aj Európsky súd pre ľudské práva.

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 páchateľov 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.

Právna úprava ITP, ich použitie v trestnom konaní a spravodajskej oblasti prináša viaceré aplikačné problémy čo predstavuje veľmi aktuálnu otázku. O aktuálnu otázku ide práve s ohľadom na problematickosť 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 dôkazných prostriedkov.

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 nadväzuje na konferenciu

z roku 2017 Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní.

Sme radi, že na konferencii okrem záujemcov z akademického prostredia, predovšetkým z právnických fakúlt z Českej republiky a Slovenskej republiky a z Akadémie Policajného zboru v Bratislave, sa na konferencii zúčastnili aj zástupcovia aplikačnej praxe, predovšetkým zo súdov, Prezídia Policajného zboru, Generálnej prokuratúry, Najvyššieho štátneho zastupiteľstva Českej republiky a spoluzástupkyňa Slovenskej republiky pred Európskym súdom pre ľudské práva.

Jednotlivé vystúpenia a následná diskusia preukázali, že pri využívaní informačno-technických prostriedkov či už v rámci trestného konania alebo výkonu spravodajských činností sa objavuje množstvo teoretických a praktických problémov, ktoré vyžadujú riešenie. Viaceré problémy boli identifikované a navrhnuté riešenia. Preto veríme, že cieľ konferencie, ktorým bolo predloženie čiastkových záverov k riešenej výskumnej úlohe, predstavenie návrhov a vytvorenie platformy na odbornú diskusiu k predloženým záverom sa v plnom rozsahu podarilo naplniť.

Program

Conference Programme

„Informačno-technické prostriedky v trestnom konaní – možnosti a perspektívy“

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.

4. apríla 2019, Paneurópska vysoká škola, Tomášikova 20, 821 02 Bratislava, miestnosť Odeon

08^{30} – 09^{00} h	***prezentácia účastníkov***	
09^{00} – 09^{10} h	***otvorenie konferencie***	
Blok I. 09^{30} – 11^{00} hod.	***JUDr. Miroslava Bálintová*** spoluzástupkyňa SR pred ESĽP, MS SR	**Použitie informačno-technických prostriedkov z pohľadu Európskeho súdu pre ľudské práva**
	prof. JUDr. Jiří Jelínek, CSc. Právnická fakulta UK Praha	**Prostorový odposlech a jeho právní (ne)úprava v České republice**
	prof. JUDr. Ivan Šimovček, CSc. Právnická fakulta Trnavskej univerzity	**Primeranosť využívania informačno-technických prostriedkov v trestnom konaní**
	prof. JUDr. Peter Polák, PhD., JUDr. Marek Talapka Fakulta práva PEVŠ Bratislava	**Limity uplatňovania ITP v základných zásadách trestného konania a v judikatúre ESĽP**
	doc. JUDr. Marek Kordík PhD., LL.M. Prezídium Policajného zboru	**Informačno-technické prostriedky – vybrané aplikačné problémy**
	JUDr. Ján Šanta, PhD., LL.M., MBA Úrad Špeciálne prokuratúry, GP SR	**K praktickým poznatkom vyplývajúcim zo zákona o ochrane pred odpočúvaním a Trestného poriadku**
	Diskusia	
11^{00} – 11^{20} h	***Coffee break***	

Blok II. 11^{20} – 13^{00} hod.	***prof. JUDr. Jozef Čentéš PhD.*** Právnická fakulta UK, Bratislava	**Posúdenie zásady proporcionality pri zaznamenaní telefonického hovoru**
	Dr. h. c. prof. JUDr. Jaroslav Ivor, DrSc. Právnická fakulta UMB, B. Bystrica, **Ing. Eduard Kolla, PhD.** Ústav znaleckého výskumu a vzdelávania, Žilinská univerzita v Žiline	**Záznam z autokamery ako dôkaz v trestnom konaní**
	doc. JUDr. Miloš Deset, PhD. Právnická fakulta, Trnavskej univerzity	**Obrazovo-zvukové záznamy vyhotovené súkromnými osobami a ich prípustnosť v trestnom konaní**
	JUDr. Peter Šamko Krajský súd v Bratislava	**Skutočne možno použiť v trestnom konaní nezákonné dôkazy získané súkromnými osobami?**
	prof. Ing. Miroslav Lisoň, PhD. Akadémia Policajného zboru	**Koncepcie a funkcie používania ITP v procesoch kriminálno-policajného poznania**
	doc. JUDr. Ladislav Pokorný, Ph.D. Právnická fakulta MU v Brne	**K vybraným problémům možného důkazního použití zpravodajských prostředků**
	JUDr. Miroslav Růžička, Ph. D. *Nejvyšší státní zastupitelství ČR*	**K některým otázkám týkajícím se odposlechu, zjišťování údajů z telekomunikačního provozu**
	JUDr. Adrián Vaško, PhD. Akadémia Policajného zboru	**Perspektívy akceptácie informácií zabezpečených mimoprocesným použitím ITP**
	JUDr. Michal Aláč, PhD. *Právnická fakulta, Trnavskej univerzity*	**Použitie informačno-technických prostriedkov a nezodpovedané otázky**
	Diskusia	
13^{10} – 14^{10} h	***Obed***	

Blok III. 14^{20} – 16^{00} hod.	***doc. PhDr. JUDr. Marcela Tittlová, PhD.*** Fakulta práva PEVŠ Bratislava	**Povoľovací mechanizmus vo vzťahu k použitiu ITP**
	doc. PhDr. JUDr. Jozef Medelský, PhD. Akadémia PZ Bratislava	**Trestnoprávne prostriedky boja proti kybernetickým hrozbám**
	JUDr. Dominik Vanek Fakulta práva PEVŠ Bratislava	**Obrazový, zvukový alebo obrazovo--zvukový záznam ako informačno--technický prostriedok v trestnom konaní**
	JUDr. Filip Korček, LL.M. Právnická fakulta Trnavskej univerzity	**Odpočúvanie a záznam telekomunikačnej prevádzky v trestnom konaní**
	Mgr. Monika Širilová Fakulta práva PEVŠ Bratislava	**Oznámenie o odpočúvaní a zničenie záznamu telekomunikačnej prevádzky**
	JUDr. *Barbora Tallová* Fakulta práva PEVŠ Bratislava	**Preskúmanie zákonnosti vydaného príkazu na odpočúvanie a záznam telekomunikačnej prevádzky**
	Mgr. Barbora Dorkinová Fakulta práva PEVŠ Bratislava	**Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní**
	Mgr. et Bc. Jakub Jagnešák Akadémia PZ Bratislava	**Operatívno-pátracia činnosť *de lege lata***
	prof. JUDr. Jozef Záhora, PhD. Fakulta práva PEVŠ Bratislava	**Vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov – *úvahy de lege ferenda***
	Diskusia	
16^{00} h	***Záver konferencie***	

Použitie informačno-technických prostriedkov z pohľadu Európskeho súdu pre ľudské práva

Using Means of Secret Surveillance from the Perspective of the European Court of Human Rights

Miroslava Bálintová[1]

Abstrakt: *Odpočúvanie a ďalšie spôsoby tajného sledovania osôb a ich komunikácie sú bezpochyby užitočným nástrojom pri zisťovaní trestnej činnosti a ochrane národnej bezpečnosti. Na druhej strane, dôsledná ochrana ľudských práv a základných slobôd vyžaduje existenciu primeraných záruk proti zneužitiu opatrení zameraných na sledovanie osôb. Judikatúra Európskeho súdu pre ľudské práva v Štrasburgu môže slúžiť vnútroštátnym orgánom ako návod pri určovaní mantinelov vnútroštátneho právneho rámca pre túto oblasť aj pri jeho aplikácii. Osobitne preto, že práve tento medzinárodný súdny orgán vo svojej judikatúre vytvoril viacero požiadaviek predovšetkým na kvalitu právnej úpravy umožňujúcej používanie takýchto opatrení.*

Abstract: *Telephone interception and other forms of secret surveillance of persons and their communication is undoubtedly a useful tool in crime detection and national security protection. On the other hand, the consistent protection of human rights and fundamental freedoms requires the existence of adequate safeguards against the abuse of measures for secret surveillance of people. The case-law of the European Court of Human Rights in Strasbourg can serve as a guide for national authorities in determining the limits of the national legal framework for this area and its application. This is particularly so because in its case-law that international court has determined a number of requirements concerning in particular the quality of the law allowing the use of such measures.*

Kľúčové slová: *tajné sledovanie; hromadné sledovanie, hromadné zachytávanie komunikácie; odpočúvanie; právo na súkromie; záruky.*

Key words*: secret surveillance; mass surveillance; bulk interception; telephone interception; right to privacy; safeguards.*

Systematický zber a uchovávanie údajov o osobách považujeme za zásah do súkromia týchto osôb. Z tohto všeobecne uznávaného právneho princípu vychádza tak rozhodovacia činnosť Európskeho súdu pre ľudské práva (ďalej len „Súd“), ako aj rozhodovacia činnosť vnútroštátnych súdov najvyšších inštancií. Takýto zásah do práv spadá pod článok 8 Dohovoru na ochranu ľudských práv a základných slobôd (ďalej len „Dohovor“), ktorý zaručuje právo na rešpektovanie súkromného a rodinného života. V zmysle tohto článku,[2] konkrétne jeho druhého odseku, môže štátny orgán zasahovať do výkonu práva na rešpektovanie súkromného a rodinného života, obydlia a korešpondencie iba v prípadoch, ak je to v súlade so zákonom a nevyhnutné v de-

[1] JUDr. Miroslava Bálintová, spoluzástupkyňa Slovenskej republiky pred Európskym súdom pre ľudské práva, Ministerstvo spravodlivosti Slovenskej republiky, Župné námestie 13, 813 11 Bratislava, tel: 02/88891561, 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, 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 nepokojom a zločinnosti, ochrany zdravia alebo morálky alebo ochrany práv a slobôd iných.

mokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom a zločinnosti, ochrany zdravia alebo morálky alebo ochrany práv a slobôd iných. Súd vo svojej rozhodovacej činnosti v zásade nerobí rozdiel medzi jednotlivými spôsobmi tajného sledovania osôb a k získavaniu a uchovávaniu údajov pristupuje vo všeobecnosti rovnakým spôsobom bez ohľadu na to, či ide o odpočúvanie telefonických hovorov, priestorové odposluchy alebo monitorovanie elektronickej komunikácie. Takisto pri posudzovaní sporného zásahu do práv nie je podstatné, či sa sťažuje osoba, voči ktorej bolo použitie sledovacích zariadení nariadené, alebo druhý z účastníkov komunikácie, teda osoba, ktorá so sledovanou osobou telefonovala alebo inak komunikovala.

Pri posudzovaní prípadov týkajúcich sa odpočúvania a použitia iných opatrení na sledovanie osôb kladie Súd osobitný dôraz na dodržanie zásady legality, teda na to, aby bolo použitie sledovacích opatrení v súlade so zákonom. V zmysle ustálenej judikatúry Súdu táto podmienka implicitne obsahuje požiadavku, aby príslušný vnútroštátny právny predpis, 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, čo kladie dôraz na jeho kvalitu. Požiadavka právnej predvídateľnosti osobitne v súvislosti s tajnými opatreniami na sledovanie znamená, že vnútroštátne právo 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. Zároveň musí vnútroštátne právo obsahovať adekvátne a účinné záruky proti zneužitiu sledovacích opatrení. 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]

Rozhodovanie o týchto prípadoch na Súde je z hľadiska miery dokazovania porušenia práv do istej miery špecifické a táto špecifickosť je daná osobitosťou predmetu sporu. Sťažovateľ vzhľadom na povahu veci, teda utajovanie používania operatívnej techniky, nie je vždy schopný preukázať, že bol skutočne objektom uskutočnených sledovacích opatrení. Pokiaľ boli informácie získané prostredníctvom sledovacích opatrení na vnútroštátnej úrovni ďalej využité v nejakom druhu konania proti sťažovateľovi, najčastejšie v trestnom konaní, situácia je pre sťažovateľa jasná. Rovnako tak sťažovateľ môže získať dôkaz o použití sledovacích opatrení vďaka tomu, že ho príslušný orgán o využití takýchto opatrení následne informuje. Mnohokrát však sťažovateľ dôkaz realizácie takýchto opatrení získa len vďaka úniku informácií pochádzajúcich z orgánu vykonávajúceho sledovacie opatrenia. Niekedy takýto dôkaz sťažovateľ ani nezíska, len má určité indície, ktoré naznačujú použitie sledovacích opatrení. Ešte zložitejšia situácia nastáva v prípade tzv. strategického sledovania, ktoré nie je namierené voči konkrétnej osobe, ale sleduje komunikáciu s určitým obsahom. Na druhej strane, neexistuje mechanizmus, ktorým by Súd „prinútil" žalovaný štát predložiť v spore dôkazy o použití sledovacích opatrení, pokiaľ sa ten sám nerozhodne tak urobiť. Tieto osobitnosti spôsobili, že 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. Súdu postačuje, ak je „rozumne pravdepodobné", že sťažovateľ bol predmetom použitia takýchto opatrení.

[3] Pozri napr. Huvig v. Francúzsko, rozsudok z 24. apríla 1990, ods. 32; Kruslin v. Francúzsko, rozsudok z 24. apríla 1990, ods. 33; alebo Bykov v. Rusko, rozsudok veľkej komory z 10. marca 2009, ods. 76 – 78.

Prípadov týkajúcich sa problematiky odpočúvania a použitia iných sledovacích opatrení je v rozhodovacej činnosti Súdu relatívne mnoho.[4] Najväčšiu skupinu prípadov predstavujú prípady odpočúvania telefonických hovorov. Menej početnú skupinu spomedzi nich tvoria prípady týkajúce sa sledovania na základe GPS údajov. V tejto súvislosti je potrebné spomenúť v prvom rade precedentný prípad *Uzun v. Nemecko* (rozsudok z 2. septembra 2010), v ktorom sa Súd zaoberal otázkou, či sledovanie na základe GPS údajov získaných na základe zariadenia inštalovaného v motorovom vozidle sťažovateľovho spolupáchateľa vôbec možno považovať za zhromažďovanie údajov o sťažovateľovi. Súd považoval za relevantné, že zámerom vyšetrovacích orgánov bolo získať informácie o pohybe sťažovateľa a jeho spolupáchateľa, keďže z predchádzajúcich vyšetrovaní vedeli, že títo podozriví používali motorové vozidlo jedného z nich pred prípravou predchádzajúcich bombových útokov. Keďže informácie o pohybe spolupáchateľovho auta mohli byť spojené so sťažovateľom iba vďaka dodatočnému audiovizuálnemu sledovaniu s cieľom potvrdiť jeho prítomnosť v aute, nebolo pochýb o tom, že sťažovateľ bol objektom sledovania. Získané informácie boli systematicky zbierané, uchovávané a využité v ďalšom vyšetrovaní a na zhromaždenie ďalších dôkazov na miestach, kam sťažovateľ cestoval, pričom tieto dôkazy boli napokon použité v trestnom konaní proti sťažovateľovi. Na základe týchto úvah Súd dospel k záveru, že GPS sledovanie síce je vzhľadom na jeho charakter potrebné odlíšiť od iných metód obrazového alebo zvukového sledovania, ktoré vo väčšej miere zasahujú do práva jednotlivca na rešpektovanie súkromného života, keďže odhaľujú viac informácií o správaní jednotlivca, jeho názoroch a pocitoch, ale s ohľadom na vyššie uvedené aspekty je potrebné aj sledovanie sťažovateľa prostredníctvom GPS za daných okolností považovať za zásah do jeho práva na rešpektovanie súkromného života, chráneného článkom 8 Dohovoru. Súd však ďalej konštatoval, že toto sledovanie bolo uskutočnené s legitímnym cieľom ochrany bezpečnosti štátu, verejnej bezpečnosti a práv obetí, ako aj predchádzania trestnej činnosti. Bolo nariadené až po tom, ako sa menej obťažujúce metódy vyšetrovania ukázali ako nedostatočné, bolo vykonávané po relatívne krátku dobu približne troch mesiacov a týkalo sa sťažovateľa iba vtedy, keď cestoval v aute spolupáchateľa. Sťažovateľ teda nebol objektom celkového a komplexného sledovania. Podľa Súdu sledovanie sťažovateľa spĺňalo kritérium primeranosti a vzhľadom na to, že vyšetrovanie sa týkalo veľmi závažných trestných činov, sledovanie bolo nevyhnutné v demokratickej spoločnosti. Súd rozhodol, že nedošlo k porušeniu článku 8 Dohovoru.

Spomenúť možno tiež relatívne nový prípad *Ben Faiza v. Francúzsko* (rozsudok z 8. februára 2018), ktorý sa týkal použitia sledovacích opatrení voči sťažovateľovi v rámci vyšetrovaní jeho účasti na obchodovaní s drogami v rokoch 2009 až 2010. Na základe príslušného ustanovenia francúzskeho trestného poriadku bol na sťažovateľovo motorové vozidlo inštalovaný geolokátor a bol vydaný súdny príkaz mobilnému operátorovi získať záznamy o prichádzajúcich a od-

[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; AÍ-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 Ekimdzhiev 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.

chádzajúcich volaniach a o signáloch z telefónov sťažovateľa, zachytených vysielačmi mobilného signálu, umožňujúcich následné sledovanie jeho pohybov. Súd v tomto prípade posudzoval osobitne obe použité opatrenia. Pokiaľ ide o geolokáciu sťažovateľovho vozidla, vykonávanú v reálnom čase prostredníctvom zariadenia GPS, Súd rozhodol, že došlo k porušeniu článku 8 Dohovoru, zaručujúceho právo na rešpektovanie súkromného života, pretože v oblasti geolokácie vykonávanej v reálnom čase francúzske právne predpisy, ani judikatúra súdov v príslušnom období dostatočne jasne nedefinovali rozsah a spôsob oprávnenia príslušných orgánov použiť svoju diskrečnú právomoc. Sťažovateľ preto nepožíval minimálnu mieru ochrany vyžadovanú z hľadiska princípu právneho štátu. Súd v tomto prípade zároveň spomenul, že Francúzsko neskôr zákonom z roku 2014 prijalo legislatívny mechanizmus, ktorý reguluje používanie geolokácie. Čo sa týka sledovania sťažovateľa na základe súdneho príkazu vydaného mobilnému operátorovi na získanie zoznamu vysielačov mobilného signálu, ktoré zachytili sťažovateľov telefón, pre účely následného sledovania jeho pohybu, Súd rozhodol, že nedošlo k porušeniu článku 8 Dohovoru. Súd konštatoval, že súdny príkaz bol v súlade so zákonom. Ďalej, bol vydaný v súvislosti s trestným konaním týkajúcim sa dovážania drog organizovanou skupinou, zločineckého spolčenia a prania špinavých peňazí, a teda sledoval legitímny cieľ. Súd bol tiež toho názoru, že toto opatrenie bolo nevyhnutné v demokratickej spoločnosti, pretože bolo zamerané na rozloženie rozsiahleho obchodovania s drogami, do ktorého bolo zainteresované množstvo osôb a ktoré bolo vykonávané v spolupráci so zahraničnými sieťami. Napokon, získané informácie boli použité pri vyšetrovaní a v trestnom konaní pred súdom, počas ktorého bola sťažovateľovi zaručená efektívna kontrola predmetného opatrenia v súlade s princípmi právneho štátu.

Je dôležité zdôrazniť, že skupinu prípadov, ktoré Súd v tejto súvislosti prejednával a prejednáva, možno rozdeliť na prípady, v ktorých sťažovateľ je preukázateľne objektom sledovacích opatrení uskutočňovaných najčastejšie v rámci trestných konaní, alebo sú to prípady, v ktorých sťažovateľ tvrdí, že je potenciálnym objektom sledovacích opatrení, ktoré vnútroštátne legislatíva umožňuje realizovať. V tých prvých musí Súd v zmysle svojej judikatúry sústrediť svoju pozornosť nie na právnu úpravu ako takú, ale na spôsob, akým bola aplikovaná na sťažovateľa za osobitných okolností prípadu.[5] V mnohých prípadoch je preto dôvodom na konštatovanie porušenia článku 8 Dohovoru nedodržanie podmienok vnútroštátnej právnej úpravy. Jedným z nich bol napríklad prípad *Heglas v. Česká republika* (rozsudok z 1. marca 2007), ktorý sa týkal záznamu o uskutočnenej telekomunikačnej prevádzke, zabezpečeného v rámci trestného konania, ktorý však nebol v súlade s príkazom sudcu, a teda s vnútroštátnou právnou úpravou. Spomedzi novších prípadov možno spomenúť prípady *Meimanis v. Lotyšsko* (rozsudok z 21. júla 2015) alebo skupinu chorvátskych prípadov *Dragojević v. Chorvátsko* (rozsudok z 15. januára 2015), *Bašić v. Chorvátsko* (rozsudok z 25. októbra 2016 a *Matanović v. Chorvátsko* (rozsudok zo 4. apríla 2017). V uvádzaných chorvátskych prípadoch Súd vnútroštátnym súdom vytkol nedostatočné odôvodnenie príkazov na odpočúvanie. Odôvodnenie príkazov sa obmedzovalo len na konštatovanie kopírujúce znenie zákonnej podmienky, že vyšetrovanie nemožno viesť inými prostriedkami, alebo by jeho vedenie inými prostriedkami bolo osobitne zložité, neobsahovalo však žiadne odôvodnenie týkajúce sa konkrétnych okolností prípadu a žiadne osobitné dôvody, prečo vyšetrovanie nie je možné viesť iným, do práv menej zasahujúcim spôsobom. Takýto postup nebol v súlade s chorvátskym trestným poriadkom, ktorý stanovoval, že príkaz na odpočúvanie musí obsahovať aj popis konkrétnych skutočností, ktoré odôvodňujú použitie odpočúvania. Chorvátsky najvyšší súd aj ústavný súd odobrili postup nižších súdov, ktoré použili informácie získané odpočúvaním v trestnom konaní, s tým, že nedostatok odôvodnenia príkazu na odpo-

[5] Pozri Goranova-Karaeneva v. Bulharsko, rozsudok z 8. marca 2011, ods. 48.

čúvanie je možné zhojiť neskorším odôvodnením jeho použitia. Takýto postup, teda možnosť spätného odôvodnenia, ktoré vnútroštátne súdy napriek zneniu trestného poriadku umožnili, však podľa Súdu neposkytuje primerané a dostatočné záruky proti zneužitiu a naopak, otvára dvere svojvôli. Súd pripomenul, že v trestnom konaní súdy posudzujú len otázku, či je možné záznamy z odpočúvania pripustiť ako dôkaz, a teda nerozhodujú o tom, či nimi nedošlo k porušeniu práva na rešpektovanie súkromného života. Podľa neho, vnútroštátne právo, tak ako ho vykladali a aplikovali chorvátske súdy, nebolo dostatočne jasné, pokiaľ ide o rozsah a výkon diskrečnej právomoci súdov rozhodujúcich o odpočúvaní a neposkytovalo v praxi dostatočné záruky proti možnému zneužitiu. Zásahy do práv sťažovateľov preto neboli ani zákonné, ani nevyhnutné v demokratickej spoločnosti a došlo k porušeniu článku 8 Dohovoru.[6]

Podobne možno spomenúť prípad *Drakšas v. Lotyšsko* (rozsudok z 31. júla 2012), v ktorom Súd konštatoval porušenie článku 8 z dôvodu, že záznam telefonickej komunikácie medzi sťažovateľom, v danom čase zakladajúcim členom Liberálnej demokratickej strany a tiež členom mestského zastupiteľstva vo Viľňuse, a Jurijom Borisovom, hlavným sponzorom volebnej kampane prezidenta Rolandasa Paksasa, ktorý bol získaný odpočúvaním realizovaným na základe súdneho príkazu štátnou bezpečnostnou službou, unikol do médií. Záznam bol v tom čase preskúmavaný generálnou prokuratúrou v rámci trestného konania a v zmysle príslušných ustanovení lotyšského trestného poriadku boli informácie o vyšetrovaní dôverné. Súd konštatoval, že napriek tomu, že právna úprava zaručovala dôvernosť týchto informácií, informácie z dispozície štátnych orgánov unikli na verejnosť. V tomto prípade nedostatok ochrany vo vzťahu k telefonickej komunikácii sťažovateľa nebol v súlade so zákonom a znamenal tiež porušenie jeho práva na rešpektovanie súkromného života. Na druhej strane, zverejnenie záznamu telefonických hovorov medzi sťažovateľom a jeho obchodnými partnermi a prezidentom Súd nepovažoval za porušenie článku 8 Dohovoru. Súd zdôraznil, že záznam rozhovoru, na základe ktorého bol proti prezidentovi vedený *impeachment*, bol prehratý na pojednávaní pred ústavným súdom, na ktoré majú prístup médiá v súlade so zásadou verejnosti súdnych pojednávaní. Ďalej Súd zdôraznil existenciu verejného záujmu na získaní týchto informácií v prípade, v ktorom vystupovali verejní činitelia. Zverejnený záznam pritom neobsahoval žiadne informácie o sťažovateľovom súkromnom živote. Súd preto zverejnenie záznamov získaných odpočúvaním v rámci konania na ústavnom súde považoval za zákonné a nevyhnutné v demokratickej spoločnosti na ochranu práv a slobôd iných a rozhodol, že právo na rešpektovanie súkromného života sťažovateľa tým porušené nebolo.

Zaujímavým v tejto súvislosti je prípad *Benedik v. Slovinsko* (rozsudok z 24. apríla 2018), v ktorom sťažovateľ namietal proti tomu, že slovinská polícia získala bez súdneho príkazu informácie o dynamickej IP adrese účastníka. V tomto prípade švajčiarska polícia v roku 2006 sledovala skupinu podozrivých, ktorí prostredníctvom *peer-to-peer* siete zdieľali súbory obsahujúce detskú pornografiu. Slovinská polícia požiadala slovinského poskytovateľa internetového pripojenia o informáciu o účastníkovi, ktorému bola v konkrétnom čase pridelená určitá dynamická IP adresa, pričom svoju žiadosť oprela o ustanovenia slovinského trestného poriadku, ktorý ukladal prevádzkovateľom elektronických komunikačných sietí povinnosť poskytnúť polícii informácie o vlastníkoch alebo užívateľoch konkrétneho komunikačného prostriedku, ak neboli známe z verejných zdrojov. Poskytovateľ pripojenia uviedol ako užívateľa adresy sťažovateľovho otca. Na základe týchto informácií polícia v dome sťažovateľovho otca, v ktorom býval aj sťažovateľ, vykonala domovú prehliadku, pri ktorej našla v počítačoch veľké množstvo

[6] Pozri Dragojević v. Chorvátsko, rozsudok z 15. januára 2015, ods. 89 – 102; Bašić v. Chorvátsko, rozsudok z 25. októbra 2016, ods. 33 – 36; Matanović v. Chorvátsko, rozsudok zo 4. apríla 2017, ods. 113 – 116.

fotografií a videí s detskou pornografiou. Užívateľom počítačov bol sťažovateľ, ktorý bol následne v trestnom konaní odsúdený. Súd konštatoval, že zákonné ustanovenie, na základe ktorého slovinská polícia získala informácie spojené s dynamickou IP adresou účastníka, nespĺňalo požiadavku zákonnosti v zmysle jeho judikatúry. Ustanovenie nebolo jasné, pretože neobsahovalo žiadne špecifické pravidlá o zistení identity užívateľa určitej dynamickej IP adresy, neposkytovalo prakticky žiadnu ochranu pred svojvoľným zásahom, neobsahovalo žiadne záruky proti zneužitiu a nestanovovalo žiadny nezávislý dohľad nad predmetnými právomocami polície. Na druhej strane, slovinský zákon o elektronickej komunikácii v relevantnom čase neumožňoval poskytnutie dát o prevádzke užívateľov internetu pre účely trestného konania, naopak, stanovoval povinnosť poskytovateľom internetového pripojenia chrániť dôvernosť týchto informácií a oprávňoval ich poskytnúť tieto údaje, iba ak zachytávanie údajov bolo nariadené príslušným orgánom. Podľa názoru Súdu bol tento stav vnútroštátneho práva nekonzistentný. Na základe toho Súd rozhodol, že došlo k porušeniu článku 8 Dohovoru.

Spomenúť možno aj prípad *Akhlyustin v. Rusko* (rozsudok zo 7. novembra 2017). Kancelária sťažovateľa, ktorý bol v tom čase členom regionálnej volebnej komisie, bola približne týždeň sledovaná skrytou kamerou. Následne bol sťažovateľ obvinený a aj odsúdený za trestný čin zneužitia právomoci. Pri nahliadnutí do spisu trestného konania zistil, že sa tam nachádzajú videozáznamy, na ktorých telefonuje vo svojej kancelárii. Súd v tomto prípade podotkol, že použité sledovacie opatrenia ruská vnútroštátna právna úprava nepovažuje za také, ktoré zasahujú do súkromného charakteru komunikácie, a preto v zmysle nej nevyžadujú predchádzajúce povolenie súdu, ani mnohé ďalšie nevyhnutné záruky. Právna úprava neobsahuje ani žiadne podmienky, za ktorých sú orgány oprávnené uchýliť sa k takýmto opatreniam. Súd preto rozhodol o porušení článku 8 Dohovoru.

Pokiaľ ide o Slovenskú republiku, za zmienku stojí prípad *Kvasnica v. Slovenská republika* (rozsudok z 9. júna 2009). Týkal sa odpočúvania 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. Po tom, ako prepisy sťažovateľových telefonických hovorov unikli a objavili sa v médiách a u tretích osôb, sťažovateľ podal viacero 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 Krajského súdu v Bratislave, 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 neoveriteľných 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 obydlia, 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.

Za zmienku stojí aj prípad *Pastyřík v. Česká republika* (rozhodnutie z 31. mája 2011), ktorý sa týkal úplatkárskej aféry v českom futbale, známej ako „Ivánku, kamaráde", do ktorej boli zapletení okrem iných aj športový riaditeľ futbalového klubu Viktoria Žižkov, ktorého telefón bol odpočúvaný, a sťažovateľ, policajt, ktorý bol futbalovým rozhodcom. Odpočúvaním telefonického rozhovoru medzi nimi dospeli vyšetrovacie orgány k presvedčeniu, že sťažovateľ za úplatok prisľúbil ovplyvniť výsledok futbalového zápasu v prospech uvedeného klubu. Sťažovateľ bol v trestnom konaní odsúdený za trestný čin prijímania úplatku. Súd konštatoval, že odpočúvanie bolo v tomto prípade nariadené sudcom na základe príslušného ustanovenia českého trestného poriadku, malo jednoznačný cieľ a bolo časovo obmedzené. Z hľadiska toho, že išlo o závažnú trestnú činnosť ohrozujúcu verejný záujem, tento zásah do súkromia podľa Súdu spĺňal podmienky zákonnosti, legality aj primeranosti. Súd v tomto prípade zamietol sťažnosť ako zjavne nepodloženú.

V prípadoch založených na všeobecných sťažnostiach, v ktorých sťažovatelia, ktorí môžu byť potenciálne objektom sledovacích opatrení, namietajú proti vnútroštátnej legislatíve, Súd tro-

chu netradične v podstate pripustil inak neprípustnú[7] *actio popularis* a uplatňuje princíp, podľa ktorého 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.[8] V takýchto prípadoch musí Súd uskutočniť úplne abstraktné posúdenie napadnutej právnej úpravy, ktorá použitie sledovacích opatrení pripúšťa.[9]

Týchto prípadov výrazne pribúda najmä v posledných rokoch a týkajú sa najmä tzv. strategického monitorovania, zameraného na určitý obsah komunikácie, nie na konkrétnu osobu. Súd v množstve prípadov podrobil kritike právne úpravy jednotlivých štátov.[10] Osobitne často býva v sťažnostiach podaných Súdu napádaná britská právna úprava. V prípade *Liberty a ďalší v. Spojené kráľovstvo* (rozsudok z 1. júla 2008) vzniesli sťažnosť pred Súdom jedna britská a dve írske 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, pravdepodobne monitorovaná prostredníctvom zariadenia prevádzkovaného britským ministerstvom obrany a určeného na hromadné sledovanie komunikácie prechádzajúcej cez telekomunikačnú sieť. 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. Na tomto mieste je potrebné spomenúť, že neskôr britská právna úprava testom splnenia kritérií vyplývajúcich z judikatúry Súdu prešla. V prípade *Kennedy v. Spojené kráľovstvo* (rozsudok z 18. mája 2010) 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.

Len nedávno Súd rozhodol v prípade *Big Brother Watch a ďalší v. Spojené kráľovstvo* (rozsudok z 13. septembra 2018), v ktorom mimovládne organizácie a novinárske združenia namietali 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. Odvolávali sa pritom na odhalenia Edwarda Snowdena, bývalého správcu systémov v Národnej bezpečnostnej agentúre Spojených štátov (NSA), o programoch na sledovanie a zdieľanie tajných informácií medzi USA a Spojeným kráľovstvom. Sťažujúce sa organizácie namietali proti hromadnému zachytávaniu komuniká-

[7] K tomu pozri napr. N. C. v. Taliansko, rozsudok z 18. decembra 2002, ods. 56.

[8] Súd vo svojej rozhodovacej činnosti uznal, že za určitých okolností si sťažovateľ môže nárokovať postavenie obete porušenia práv aj z dôvodu samotnej existencie tajných opatrení alebo zákonnej úpravy, ktorá umožňuje ich uskutočnenie, bez toho, aby zároveň tvrdil, že voči nemu boli uplatnené. Odchýlka od všeobecného pravidla, pripúšťajúca možnosť domáhať sa abstraktného prieskumu právnej úpravy je osobitne ospravedlniteľná práve v oblasti tajného sledovania osôb, pretože v opačnom prípade by tieto opatrenia v podstate nebolo možné účinne napadnúť. Tým by však boli dotknuté osoby de facto zbavené ochrany práv podľa článku 8 Dohovoru iba preto, že sú porušované prostredníctvom utajovaných metód práce, o ktorých existencii sa tieto osoby nemajú ako dozvedieť. K tomu bližšie pozri napr. Klass a ďalší v. Nemecko, rozsudok zo 6. septembra 1978, ods. 34, 37 – 38; Kennedy v. Spojené kráľovstvo, rozsudok z 18. mája 2010, ods. 124; alebo Liberty a ďalší v. Spojené kráľovstvo, rozsudok z 1. júla 2008, ods. 56.

[9] Pozri Goranova-Karaeneva v. Bulharsko, rozsudok z 8. marca 2011, ods. 48.

[10] 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 atď.

cie, zdieľaniu tajných informácií so zahraničnými vládami a získavaniu údajov o komunikácii od poskytovateľov služieb. Súd rozhodol, že režim hromadného sledovania, umožnený britskou právnou úpravou, je porušením článku 8 Dohovoru, pretože dohľad nad celkovým procesom výberu, ako aj nad filtrovaním, vyhľadávaním a selekciou zachytenej komunikácie nebol dostatočný a neexistovali prakticky žiadne záruky vzťahujúce sa na preskúmanie selekcie tzv. súvisiacich údajov o komunikácii. Súd v tejto súvislosti konštatoval, že fungovanie režimu hromadného sledovania samo o sebe neporušuje Dohovor, ale poznamenal, že takýto režim musí rešpektovať kritériá stanovené v jeho judikatúre. Súd ďalej rozhodol, že režim na získavanie údajov o komunikácii od poskytovateľov komunikačných služieb porušil článok 8 Dohovoru, keďže nespĺňal požiadavku zákonnosti v zmysle judikatúry podľa Dohovoru. Ďalej Súd konštatoval, že režim na zdieľanie tajných informácií so zahraničnými vládami neporušil článok 8 Dohovoru. Súd v tomto prípade rozhodoval aj o námietkach vznesených na poli článku 10 Dohovoru, zaručujúceho slobodu prejavu, v súvislosti so spomínanými sledovacími opatreniami. Tento rozsudok zatiaľ nie je právoplatný, pretože 4. februára 2019 bola akceptovaná žiadosť o opätovné prejednanie veci veľkou komorou Súdu.

V prípade *Centrum För Rättvisa v. Švédsko* (rozsudok z 19. júna 2018) sa právnická firma pôsobiaca vo verejnom záujme sťažovala, že legislatíva umožňujúca hromadné zachytávanie elektronických signálov vo Švédsku pre účely zahraničnej tajnej služby porušuje jej právo na rešpektovanie súkromného života. Súd konštatoval, že príslušná právna úprava zakotvuje právny rámec pre systém tajného sledovania, ktorý potenciálne zasahuje všetkých používateľov mobilných telefónov a internetu bez ich upovedomenia. Podotkol, že napriek tomu, že systém má určité rezervy a isté oblasti by bolo vhodné vylepšiť, celkovo tento systém hromadného sledovania poskytuje primerané a dostatočné záruky proti svojvôli a riziku zneužitia. Rozsah spravodajských opatrení a nakladanie so zachytenými údajmi sú v zákone jasne definované, súhlas na sledovanie musí byť daný súdnym príkazom po podrobnom preskúmaní žiadosti, sledovať je možné iba komunikáciu prekračujúcu švédske hranice a nie komunikáciu v samotnom Švédsku, sledovanie môže trvať maximálne šesť mesiacov a každé predĺženie vyžaduje preskúmanie. Navyše, právna úprava zakotvuje dohľad nezávislých orgánov nad týmto sledovaním. Súd bol toho názoru, že nedostatok v podobe chýbajúceho následného upovedomenia o uskutočnených sledovacích opatreniach je kompenzovaný existenciou viacerých mechanizmov na vybavovanie sťažností na toto sledovanie, najmä prostredníctvom inšpektorátu, parlamentného ombudsmana a ministra spravodlivosti. Súd zároveň vzal do úvahy diskrečné právomoci štátu pri ochrane národnej bezpečnosti, predovšetkým vzhľadom na súčasné hrozby globálneho terorizmu a závažnej cezhraničnej kriminality. Súd rozhodol, že v tomto prípade nedošlo k porušeniu článku 8 Dohovoru. Ani tento rozsudok zatiaľ nie je právoplatný, pretože 4. februára 2019 bola akceptovaná žiadosť o opätovné prejednanie veci veľkou komorou Súdu.

Z aktuálnejších prípadov možno spomenúť tiež prípad *Roman Zakharov v. Rusko* (rozsudok zo 4. decembra 2015), o ktorom rozhodovala veľká komora Súdu a dospela k záveru, že ruská vnútroštátna právna úprava, umožňujúca tajné zachytávanie mobilných telefonických komunikácií, neobsahuje adekvátne a účinné záruky proti zneužitiu. Sťažovateľom v tomto prípade bol riaditeľ vydavateľstva, šéfredaktor a zároveň predseda mimovládnej organizácie, ktorý namietal proti tomu, že operátori mobilných sietí v Rusku boli zo zákona povinní inštalovať zariadenie umožňujúce bezpečnostným zložkám vykonávať operatívno-pátracie činnosti. Tvrdil, že to umožňovalo plošné zachytávanie komunikácie bez dostatočných záruk. Súd konštatoval, že ruské právne predpisy upravujúce zachytávanie komunikácie umožnili v podstate plošné odpočúvanie mobilnej komunikácie obyvateľstva, ale neposkytli dostatočné a účinné záruky proti svojvôli a riziku zneužitia, ktoré sú spojené s každým systémom tajného sledovania a ktoré sú

obzvlášť vysoké v systémoch ako je v Rusku, kde má tajná služba a polícia vďaka technickým prostriedkom priamy prístup ku všetkým mobilným telefonickým komunikáciám. Súd zistil nedostatky v právnej úprave, najmä pokiaľ ide o okolnosti, za ktorých sú orgány v Rusku oprávnené použiť tajné sledovacie opatrenia, dobu trvania týchto opatrení a osobitne okolnosti, za ktorých by mali byť zastavené, ďalej postupy pre povoľovanie zachytávania, ako aj pre uchovávanie a likvidáciu zachytených údajov a dohľad nad zachytávaním. Okrem toho, účinnosť prostriedkov nápravy, ktorými bolo možné napadnúť zachytávanie komunikácie, bola oslabená tým, že boli dostupné len osobám, ktoré boli schopné predložiť dôkaz o zachytávaní, a že získanie takéhoto dôkazu nebolo možné za absencie akéhokoľvek systému oznamovania alebo možnosti prístupu k informáciám o zachytávaní. Súd na základe uvedeného rozhodol, že došlo k porušeniu článku 8 Dohovoru.[11]

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, opatrenia 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 svojvoľným zásahom do ich práv.

Osobitným aspektom v tejto súvislosti je požiadavka, aby o použití tajných opatrení na sledovanie osôb bola informovaná, samozrejme až a *posteriori,* sledovaná osoba. V starších rozsudkoch Súd túto požiadavku explicitne nevyslovil a pridržiaval sa názoru, že povaha a logika tajného sledovania vyžaduje, aby sa nielen sledovanie samotné, ale aj jeho následná kontrola

[11] V nasledujúcom období sa Súd zaoberal skupinou prípadov, v ktorých sa sťažovatelia sťažovali na to, že odpočúvanie ich telefonických hovorov, realizované v rámci trestného konania na základe súdnych príkazov a podľa spomínanej právnej úpravy, porušilo ich právo na rešpektovanie súkromného života. Ide o prípady Zubkov a ďalší v. Rusko (rozsudok zo 7. novembra 2017), Moskalev v. Rusko (rozsudok zo 7. novembra 2017), Konstantin Moskalev v. Rusko (rozsudok zo 7. novembra 2017) a Rodionov v. Rusko (rozsudok z 11. decembra 2018). Súd v týchto prípadoch poukázal na nedostatky dotknutej ruskej právnej úpravy a konštatoval, že nebolo preukázané, že vnútroštátne súdy, ktoré nariadili odpočúvanie, overili, či proti sťažovateľom existuje dôvodné podozrenie zo spáchania trestného činu a aplikovali testy proporcionality a nevyhnutnosti v demokratickej spoločnosti. Súd rozhodol, že článok 8 Dohovoru bol v týchto prípadoch porušený.

uskutočňovali bez vedomia kontrolovanej osoby. 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. 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 prípade *Združenie pre európsku integráciu a ľudské práva a Ekimdzhiev v. Bulharsko* (rozsudok z 28. júna 2007) posudzoval existenciu bulharskej vnútroštátnej právnej úpravy umožňujúcej použitie osobitných opatrení na tajné sledovanie za účelom odhaľovania a zabránenia závažným trestným činom alebo ochrany národnej bezpečnosti. Konštatoval, že zatiaľ čo v počiatočnom štádiu sledovania príslušné zákonné ustanovenia poskytujú dostatočné záruky proti svojvoľnému sledovaniu osôb, pretože 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 zákon neupravuje možnosť preskúmania realizácie opatrení zameraných 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. Ďalej mal výhrady voči tomu, že v zákone absentujú pravidlá upravujúce zaznamenávanie spravodajskej činnosti a uchovávanie a zničenie záznamov, celá kontrola systému tajného sledovania je zverená výlučne ministerstvu vnútra, pričom spôsob, akým minister vykonáva túto kontrolu, zákonom stanovený nie je, a osoby, ktoré sú objektom tajného sledovania, nie sú o použití týchto opatrení nikdy, teda 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 porušení 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.[12] V tejto súvislosti je namieste podotknúť, 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. Zároveň zakotvuje možnosť podať návrh na preskúmanie zákonnosti príkazu na odpočúvanie a záznam telekomunikačnej prevádzky Najvyššiemu súdu Slovenskej republiky.[13] 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,[14] hoci predpokladá zodpovednosť štátu podľa zákona č. 514/2003 Z. z. o zodpovednosti za škodu spôsobenú pri výkone verejnej moci a o zmene niektorých zákonov, za použitie informačno-technického prostriedku, vyhotovenie záznamu alebo skopírovanie záznamu, ktoré sa uskutoční v rozpore s týmto zákonom. Uvedený nedostatok nebol napravený ani poslednou novelou tohto právneho predpisu, účinnou od 1. januára 2016, ktorou bola zavedená kontrola zo strany komisie na kontrolu používania informačno-technických prostriedkov, zriaďovanej Národnou radou Slovenskej republiky.

Súd v súčasnosti prejednáva aj prípady proti ďalším štátom, v ktorých sa sťažovatelia sťažujú na nedostatky v právnej úprave týkajúcej sa využívania sledovacích opatrení, ktoré podľa nich predstavujú porušenie článku 8 Dohovoru. Ide napríklad o prípady *Tretter a ďalší v. Rakúsko* alebo *Ringler v. Rakúsko*, ktoré sa týkajú rakúskej právnej úpravy účinnej od januára 2008, prípady *Association confraternelle de la presse judiciaire a 11 ďalších sťažností v. Francúzsko*, *Follorou v. Francúzsko* a *Johannes v. Francúzsko*, ktoré sa týkajú francúzskeho zákona o spravodajskej službe z roku 2015, ako aj ďalšie.

Záverom je namieste pripomenúť, že odpočúvanie a ďalšie spôsoby tajného sledovania osôb a ich komunikácie sú bezpochyby užitočným nástrojom pri zisťovaní trestnej činnosti a ochrane národnej bezpečnosti. Na druhej strane, dôsledná ochrana ľudských práv a základných slobôd,

[12] K tomu pozri tiež Roman Zakharov v. Rusko, rozsudok zo 4. decembra 2015, ods. 287, ako aj Szabó a Vissy v. Maďarsko, rozsudok z 12. januára 2016, ods. 86.

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

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

v tomto prípade práva na súkromie, vyžaduje existenciu primeraných záruk proti zneužitiu sledovacích opatrení. Judikatúra Súdu môže slúžiť vnútroštátnym orgánom ako návod pri určovaní mantinelov vnútroštátneho právneho rámca pre túto oblasť aj pri jeho aplikácii. Osobitne preto, že práve tento medzinárodný súdny orgán vo svojej judikatúre vytvoril viacero požiadaviek predovšetkým na kvalitu právnej úpravy umožňujúcej používanie takýchto opatrení.

Prostorový odposlech a jeho právní (ne)úprava v České republice

Surround Interception and Its Legal (Non)regulation in the Czech Republic

Jiří Jelínek[1]

Abstrakt: *Článek pojednává o chybějící právní úpravě tzv. prostorového odposlechu (v bytě, v restauraci, ve škole, v zaměstnání etc.) v českém trestním řádu. Přitom se tzv. prostorový odposlech v praxi používá a skutečnosti při něm zjištěné slouží jako důkaz v trestním řízení. Autor naléhavě doporučuje výslovnou zákonnou právní úpravu v českém trestním řádu a uvádí požadavky na takovou úpravu. Druhá část článku 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 the missing legal regulation of the so-called surround interception (in the apartment, in the restaurant, in school, in employment etc.) in the Czech Criminal Procedure Code. At the same time, the so-called surround interception is used in practice and the facts identified therein serve as evidence in criminal proceedings. The author urgently recommends an explicit legal regulation in the Czech Criminal Procedure Code and specifies requirements for such regulation. The second 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, prostorový odposlech, přezkoumání zákonnosti nařízeného odposlechu, mimořádné opravné prostředky.*

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

Úvodem

Základním pramenem českého trestního řízení je stále ještě mnohokrát novelizovaný zákon č. 141/1961 Sb., trestní řád. I když legislativní práce na vytvoření nového trestního řádu pokračují tu více tu méně rychlým tempem již několik desetiletí, nového českého trestněprocesního kodexu jsme se zatím nedočkali, ba dokonce žádná z průběžně předkládaných verzí nového trestního řádu nedorazila ani jako legislativní předloha do Parlamentu České republiky. Teprve vytvořením a schválením nového trestního řádu bude dovršena celková reforma trestního soudnictví v České republice po roce 1989.[2]

[1] Prof. JUDr. Jiří Jelínek, CSc., Právnická fakulta Univerzity Karlovy, Praha, e-mail: jelinek@prf.cuni.cz.

[2] Za první krok k celkové reformě systému trestního soudnictví po roce 1989 považuji přijetí nového českého trestního zákoníku, ke kterému došlo v roce 2009 přijetím zákona č. 40/2009 Sb., trestního zákoníku; shodou okolností si připomínáme letos deset let od jeho přijetí. Za druhý krok reformy považuji přijetí zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim. Třetím, závěrečným krokem bude přijetí nového trestního řádu.

V současné době v tak v České republice žijeme v období poloviční rekodifikace trestního práva, protože bylo rekodifikováno pouze trestní právo hmotné, nikoliv trestní právo procesní.[3]

Rekodifikační práce na novém českém trestním řádu po roce 2014 pokročily a zintenzivněly. Současný český ministr spravedlnosti Milan Kněžínek v médiích oznámil, že do konce letošního kalendářního roku hodlá představit paragrafový koncept nového trestního řádu veřejnosti. Koncept nového trestního řádu představený odborné veřejnosti ovšem ještě není nový trestní řád schválený Parlamentem České republiky.

Názory na obsah nového budoucího trestně procesního kodexu se samozřejmě různí. Podle mého názoru by však měl nový trestní řád obsahovat nové, dosud chybějící ustanovení o tzv. prostorovém odposlechu, resp. komplexní úpravu tří forem odposlechu, tj. odposlechu a záznamu telekomunikačního provozu (§ 88 a § 88a tr. řádu) a právě dosud neupraveného prostorového odposlechu.

Prostorovým odposlechem rozumím utajené získávání informací pomocí speciálních, pro tyto účely sestrojených technických prostředků a zařízení zaznamenávajících obraz, zvuk, přesný pohyb i činnost sledovaných osob v reálném čase a prostoru. Zjednodušeně řečeno nejde ani o odposlech telekomunikačního provozu v širokém slova smyslu či získávání údajů o již uskutečněném telekomunikačním provozu, ale o sledování obrazu či zvuku v soukromí, domě či bytě, na ulici, v přírodě, na pracovišti, v dopravním prostředku, v restauraci, prostě kdekoliv je to technicky možné.

Prostorové odposlechy jsou oproti těm telefonním invazivnější. Zasahují do svobod mnohem většího počtu osob než jen telefonujícího. Prostorové odposlechy zaznamenávají všechno a všechny. I tuto okolnost je třeba mít na paměti při úvaze o naléhavé potřebnosti právní úpravy.

Termín „prostorový odposlech" český trestní řád na žádném ze svých míst nedefinuje a ponechává toto vymezení nauce a právní praxi.[4]

V každém případě prostorový odposlech je specifickým důkazním prostředkem, pomocí kterého je možné získávat a zajišťovat věci důležité pro trestní řízení. Odhalování a dokazování těch nejzávažnějších druhů trestné činnosti prostřednictvím klasických prostředků je málo efektivní a v některých případech dokonce nemožné.

Efektivní a účinné odhalování a dokazování těch nejzávažnějších druhů kriminality si vyžaduje použití specifických a zároveň silně ofenzivních prostředků, které umožňují získávání objektivních a nezkreslených informací o kriminálním jednání.

Rozkrývání specifické trestné činnosti (korupce, drogová kriminalita, kuplířství, nedovolený obchod s lidmi, s pornografií, legalizace výnosů z trestné činnosti, terorismus) činí v praxi ne-

[3] Odhlížím od toho, že zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, obsahuje od ustanovení § 29 cit. zák. procesní část – nicméně jde jen o několik procesních ustanovení speciálních pro případy trestního řízení proti právnickým osobám.

[4] Český trestní řád v části první („Společná ustanovení"), hlavě čtvrté („Předběžná opatření a zajištění osob a věcí důležitých pro trestní řízení"), oddílu sedmém („Odposlech a záznam telekomunikačního provozu") obsahuje pod jedním názvem „Odposlech a záznam telekomunikačního provozu" dvě obsahově odlišná ustanovení upravujících podmínky pro nestandardní zjišťování skutečností důležitých pro trestní řízení. Je to jednak ustanovení § 88 tr. řádu upravující odposlech telekomunikačního provozu a jednak ustanovení § 88a tr. řádu upravující záznam telekomunikačního provozu. Na jiném místě – v části druhé („Přípravné řízení"), hlavě deváté („Postup před zahájením trestního stíhání") pod názvem „Sledování osob a věcí" obsahuje trestní řád ustanovení § 159d odst. 2 tr. řádu umožňující sledování, při kterém mají být pořizovány zvukové, obrazové nebo jiné záznamy. Pro úplnost nutno uvést, že v § 159d odst. 3 tr. řádu je upraveno sledování, kterým má být zasahováno do nedotknutelnosti obydlí, do listovního tajemství nebo zjišťován obsah jiných písemností, a dále v ustanovení § 158e odst. 5 nazvaném „Použití agenta" je upraveno sledování osob a věcí v rozsahu uvedeném v § 158d odst. 2 a provedení předstíraného převodu podle § 158c tr. řádu (k oběma činnostem policejní agent nepotřebuje další povolení).

malé potíže, což způsobuje disproporci mezi veřejným zájmem na jejím postihu a dodržováním práva na spravedlivý proces.

Je potřebné si uvědomit, že sice na jedné straně jde o efektivní, ofenzivní a účinný prostředek směřující k odhalování závažných druhů trestné činnosti, ale na druhé straně jde také o prostředek ofenzivní, které silně zasahuje do oblasti základních lidských práv, na což již několikrát ve své judikatuře upozornil i Evropský soud pro lidská práva. Využití odposlechů, tedy nejen tzv. prostorového odposlechu, v trestním řízení je proto potřebné vždy důsledně zvažovat. V každém případě je potřebné dbát na splnění zákonných podmínek, na jejichž naplnění je jejich použití vázané, a na respektování základních zásad trestního řízení. Při splnění zákonných podmínek, na které se použití uvedených prostředků váže, je takto získaným informacím, věcem či listinám v trestním řízení přiznána povaha zákonného důkazu.[5]

Vždy je třeba důkladně a důsledně zvažovat, zda je využití takto ofenzivních prostředků v dané situaci nezbytné, neboť tím nepochybně dochází k zásahům do soukromí osob. Stejně tak musí být splněny zákonné podmínky stanovené trestněprocesními předpisy, a to při současném respektování základních zásad trestního řízení.

Zájem veřejnosti na odhalování a potírání trestných činů tak nelze bez dalšího nadřadit nad zájem na ochraně osob nevinných (byt v postavení osob podezřelých) a nad neméně důležité ústavní principy demokratického právního státu.

Jde o téma aktuální a mimořádně společensky závažné, jako ostatně vždy, když jde v trestním řízení o zásahy do občanských práv a svobod jednotlivce (například práva na ochranu soukromí, práva na ochranu zpráv podávaných telefonem nebo jiným podobným zařízením, práva na ochranu soukromého a rodinného života) zaručených Listinou základních práv a svobod, Ústavou a mezinárodními dokumenty.

Jinak řečeno pro odposlechy obecně platí, co je uvedeno v nejnovější monografii o obrazových a zvukových záznamech v trestním řízení, totiž že:

1. jde o velmi intenzivní zásah do základních práv a svobod, což si vyžaduje velmi precizní a podrobnou zákonnou úpravu,
2. jde o postupy, u kterých efektivnost jejich použití předpokládá utajenou aplikaci, v důsledku čehož jsou některé kontrolní mechanismy značně omezené,
3. pro důkazní využití takových prostředků za současného garantování řádného procesu (čl. 6 Úmluvy)[6] se předpokládá speciální legislativní úprava a její důsledné dodržování v aplikační praxi.

Odposlechy a jejich použití v českém trestním řízení jsou poměrně kontroverzní otázkou, které bylo věnováno několik rozhodnutí Nejvyššího soudu[7] nebo Ústavního soudu,[8] a také odborné články, například na stránkách Bulletinu advokacie.[9] V poslední době se otázkám odpo-

[5] Záhora, J. a kol.: Dokazovanie v trestnom konaní, Praha: Leges, 2013, s. 251.

[6] Úmluva o ochraně lidských práv a základních svobod, ve znění Protokolů č. 3, 5, 7, 8 a 11 (Sdělení č. 209/1992 Sb.).

[7] Např. č. 19/2004 – II., č. 54/2013, č. 13/2014 – I., č. 13/2014 – II. Sb. rozh. tr.

[8] Např. ÚS svazek 46 nález č. 150, svazek 48 nález č. 46, svazek 56 nález č. 15, svazek 58 nález č. 144 a č. 152, svazek 60 nález č. 52, svazek 73 nález č. 76 Sb. n. a u.

[9] Srov. např. Vantuch, P.: Nová úprava odposlechu v trestním řádu od 1. 7. 2008, Bulletin advokacie č. 10/2008; Jelínek, M.: Ústavní meze prostorových odposlechů ke sledování osob a věcí podle § 158d trestního řádu, Bulletin advokacie č. 5/2010; Jelínek, J.: K chybějící právní úpravě tzv. prostorového odposlechu v trestním řádu, Bulletin advokacie č. 7–8/2018; Novotná, J.: Opatření důkazu odposlechem a záznamem telekomunikačního provozu v cizině a jeho použití v České republice, Trestněprávní revue č. 4/2009; Potměšil, J.: Použitelnost zvukových a obrazových záznamů jako důkazů, Správní právo č. 3/2010; Šámal, P.: Odposlech a záznam telekomunikačního provozu ve světle judikatury, Soudní rozhledy č. 3/2000, s. 69. Pokud jde o právní úpravu nám historicky nejbližší,

slechu věnuje literatura v souvislosti se zvýšeným zájmem o doktrínu tzv. plodů z otráveného stromu.[10]

Současný diskurs v České republice je veden například o otázce, zda mohou skutečnosti zjištěné z prostorových odposlechů pořízených v obydlí posloužit za důkaz stejně dobře i proti obžalovaným v jiných trestních případech.[11]

Pozornost vzbudila také v nedávné době hojně medializovaná kauza soudce Vrchního soudu v Praze, který byl obviněn z údajné trestné činnosti, v níž hrály důležitou roli „odposlechy", zejména odposlechy z úřední kanceláře soudce. Zajímavosti na celé kauze pak dodává skutečnost, že odposlechy byly provedeny v budově soudu a úřední místnosti (kanceláři) přidělené tomuto soudci a že nepochybně zachytily i skutečnosti a informace při poradě senátu o rozsudku, které nesmí být podle ustanovení trestního řádu přítomen kromě soudce, přísedících a zapisovatele nikdo jiný a jejíž obsah má zůstat utajen, případně i jednání v tzv. neveřejném zasedání soudu, o kterém platí totéž. Odposlechy zachytily skutečnosti nejen z jednání, které mohlo být předmětem operativního zájmu policie v dané kauze, ale i nezjištěný (a pravděpodobně ani nezjistitelný) počet dalších jednání, které s celou kauzou nemusely mít nic společného a že tak stalo opakovaně a že nikdo neví, jaký je další osud takových záznamů. Okolnost, že tak stalo v budově soudu, do něhož je jinak přístup omezen jen pro určené osoby a budova střežena Justiční stráží a že se tak stalo bez vědomí funkcionářů soudu, dodává celé kauze na mimořádné závažnosti.[12]

Co je nejdůležitější – výslovná právní úprava v českém trestním řádu

Podle mého názoru je třeba podmínky pro provedení a následné použití skutečností zjištěných při prostorovém odposlechu výslovně upravit v trestním řádu. Chystaná rekodifikace českého trestního procesu je k tomu vhodnou příležitostí. Připomínám, co jsem navrhl a doporučil již dříve:[13]

1. Právní úprava tzv. prostorových odposlechů v českém trestním řádu chybí, ačkoliv také prostorový odposlech svým provedením a důsledky představuje vážný zásah do ústavně

tj. právní úpravu slovenskou, můžeme odkázat na monografii Čentéš, J.: Odpočúvanie – procesnoprávne a hmotnoprávne aspekty, Bratislava: C. H. Beck, 2013.

[10] Herczeg, J.: Plody z otráveného stromu a ústavněprávní limity získávání informací v trestním řízení, Trestněprávní revue č. 3/2009; Tlapák Navrátilová, J.: Doktrína plodů z otráveného stromu v kontextu nezákonných odposlechů, in Jelínek, J. a kol.: Dokazování v trestním řízení v kontextu práva na spravedlivý proces. Praha: Leges, 2018, s. 224–232.

[11] Viz https://www.ceska-justice.cz/2019/04/advokat-rampula-statni-zastupce-lata-chtel-chybnou-zmenou-stanoviska-k-pouzitelnosti-odposlechu-pomoci-obzalobe/ [zobrazeno 6. 4. 2019].

[12] Srov. např. https://www.irozhlas.cz/zpravy-domov/ivan-elischer-vrchni-soud-v-praze-zasah-policie-obvineni_1803131331_hm [zobrazeno 22. 3. 2018] nebo http://www.ceska-justice.cz/2018/03/povolil-soud-odposlechy-kancelari-vrchniho-soudu-policie-i-statni-zastupci-mlci/ [zobrazeno 22. 3. 2018]. Z otevřených novinářských zdrojů se dále můžeme dozvědět, že v dané kauze policie při sledování kanceláře soudce manipulovala bez oprávnění s jeho služebním počítačem, odkud získala i několik protokolů o hlasování v trestních věcech, jimž obviněný soudce jako předseda senátu předsedal. Policejní orgán průběh hlasování „vyhodnocoval" a konstatoval průběh hlasování členů senátu, přičemž vyhodnocení je založeno ve spisovém materiálu této trestní kauzy a jeden výtisk vyhodnocení obdržel i státní zástupce Městského státního zastupitelství, který podle zákona má vykonávat dozor nad zákonností v přípravném řízení. V současné době jsou tyto informace, které jinak podle zákona mají zůstat utajené a nepřístupné, obsažené ve spise, a tedy přístupné i dalším osobám, které mají do spisu přístup, viz http://www.ceska-justice.cz/2018/04/policie-si-v-pripadu-soudce-elischera-mela-nezakonne-opatrit-protokoly-o-hlasovani-soudcu/ [zobrazeno 1. 5. 2018]. Tyto skutečnosti naznačují, že celá kauza bude mít mimo prostorového odposlechu ještě další trestněprávní i trestněprocesní souvislosti.

[13] Jelínek, J.: K chybějící právní úpravě tzv. prostorového odposlechu v trestním řádu, Bulletin advokacie č. 7–8/2018, s. 17–18.

chráněných občanských práv a svobod. Tento zásah je nejen srovnatelný s případy odposlechů výslovně v českém trestním řádu upravených (§ 88 a § 88a tr. řádu),[14] ale může být i závažnější, což souvisí s jeho podstatou (je nečekaný, nepředvídaný, nepředvídatelný), a také s tím, že stále dochází ke zlepšování technických prostředků pro prostorový odposlech, takže je i výkonnější a univerzálnější. Zákonná úprava prostorových odposlechů je nutná proto, aby prostorový odposlech nemohl být využíván jako obvyklý (běžný) způsob získávání informací v trestním řízení a aby nedostatek výslovné právní úpravy nesváděl k přesvědčení a praxi, že lze odposlouchávat kohokoliv a kdekoliv. Absenci specifických pravidel pro jeho uskutečňování v českém trestním řádu považuji za podstatný nedostatek současné právní úpravy. Aplikační praxe si při neexistenci výslovné právní úpravy „vypomáhá" aplikací § 159d odst. 3 tr. řádu jako východiskem z nouze, protože analogická aplikace ustanovení § 88 a § 88a tr. řádu (dvou klasických případů odposlechů upravených v trestním řádu) by byla neústavní. Takový postup je nejen problematický z hlediska zákonnosti, ale praktická aplikace ustanovení § 158d odst. 3 tr. řádu navíc přináší dlouhou řadu teoretických a zejména praktických problémů, jak o tom svědčí nejlépe i protikladná judikatura v kauze řadu let stíhaného obviněného Davida Ratha.[15]

2. Dosavadní demonstrativní výčet důkazních prostředků uvedený v ustanovení § 89 odst. 2 českého tr. řádu bude třeba doplnit o nový důkazní prostředek – prostorový odposlech. Do budoucna bude podle mého názoru ovšem žádoucí přistoupit k zavedení taxativního výčtu důkazních prostředků namísto dosavadního demonstrativního výčtu (dnes § 89 odst. 2 tr. řádu). Legislativní praxe se ovšem tomuto taxativnímu výčtu řadu let brání. Navrhovaná právní úprava by byla z hlediska obhajoby, respektive právní jistoty nepochybně vhodnější. Pokud by zákon zakotvil, že důkazy lze čerpat jen z určitých pramenů, které jsou vyjmenovány zákonem taxativně, byl by tím naplněn požadavek zákonnosti, právní jistoty a ochrany práv fyzických i právnických osob. Jako krajně problematický lze hodnotit současný stav, kdy některé důkazní prostředky (například pachové stopy, fyziodetekční vyšetření, analýza DNA, mikrostopy) nejsou trestním právem vůbec upraveny a musí se k jejich použitelnosti v trestním řízení vyjadřovat soudní judikatura.[16]

3. Vlastní úprava prostorového odposlechu by v trestním řádu byla vhodná současně s dvěma klasickými odposlechy (odposlech a záznam telekomunikačního provozu podle

[14] Ponechávám stranou požadavek, aby i právní a terminologická úprava obou „klasických" odposlechů odpovídala vývoji a terminologii v oblasti komunikačních a informačních technologií – považuji jej za oprávněný a samozřejmý. Srov. v této spojitosti informaci o tom, že v roce 2015 Nejvyšší státní zastupitelství vypracovalo legislativní návrh na změnu dotčených institutů, která by zahrnovala i změnu jejich názvu. Tak například „Příkaz k zjištění údajů o telekomunikačním provozu" měl být změněn na „Příkaz k zjištění údajů o elektronických zprávách", viz Růžička, M.: K aplikačním problémům týkajícím se odposlechu, zjišťování údajů z telekomunikačního provozu a sledování osob a věcí v České republice, in Záhora, J. (ed.): Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní, Praha: Leges, 2017, s. 99.

[15] Srov. rozsudek Krajského soudu v Praze sp. zn. 4 T 21/2013, usnesení Vrchního soudu v Praze sp. zn. 6 To 106/2015, rozsudek Nejvyššího soudu sp. zn. 6 TZ 3/2017 a stížnost pro porušení zákona podanou ministrem spravedlnosti v neprospěch obviněného D. Ratha čj. MSP-87/2017-03D- SPZ/1.

[16] Jde o problém letitý, upozorňoval na něj v literatuře již v roce 1982 Repík, který také přiléhavě argumentoval: Důvody jen demonstrativního výčtu důkazních prostředků v trestním řádu, pokud nejde jen o záměnu pojmů důkaz a důkazní prostředek, jak se někdy tvrdí, mohou spočívat jen na obavě, že taxativní výčet důkazních prostředků by mohl být překážkou pružného a potřebám praxe odpovídajícího uplatnění nových vědeckých poznatků při dokazování. Tato obava je však lichá. Dosavadní zkušenosti ukazují, že zákon se mění častěji a rychleji než v praxi již po desetiletí, ne-li staletí používané důkazní prostředky. Kromě toho je výčet pronikání nových vědeckých postupů do procesu dokazování. Důkazem toho je i skutečnost, že v rámci daném trestním řádem se v kriminalistice nerušeně uplatňují stále nové a nové poznatky moderních věd, viz Repík, B.: Procesní důsledky porušení předpisů o dokazování v trestním řízení, Bulletin advokacie, 1982, červenec–srpen, s. 133.

§ 88 a § 88a tr. řádu), a to v hlavě páté trestního řádu upravující dokazování, nikoliv v hlavě čtvrté, která pojednává o zajištění osob, věcí a jiných majetkových hodnot, jako je tomu podle současné právní úpravy. Ostatně i poslední vydání vysokoškolské učebnice trestního práva procesního považuje odposlechy a sledování za výjimku z pravidla, že jednotlivé důkazní prostředky jsou v trestním řádu situovány do páté hlavy nazvané „Dokazování".[17] Za důkazní prostředek se přeci považují i informace získané použitím informačně technických prostředků. Jako žádoucí se jeví právní úprava v samostatném oddílu pojednávajícím o všech třech typech odposlechu.

4. Zákonná úprava prostorového odposlechu by měla být souladná s oběma případy klasického odposlechu (§ 88, § 88a tr. řádu). Zejména by měla být v zákoně vymezena typová závažnost trestných činů, u kterých je možný prostorový odposlech. Dosud taková úprava v ustanovení § 158d tr. řádu není. Doporučoval bych stejnou úpravu jako v ustanovení § 88 tr. řádu, tj. omezit prostorový odposlech na případy úmyslných trestných činů, na které zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně osm let nebo trestný čin, k jehož trestnímu stíhání zavazuje Českou republiku mezinárodní smlouva. Omezení prostorového odposlechu jen na případy závažných trestných činů, resp. trestných činů, k jejichž stíhání nás zavazují mezinárodní právní nástroje, by jako předpoklad provedení zásahu vyjádřilo subsidiaritu použití těchto prostředků a charakter *ultima ratio* mezi prostředky, jež mají státní orgány při plnění svých úkolů k dispozici (srov. čl. 8 odst. 2 Úmluvy). Zákon by měl výslovně pamatovat i na vymezení okruhu osob, které lze odposlouchávat.

5. V souvislosti s kauzou soudce Vrchního soudu Elischera, u kterého byl tzv. prostorový odposlech instalován nejen v jeho služební kanceláři, ale i v poradních místnostech a mohl tak zachytit i údaje, které vůbec s prošetřovanou kauzou nesouvisely, se nabízí otázka, zda by prostorový odposlech neměl být vyloučen v tzv. poradních místnostech soudu, resp. i na jiných místech. Taková úprava by zjevně dala přednost profesionálnímu tajemství před potřebou zjistit okolnosti potřebné pro trestní řízení.

6. Nařídit prostorový odposlech by byl oprávněn jen předseda senátu a v přípravném řízení soudce, což v trestním řádu v § 159d chybí. Se souhlasem odposlouchávané osoby by bylo možné provést odposlech i bez příkazu oprávněných osob.

7. Prostorový odposlech by bylo možné povolit jen na určitou dobu s povinností policejního orgánu průběžně vyhodnocovat důvody, které vedly k vydání prostorového odposlechu. Prodloužení prostorového odposlechu by mělo být možné zase jen na dobu určitou a za zpřísněných podmínek. Průběžné vyhodnocování výsledků a průběhu prostorového odposlechu je nutné proto, že jde o významný průlom do práva na ochranu soukromí. Soud je přitom povinen i z vlastní povinnosti provést takové důkazy, které legitimitu nařízených, resp. povolených odposlechů osvědčují, pokud tak nečiní v rámci svých povinností již orgány veřejné žaloby.[18]

8. Nová právní úprava by měla také jednotně upravit další nakládání se záznamy o odposleších včetně podmínek, za kterých se uskutečněné záznamy zničí.

9. Samostatnou otázkou, také společnou pro všechny případy odposlechů, je pak informační povinnost k odposlouchávané osobě, která by měla být také jednotná pro všechny tři případy odposlechu, ale zejména by měl zákon nově stanovit důsledky nezákonných odpo-

[17] Jelínek, J. a kol.: Trestní právo procesní. 5. aktualizované vydání podle stavu k 1. 3. 2018. Praha: Leges, 2018, s. 397.

[18] Jelínek, M.: Ústavní meze prostorových odposlechů ke sledování osob a věcí podle § 158d trestního řádu, Bulletin advokacie č. 5/2010, s. 32.

slechů. 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. To by mělo nově platit také u případů tzv. prostorového odposlechu.

Na tento požadavek reagují ustanovení § 88 odst. 8 a 9 tr. řádu, podle nichž státní zástupce nebo policejní orgán, jehož rozhodnutím byla věc pravomocně skončena, a v řízení před soudem předseda senátu soudu prvého 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, jíž 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 telekomunikačním 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 skutečnost, na jejichž základě Nejvyšší soud o zákonnosti odposlechu rozhoduje. Aby mohl soud odpovědně posoudit, zda byl v konkrétním případě odposlech

zákonný, musel by mít k dispozici především takové informace, které měl 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 jejímž základě 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 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 zákonnost navazujícího meritorního rozhodnutí.

Závěr

Provádění prostorového odposlechu jako prostředku k získání informací potřebných pro trestní řízení a jako možnosti využít záznam o odposlechu jako důkaz v trestním řízení výslovně v českém trestním řádu upraveno není. Jeví se naléhavě žádoucím tuto situaci změnit a do trestního řádu zakotvit výslovnou právní úpravu. Závažnost této otázky a její aktuálnost si vyžadují, aby zákonodárce se touto otázkou zabýval ještě dříve, než přijme celkovou novou právní úpravu v oblasti trestního práva procesního. Nesouhlasím s tím, aby se tato otázka odkládala až na připravovanou rekodifikaci trestního práva procesního, jak navrhuje, patrně z obavy, že by to mohlo vést k omezení nástrojů k eliminaci trestné činnosti, v odborné literatuře Růžička.[19]

[19] Růžička, M.: Op. cit. s. 117.

Primeranosť využívania informačno-technických prostriedkov v trestnom konaní[1]

Relevance of the Use of Information Technology in Criminal Proceedings

Ivan Šimovček[2]

Abstrakt: *Vo všeobecnosti môžeme primeranosť charakterizovať ako hodiaci sa do nejakých okolností, do istého prostredia. Zásada primeranosti je základnou zásadou trestného konania ako všeobecné interpretačné pravidlo pri obmedzovaní základných práv a slobôd občanov. Niekedy je tiež označovaná ako zásada zdržanlivosti. Orgány činné v trestnom konaní musia v zmysle zásady primeranosti dbať na to, aby čo najmenej zasahovali do základných práv a slobôd občanov. Táto zásada, pokiaľ ide o obvineného, nadväzuje na zásadu riadneho zákonného procesu a prezumpcie neviny.*

Abstract: *In general, adequacy can be characterized as fitting under some circumstances, into a certain environment. The principle of proportionality is a fundamental principle of criminal procedure as a rule of interpretation in limiting the fundamental rights and freedoms of citizens. Sometimes it is also called the principle of restraint. The law enforcement authorities must ensure, in the sense of the principle of proportionality, that they are least likely to interfere with the fundamental rights and freedoms of citizens. This principle, as far as the accused is concerned, follows the principle of proper legal process and the presumption of innocence.*

Kľúčové slová: *Trestné konanie, informačno-technické prostriedky, primeranosť*

Key words: *Criminal proceedings, information and technical means, proportionality.*

Úvod

Medzi základné princípy trestného konania patria tie, ktoré sú založené na ústavných tradíciách.[3] Medzi základné hodnoty môžeme zaradiť demokraciu a právny štát, slobodu, rešpektovanie ľudských práv, ľudskú dôstojnosť a rovnosť. Právo na prerokovanie veci bez zbytočných prieťahov je jednou zo základných záruk spravodlivého trestného konania, ktorý je súčasťou práva na súdnu a inú právnu ochranu. Podstatou práva na primeranosť prerokovania veci je odstránenie stavu právnej neistoty, ktorú spôsobujú prieťahy v trestnom konaní. Stav právnej neistoty je odstránený až právoplatným rozhodnutím vo veci.[4]

Rešpektovanie ľudských práv

Medzi nosné princípy patrí aj rešpektovanie ľudských práv.[5] Účinnosťou Lisabonskej zmluvy sa v zmysle čl. 6 ZEÚ prameňom práva EÚ stala aj Charta základných práv EÚ. Z trestnoprávnych

---

[1] Článok bol napísaný v rámci riešenia vedecko-výskumného projektu VEGA Ministerstva školstva, vedy, výskumu a športu Slovenskej republiky a Slovenskej akadémie vied 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., Trnavská univerzita v Trnave, Právnická fakulta, Hornopotočná 23, 918 43 Trnava, Slovenská republika, e-mail: ivan.simovcek@truni.sk.

[3] CALLIESS, CH.: The Trans-nationalization of Values by European Law, German Law Journal 10/2009 s. 1369.

[4] KLÁTIK, J.: Rýchlosť trestného konania ako základná hodnota práva na zákonný a včasný trestný proces. In: ŠIMOVČEK, I. a kol.: Hodnoty trestného práva v teórii a praxi. Trnava: Typi Universitatis Tyrnaviensis 2012, s. 194.

[5] ZÁHORA, J.: Európske hodnoty trestného práva a ich zobrazenie v slovenskom trestnom práve. In: ŠIMOVČEK, I. a kol.: Hodnoty trestného práva v teórii a praxi. Trnava: Typi Universitatis Tyrnaviensis, 2012, s. 24.

ustanovení Charty týkajúcich sa limitov využívania informačno-technických prostriedkov treba spomenúť právo na rešpektovanie súkromného a rodinného života (čl. 7 Charty), právo na ochranu osobných údajov (čl. 8 Charty), právo na slobodu prejavu a právo na informácie (čl. 11 Charty), právo na účinný prostriedok nápravy a na spravodlivý proces (čl. 47 Charty), zásadu zákonnosti a primeranosti (čl. 49 Charty).[6]

Európska úroveň trestného konania je podmienená dosiahnutou úrovňou všeobecného dodržiavania ľudských práv a základných slobôd. Ľudské práva a základné slobody nie je možné oddeľovať od procesných práv subjektov trestného konania. Obdobný názor zastáva väčšina právnikov, zaoberajúcimi sa touto vysoko aktuálnou problematikou. Dodržiavaniu ľudských a občianskych práv v trestnom konaní sú venované viaceré odborné monografie a články a boli publikované viaceré výstupy zo špeciálne zameraných vedeckých projektov.[7]

Mimoriadny význam pre stanovenie základných hodnôt trestného konania v demokratickej spoločnosti má ústava, pretože reguluje v trestnom konaní nevyhnutné zásahy štátu do základných práv a slobôd občanov. Ústava stanovuje neprekročiteľné mantinely v trestnom konaní pri obmedzovaní základných práv a slobôd.

Primeranosť použitia informačno-technických prostriedkov

V trestnom konaní sa uplatňujú najmä tri základné ústavné princípy v tom zmysle, že každý môže konať, čo nie je zákonom zakázané a nikoho nemožno nútiť, aby konal niečo, čo zákon neukladá (čl. 2 ods. 3 Ústavy SR). Povinnosti možno ukladať zákonom alebo na základe zákona, v jeho medziach a pri zachovaní základných práv a slobôd, medzinárodnou zmluvou, ktorá priamo zakladá práva a povinnosti fyzických osôb alebo právnických osôb, alebo nariadením vlády (čl. 13 ods. 1 Ústavy SR). Pri obmedzovaní základných práv a slobôd sa musí dbať na ich podstatu a zmysel. Takéto obmedzenia sa môžu použiť len na ustanovený cieľ (čl. 13 ods. 4 Ústavy SR).[8]

Vo všeobecnosti môžeme primeranosť charakterizovať ako hodiaci sa do nejakých okolností, do istého prostredia.[9] Zásada primeranosti je základnou zásadou trestného konania a ústavne je zakotvená v čl. 13 ods. 4 Ústavy SR ako všeobecné interpretačné pravidlo pri obmedzovaní základných práv a slobôd. Niekedy je tiež označovaná ako zásada zdržanlivosti.

Orgány činné v trestnom konaní musia v zmysle primeranosti dbať na to, aby čo najmenej zasahovali do základných práv a slobôd občanov. Táto zásada, pokiaľ ide o obvineného, nadväzuje na zásadu riadneho zákonného procesu a prezumpcie neviny, ktorým dáva hlbší význam a zároveň ju možno tiež chápať komplexnejšie, pretože sa vzťahuje nielen na obvineného, ale na

[6] ZÁHORA, J.: Európske hodnoty trestného práva a ich zobrazenie v slovenskom trestnom práve. In: ŠIMOVČEK, I. a kol.: Hodnoty trestného práva v teórii a praxi. Trnava: Typi Universitatis Tyrnaviensis, 2012, s. 24

[7] Pozri napríklad: ESEA, J. K.: Comparison of Procedural Rules in Criminal Proceedings. Congressional Research Service. Washington, D.C 20540-7000. LÖÖF, R.: Proposed Minimum Rights in Criminal Proceedings thought-out the EU. In: European Law Journal, Volume 12, Issue 3, 2006. TRESCHEL, S.: Human Rights in Criminal Proceedings. European University Institute, Academy of European Law, Oxford University 2005. SPRONKEN, T. – ATTINGER, M.: Procedural Rights in Criminal Proceedings: Existing Level of Safeguards in the European Union. University of Maastricht 2005. ŠÁMAL, P.: Základní zásady trestního řízení v demokratickém systému. Praha: Codex Bohemia 1999. REPÍK, B.: Evropská úmluva o lidských právech a trestní právo. Praha: ORAC, 2002. Green Paper on Criminal Proceedings. In: http://europa.eu/scadplus/print version/en/lvb/133214.htm. MAFFEI, S.: The European Right to Confrontation in Criminal Proceedings, Absent, Anonymous and Vulnerable Witnesses. Europa Law Publishing, Groningen 2006.

[8] JALČ, A.: Základné zásady trestného konania. In ŠIMOVČEK, I. a kol.: Trestné právo procesné. Plzeň: Aleš Čeněk, 2011, s. 33.

[9] https://slovnik.azet.sk/pravopis/slovnik-sj/?q=primeranos%C5%A5 (stiahnuté dňa 12. 2. 2019).

všetky osoby, ktorých trestné konanie akýmkoľvek spôsobom postihuje (napr. svedkov, znalcov, poškodených).[10]

V zmysle zásady primeranosti v trestnom konaní (§ 2 ods. 2 TP) možno zasahovať do základných práv a slobôd osôb v prípadoch dovolených zákonom len v miere nevyhnutnej na dosiahnutie účelu trestného konania, pričom treba rešpektovať dôstojnosť osôb a ich súkromie. Primeranosť je obsiahnutá vo viacerých trestnom-procesných inštitútoch, ktoré zasahujú do práv a oprávnených záujmov občanov, vrátane odpočúvania a záznam telekomunikačnej prevádzky a použitia prostriedkov operatívno-pátracej činnosti.[11]

Zásada primeranosti platí pre súdy a orgány činné v trestnom konaní a podmieňuje spôsob vykonávania úkonov trestného konania, t. j. zaobchádzať s osobami zúčastnenými na úkone tak, ako to vyžaduje účel trestného konania a vždy rešpektovať ich dôstojnosť a ústavou zaručené práva a slobody. Súčasne jednotlivé procesné úkony nesmú byť vykonávané v nevhodnom čase, v nevhodných priestoroch a čím by mohlo dôjsť k narušeniu účelu trestného konania a k nerešpektovaniu dôstojnosti a súkromia dotknutých osôb.

Pri posudzovaní primeranosti použitia informačno-technických prostriedkov treba vychádzať z princípu, podľa ktorého každý má právo na to, aby jeho záležitosť bola spravodlivo, verejne a v primeranej lehote prejednaná nezávislým a nestranným súdom, ktorý rozhodne o jeho občianskych právach alebo záväzkoch alebo o oprávnenosti akéhokoľvek trestného obvinenia proti nemu. Základným požiadavkám spravodlivosti a rýchlosti musí zodpovedať celé trestné konanie.

Primeranosť použitia informačno-technických prostriedkov sa musí vždy posudzovať podľa konkrétnych okolností trestnej veci. Primeranosť možno chápať v niektorých základných rovinách:

- zákonnosť použitia informačno-technických prostriedkov verzus právo na ochranu súkromia,
- rozsah použitia informačno-technických prostriedkov z trestno-procesného hľadiska,
- rozsah použitia informačno-technických prostriedkov z časového hľadiska.

Zákonnosť použitia informačno-technických prostriedkov verzus právo na ochranu súkromia

Zásadu primeranosti použitia informačno-technických prostriedkov možno chápať dvojakým spôsobom:

- ako podmienku, podľa ktorej možno použiť uvedené prostriedky len pre presne určené trestné činy
- ak možno dôvodne predpokladať, že budú zistené skutočnosti významné pre trestné konanie.

Primeranosť zabezpečuje rešpektovanie ústavou zaručených práv občanov pri využití informačno-technických prostriedkov, najmä ich právo na ochranu súkromia.

Nasadením informačno-technických prostriedkov sa významne zasahuje do súkromia osoby, hoci sa dané úkony vykonávajú utajene a v záujme naplnenia ich účelu sa vyžaduje, aby dotknutá osoba o ich realizácii nevedela. Utajený spôsob využívania daných úkonov takto podčiarkuje nevyhnutnosť dodržiavania zásady primeranosti ich použitia.

[10] JALČ, A.: Základné zásady trestného konania. In: ŠIMOVČEK, I. a kol.: Trestné právo procesné. Plzeň: Aleš Čeněk, 2011, s. 39.

[11] Tamtiež, s. 40.

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").

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

- každý má právo na rešpektovanie svojho súkromného a rodinného života, obydlia a korešpondencie,
- 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.

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

Rozsudok ESĽP 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. 26

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 ESĽP 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.

Európsky súd pre ľudské práva v tejto súvislosti sformuloval niekoľko hľadísk, ktoré sa posudzujú pri konkrétnom prípade zásahu do práva na súkromie, a to hľadiská legitimity, 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 morálky, zabezpečeniu hospodárskeho blahobytu krajiny) a v záujme jednotlivca (na ochranu jeho práv a slobôd).

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

Proporcionalita 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.

ESĽP 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 ESĽP vo veci Sunday Times proti Spojenému kráľovstvu (rozhodnutie z 26. apríla 1979) 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, legitimity a proporcionality.

Interpretačným pravidlom ESĽP 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.

Právo na súkromie možno vymedziť aj negatívne. V Rozsudku ESĽP vo veci Brüggemann 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.

Rozsah použitia informačno-technických prostriedkov z hľadiska trestno-procesného

V Trestnom poriadku sú stanovené konkrétne trestné činy, v súvislosti s dokazovaním ktorých možno používať informačno-technické prostriedky. Ide o skupiny závažnejších trestných činov, ako sú zločiny, trestné činy korupcie, extrémizmu, zneužívania právomoci verejného činiteľa, trestný čin legalizácie príjmu z trestnej činnosti alebo iný úmyselný trestný čin, o ktorom na konanie zaväzuje medzinárodná zmluva.[12]

Primeranosť použitia informačno-technických prostriedkov musí byť obsiahnutá v príkaze na ich nasadenie. Príkaz je osobitná forma rozhodnutia orgánov činných v trestnom konaní a súdu v prípadoch ustanovených zákonom. Príkazom sa rozhoduje vtedy, keď sa vyžaduje, aby rozhodol orgán činný v trestnom konaní alebo súd, pretože ide o zásah do základných ľudských práv a slobôd občanov, ale tento procesný úkon je nevyhnutné vykonať bez zbytočného odkladu, lebo inak by bol ohrozený účel trestného konania.[13]

Príkaz na odpočúvanie a záznam telekomunikačnej prevádzky (§ 115 TP) a príkaz na zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke (§ 116 TP patria do tej skupiny príkazov, ktorými sa nariaďuje použitie informačno-technických prostriedkov a prostried-

[12] § 115 ods. 1 Trestného poriadku.

[13] ZÁHORA, J.: Príkaz v trestnom konaní. In: Justičná revue: časopis pre právnu prax. č. 5/2004, s. 538.

kov operatívno-pátracej činnosti. Odpočúvanie sa vykonáva na základe príkazu na odpočúvanie a záznamu telekomunikačnej prevádzky, ktorý vydáva predseda senátu a 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 a ak odpočúvanie a záznam telekomunikačnej prevádzky nie je spojené so vstupom do obydlia, môže taký príkaz pred začatím trestného stíhania alebo v prípravnom konaní vydať prokurátor. Príkaz prokurátora 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.

Rozsah použitia informačno-technických prostriedkov z hľadiska z časového hľadiska

Požiadavka primeranej rýchlosti trestného konania je základným cieľom, ktorému sú jednotlivé ustanovenia Trestného poriadku prispôsobené,[14] vrátanie časového rozsahu nasadenia informačno-technických prostriedkov. Časová primeranosť použitia informačno-technických prostriedkov sa musí vždy posudzovať podľa konkrétnych okolností trestnej veci.

Príkaz na odpočúvanie a záznam telekomunikačnej prevádzky sa musí vydať písomne a musí byť odôvodnený a to osobitne na každú účastnícku stanicu alebo zariadenie.[15] V príkaze musí byť určený čas, po ktorý sa bude odpočúvanie a záznam telekomunikačnej prevádzky vykonávať. Čas odpočúvania môže trvať najviac šesť mesiacov. Tento čas môže v prípravnom konaní predĺžiť sudca pre prípravné konanie na návrh prokurátora vždy o ďalšie dva mesiace, a to aj opakovane. Odpočúvanie a záznam telekomunikačnej prevádzky robí príslušný útvar Policajného zboru,[16] ktorý je povinný počas celej doby, po ktorú vykonáva odpočúvanie skúmať, či trvajú dôvody, pre ktoré sa odpočúvanie začalo. Ak takéto dôvody pominuli, odpočúvanie musí byť ihneď zastavené. Ak sa počas odpočúvania zistí, že obvinený komunikuje so svojim obhajcom, takto získané informácie nemožno použiť na účely trestného konania a musia byť predpísaným spôsobom bez meškania zničené.[17]

Záver

Orgány činné v trestnom konaní postupujú tak, aby bol zistený taký skutkový stav veci, o ktorom nie sú dôvodné pochybnosti, a to v rozsahu nevyhnutnom na ich rozhodnutie. Ak by rešpektovali právo na osobnú integritu obvineného absolútne, nemohli by trestné stíhanie vôbec začať. Zásada primeranosti sa aplikuje ako korektív, ktorý umožňuje v rámci trestného konania použiť proti obvinenému informačno-technické prostriedky, pričom platí, že čím závažnejší zásah do osobnej integrity sa realizuje, tým je pre súdne orgány a orgány činné v trestnom konaní dôležitejšie náležite odôvodniť takéto rozhodnutie. Primeranosť použitia informačno-technických prostriedkov sa preto musí vždy posudzovať podľa konkrétnych okolností trestnej veci.

[14] KLÁTIK, J.: Rýchlosť trestného konania ako základná hodnota práva na zákonný a včasný trestný proces. In: ŠIMOVČEK, I. a kol.: Hodnoty trestného práva v teórii a praxi. Trnava: Typi Universitatis Tyrnaviensis 2012, s. 193.

[15] DESET, M.: Zaistenie osôb a vecí a získavanie informácií dôležitých pre trestné konanie. In: ŠIMOVČEK, I. a kol.: Trestné právo procesné. Plzeň: Aleš Čeněk, 2011, s. 122.

[16] § 115 ods. 3 Trestného poriadku.

[17] DESET, M.: Legalita a proporcionalita odpočúvania a záznamu telekomunikačnej prevádzky. In: ŠIMOVČEK, I. a kol.: Hodnoty trestného práva v teórii a praxi. Trnava: Typi Universitatis Tyrnaviensis 2012, s. 315.

Literatúra

CALLIESS, CH. The Trans-nationalization of Values by European Law, German Law Journal 10/2009 s. 1369

DESET, M.: Zaistenie osôb a vecí a získavanie informácií dôležitých pre trestné konanie. In: ŠIMOVČEK, I. a kol.: Trestné právo procesné. Plzeň: Aleš Čeněk, 2011, s. 122

DESET, M.: Legalita a proporcionalita odpočúvania a záznamu telekomunikačnej prevádzky. In: ŠIMOVČEK, I. a kol.: Hodnoty trestného práva v teórii a praxi. Trnava: Typi Universitatis Tyrnaviensis 2012

ESEA, J. K.: Comparison of Procedural Rules in Criminal Proceedings. Congressional Research Service. Washington, D.C 20540-7000

JALČ, A.: Základné zásady trestného konania. In ŠIMOVČEK, I. a kol.: Trestné právo procesné. Plzeň: Aleš Čeněk, 2011, s. 33

KLÁTIK, J.: Rýchlosť trestného konania ako základná hodnota práva na zákonný a včasný trestný proces. In: ŠIMOVČEK, I. a kol.: Hodnoty trestného práva v teórii a praxi. Trnava: Typi Universitatis Tyrnaviensis 2012

LÖÖF, R.: Proposed Minimum Rights in Criminal Proceedings thought-out the EU. In: European Law Journal, Volume 12, Issue 3, 2006

MAFFEI, S.: The European Right to Confrontation in Criminal Proceedings, Absent, Anonymous and Vulnerable Witnesses. Europa Law Publishing, Groningen 2006

REPÍK, B.: Evropská úmluva o lidských právech a trestní právo. Praha: ORAC, 2002

SPRONKEN, T. – ATTINGER M.: Procedural Rights in Criminal Proceedings: Existing Level of Safeguards in the European Union. University of Maastricht 2005

SYLLOVÁ, J., PÍTROVÁ, L., PALDUSOVÁ, H. a kol.: Lisabonská smlouva: komentář. Praha: C. H. Beck, 2010. s. 40 a nasl.

ŠÁMAL, P.: Základní zásady trestního řízení v demokratickém systému. Praha: Codex Bohemia, 1999

TRESCHEL, S.: Human Rights in Criminal Proceedings. European University Institute, Academy of European Law, Oxford University 2005

ZÁHORA, J.: Príkaz v trestnom konaní. In: Justičná revue: časopis pre právnu prax. č. 5/2004

ZÁHORA, J.: Európske hodnoty trestného práva a ich zobrazenie v slovenskom trestnom práve. In: ŠIMOVČEK, I. a kol.: Hodnoty trestného práva v teórii a praxi. Trnava: Typi Universitatis Tyrnaviensis, 2012, s. 24

Konsolidované znenie Zmluvy o Európskej únii a Zmluvy o fungovaní Európskej únie, Ú. v. EÚ C 83, 30. 3. 2010, s. 1 – 388.

Zákon č. 301/2005 Z. z. v znení noviel

https://slovnik.azet.sk/pravopis/slovnik-sj/?q=primeranos%C5%A5 (stiahnuté dňa 12. 2. 2019)

Limity uplatňovania informačno-technických prostriedkov vyplývajúce zo základných zásad trestného konania a z judikatúry Európskeho súdu pre ľudské práva[1]

Limits on the Application of Information and Technology Resources Stemming from the Basic Principles of Criminal Proceedings and the Case Law of the European Court of Human Rights

Peter Polák[2]
Marek Talapka[3]

Abstrakt: *Informačno-technické prostriedky patria k špecifickým prostriedkom získavania informácií dôležitých pre trestné konanie. Ich použitie je spojené so zásahom do ústavných práv občanov, najmä do súkromia. Preto ich použitie je možné len keď je to pre trestné konanie nevyhnutné a len v nevyhnutnom rozsahu. Limity uplatňovania informačno-technických prostriedkov vyplývajú aj zo základných zásad trestného konania a z judikatúry Európskeho súdu pre ľudské práva. Príspevok má snahu tieto limity uplatňovania informačno-technických prostriedkov zistiť a ich obsah vysvetliť.*

Abstract: *Information technology are specific means of obtaining information relevant to criminal proceedings. Their use is linked to interference with citizens' constitutional rights, especially privacy. Therefore, their use is only possible when it is necessary for the criminal proceedings and only to the extent necessary. The limits of application of information and technical means also stem from the basic principles of criminal proceedings and from the case law of the European Court of Human Rights. This contribution seeks to identify these limits of application of information and technical means and to explain their content.*

Kľúčové slová: *Informačno-technické prostriedky, limity použitia informačno-technických prostriedkov, základné zásady trestného konania, judikatúra Európskeho súdu pre ľudské práva.*

Keywords: *Information and technical means, limits of use of information and technical means, basic principles of criminal proceedings, case law of the European Court of Human Rights.*

Úvod

Dosiahnuť účel trestného konania pri vyšetrovaní niektorých sofistikovaných trestných činoch, vrátane tých, ktoré sú vykonané za využitia organizovaných prvkov, medzinárodných prvkov, prípadne konšpiratívnych metód, je skoro nemožné bez využitia adekvátnych prostriedkov na získavanie informácií dôležitých pre trestné konanie. K takýmto špecifickým prostriedkom získavania informácií pre proces dokazovania v rámci trestného konania patria informačno-technické prostriedky. Ich použitie je spojené so zásahom do ústavných práv občanov, najmä do súkromia. Preto ich použitie je možné len keď je to pre trestné konanie nevyhnutné a len v ne-

[1] Tento príspevok je podporovaný Agentúrou na podporu výskumu a vývoja na základe Zmluvy č. APVV-15-0644.

[2] Prof. JUDr. Peter Polák, PhD. Ústav verejného práva, Fakulta práva Paneurópskej vysokej školy, Tomášikova 20, 821 02 Bratislava, e-mail: peter.polak@paneurouni.com.

[3] JUDr. Marek Talapka, Interný doktorand Ústavu verejného práva, Fakulta práva Paneurópskej vysokej školy, Tomášikova 20, 821 02 Bratislava, e-mail: marek.talapka@paneurouni.com.

vyhnutnom rozsahu. Limity uplatňovania informačno-technických prostriedkov vyplývajú aj zo základných zásad trestného konania a z judikatúry Európskeho súdu pre ľudské práva. Zásadným predpokladom uplatňovania limitov pri využívaní informačno-technických prostriedkov v trestnom konaní je ich poznanie . Príspevok je preto zameraný na zistenie a vysvetlenie tých limitov, ktoré vyplývajú zo spomínaných základných zásad trestného konania a z judikatúry Európskeho súdu pre ľudské práva (ďalej len „ESĽP“).

1. Charakter informačno-technických prostriedkov a potreba limitov ich uplatňovania

Vlastným účelom trestného konania je náležite zistiť trestné činy a ich páchateľov podľa zákona spravodlivo potrestať. Ako už bolo uvedené vyšetrovanie niektorých trestných činov by nebolo možné bez použitia niektorých špecifických prostriedkov, ktorými sa zabezpečujú informácie dôležité pre trestné konanie. Takýmito špecifickými prostriedkami sú práve informačno-technické prostriedky, ktoré predstavujú signifikantný nástroj slúžiaci na efektívne odhaľovanie závažných foriem trestnej činnosti. Jedným z podstatných znakov použitia informačno-technických prostriedkov je ich utajovaný spôsob použitia. O takomto použití informačno-technických prostriedkov dotknuté osoby nemajú vedomosť. Informačno-technické prostriedky sa využívajú po určitý čas, a pritom nejde o jednorazovú záležitosť, pričom v priebehu využívania informačno-technických prostriedkov dochádza k intenzívnemu zásahu do základných ľudských práv a slobôd dotknutých osôb. I keď informačno-technické prostriedky predstavujú efektívny nástroj boja proti závažnej trestnej činnosti, získavanie informácií použitím informačno-technických prostriedkov je spojené, a aj vždy bude spojené, so zásahom do základných ľudských práv dotknutých osôb, a to najmä do práva na súkromie. Uvedená skutočnosť priamo evokuje nevyhnutnosť stanovenia jasných právnych podmienok použitia týchto prostriedkov, vrátane stanovenia limitov ich uplatňovania.

Samotný pojem súkromie možno definovať ako tú sféru života, do ktorej nikto (ani štát) nesmie bez súhlasu dotyčnej osoby alebo bez výslovného zmocnenia zákona zasahovať alebo o nej požadovať, či získavať informácie a o ktorej subjekt súkromia nie je povinný informácie dávať, pokiaľ mu to zákon neukladá. Hranice súkromia v tomto zmysle možno vymedziť tak, že súkromím je to, čo subjekt podľa zákona nie je povinný sprístupniť alebo prezradiť niekomu inému.[4]

Pojem súkromie možno chápať v užšom slova zmysle ako ochranu subjektívne vytváranej predstavy o súkromnom živote človeka, v širšom slova zmysle aj ako ochranu širšieho okolia, ktoré bezprostredne nadväzuje na životné potreby a záujmy danej osoby. V zmysle Ústavy SR, medzinárodných dokumentov, ako i judikatúry ESĽP je potrebné pod pojmom súkromie rozumieť súkromie v najširšom zmysle slova. To znamená širšie okolie človeka bezprostredne nadväzujúce na jeho život, životné potreby a záujmy ako napríklad rodina, priatelia, telefonické rozhovory v rámci rodiny a pod.[5]

Na druhej strane treba uviesť, že právo na súkromie nie je právom absolútnej povahy, čo predstavuje, že je možné ho za určitých podmienok obmedziť. K jeho obmedzeniu zo strany štátneho orgánu však môže dôjsť len celkom výnimočne, a to iba na základe zákona, pokiaľ ide o zásah nevyhnutný v demokratickej spoločnosti a smerujúci k uskutočneniu legitímneho cieľa, ktorému je tento zásah primeraný. V tejto spojitosti sa predovšetkým zdôrazňuje, že zasahova-

[4] KLÍMA, K., a kol., 2007. Encyklopedie ustavního práva. Praha: ASPI, 2007, s. 368.
[5] FRIDRICH, B., a kol., 2013. Ústavné garancie ľudských práv. Bratislava: PraF UK, 2013, s. 62 a nasl.

nie štátu musí vždy rešpektovať spravodlivú rovnováhu medzi všeobecným/verejným záujmom spoločnosti na jednej strane a ochranou práva na súkromie jednotlivca na druhej strane pri súčasnom šetrení podstaty a zmyslu obmedzovaného práva. V prípade definovania verejného záujmu ide v zásade o hľadanie legitímneho cieľa, ktorý odôvodňuje zásah do ľudského práva alebo slobody.[6]

Je všeobecne známou skutočnosťou, že limity uplatňovania informačno-technických prostriedkov vychádzajú z troch zdrojov, a to

a) z dokumentov Organizácie spojených národov (ďalej len „OSN"), ktoré obsahujú ustanovenia o ochrane práva na súkromie,
b) z dokumentov Rady Európy a judikatúry ESĽP, ako aj z právnych aktov Európskej únie, ktoré obsahujú ustanovenia o ochrane práva na súkromie, a
c) z vnútroštátneho právneho rámca ochrany práva na súkromie.

Ad a) Z pohľadu roviny ochrany práva na súkromie podľa medzinárodnoprávnych dokumentov v pôsobnosti OSN sú významné najmä dva dokumenty, a to Všeobecná deklarácia ľudských práv[7] a Medzinárodný pakt o občianskych a politických právach.[8] Všeobecná deklarácia ľudských práv v čl. 12 deklaruje, 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 takýmto zásahom alebo útokom".** Zároveň je potrebné poukázať aj na generálnu klauzulu stanovujúcu určitý limit uvedenú v čl. 29 ods. 2, podľa ktorej **„každý je pri výkone svojich práv a slobôd podrobený len takým obmedzeniam, ktoré stanoví zákon a ktoré slúžia výhradne len preto, aby bolo zaručené uznanie a zachovanie práv a slobôd ostatných a aby sa vyhovelo spravodlivým požiadavkám morálky, verejného poriadku a všeobecného blaha v demokratickej spoločnosti".** Podľa čl. 17 Medzinárodného paktu o občianskych a politických právach **„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 zákonnú ochranu proti takým zásahom alebo útokom".**

Aj keď z formálneho hľadiska je Všeobecná deklarácia ľudských práv právne nezáväzná, možno v tejto súvislosti spomenúť Nález Ústavného súdu SR, sp. zn. PL. ÚS 43/95, podľa ktorého **„pri obmedzovaní práva na súkromie nemožno porušiť podmienky prijaté na ochranu súkromia podľa medzinárodných dohovorov o ľudských právach a základných slobodách".**

Ad b) Z pohľadu európskej roviny ochrany práva na súkromie je významný Európsky Dohovor o ochrane ľudských práv a základných slobôd[9] (ďalej len „Dohovor") a Charta základných práv Európskej únie[10] (ďalej len „Charta"). V čl. 8 Dohovor deklaruje právo na súkromie a zároveň stanovuje podmienky, za ktorých štát môže do súkromia zasiahnuť. Podľa čl. 8 **„každý má právo na rešpektovanie svojho súkromného a rodinného života, obydlia 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".**

---

[6] SVÁK, J., 2006. Ochrana ľudských práv (z pohľadu judikatúry a doktríny štrasburských orgánov ochrany práv). II. rozšírené vydanie. Bratislava: Eurokódex, 2006, s. 146.

[7] Prijatá Valným zhromaždením OSN 10. decembra 1948 v Paríži.

[8] Prijatý Valným zhromaždením OSN 16. decembra 1966 v New Yorku.

[9] Európsky Dohovor o ochrane ľudských práv a základných slobôd podpísaný 4. novembra 1950 v Ríme. Oznámenie MZV č. 209/1992 Z. z.

[10] Charta základných práv Európskej únie podpísaná 7. decembra 2000 v Nice.

Zásah štátnych orgánov do práva na súkromie ESĽP posudzuje 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. Pri posudzovaní splnenia podmienky legality štrasburské orgány vychádzajú z toho, či bola rešpektovaná dostupnosť a predvídateľnosť zákona. 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, podobne ako legalita, je priamo stanovená **legitímnosť** zásahu štátnych orgánov. Legitímnosť 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 legitímnosť.

Proporcionalita 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 dosiahnuť 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 prikročiť len vtedy, keď je to nevyhnutné a sledovaný cieľ nemožno dosiahnuť miernejšími prostriedkami.[11]

Z uvedeného teda vyplýva, že do práva na súkromie v zmysle Dohovoru možno zasiahnuť výlučne vtedy a len vtedy, ak je takýto zásah legálny, legitímny a proporcionálny pričom musí ísť o kumulatívne splnenie uvedených podmienok.

Charta v čl. 7 deklaruje, že **„každý má právo na rešpektovanie svojho súkromného a rodinného života, obydlia a komunikácie“**. Podľa čl. 8 **„každý má právo na ochranu osobných údajov, ktoré sa ho týkajú. Tieto údaje musia byť riadne spracované na určené účely na základe súhlasu dotknutej osoby alebo na inom oprávnenom základe ustanovenom zákonom. Každý má právo na prístup k zhromaždeným údajom, ktoré sa ho týkajú, a právo na ich opravu“.** Rovnako nemožno opomenúť čl. 52 ods. 1 Charty, podľa ktorého **„akékoľvek obmedzenie výkonu práv a slobôd uznaných v tejto charte musí byť ustanovené zákonom a rešpektovať podstatu týchto práv a slobôd. Za predpokladu dodržiavania zásady proporcionality možno tieto práva a slobody obmedziť len vtedy, ak je to nevyhnutné a skutočne to zodpovedá cieľom všeobecného záujmu, ktoré sú uznané Úniou, alebo ak je to potrebné na ochranu práv a slobôd iných“.**

Ad c) Z pohľadu vnútroštátnej roviny limity uplatňovania informačno-technických prostriedkov vychádzajú jednak z ústavy č. 460/1992 Zb. Ústava Slovenskej republiky (ďalej len „Ústava SR), z Listiny základných práv a slobôd[12] (ďalej len „Listina“) a jednak zo samostatných práv-

[11] Pozri SVÁK, J., 2006. Ochrana ľudských práv (z pohľadu judikatúry a doktríny štrasburských orgánov ochrany práv). II. rozšírené vydanie. Bratislava: Eurokódex, 2006, s. 584 – 585, a PERHÁCS, Z., PERHÁCSOVÁ, A., 2013. Právna úprava používania informačno-technických prostriedkov (1. časť). In: Justičná revue: časopis pre právnu prax, 2013, roč. č. 4, s. 543 – 545.

[12] Listina základných práv a slobôd bola do právneho poriadku Slovenskej republiky zavedená ústavným zákonom č. 23/1991 Zb., ktorým sa uvádza Listina základných práv a slobôd.

nych predpisov. Podľa čl. 13 ods. 4 Ústavy SR **„pri obmedzovaní základných práv a slobôd sa musí dbať na ich podstatu a zmysel. Takéto obmedzenia sa môžu použiť len na ustanovený cieľ“**. Právo na súkromie je vnútorne členené, a preto je upravené vo všeobecnej rovine i v konkrétnejších ustanoveniach, ktoré upravujú a chránia rôzne vzťahy vyplývajúce z práva na súkromie.[13] Všeobecnú klauzulu ochrany súkromia upravuje čl. 16 ods. 1 Ústavy SR, podľa ktorého **„nedotknuteľnosť osoby a jej súkromia je zaručená**. **Obmedzená môže byť len v prípadoch ustanovených zákonom“.** V ustanoveniach čl. 19 ods. 2 a 3, čl. 21, čl. 22 Ústavy SR sú následne konkretizované ďalšie práva. Podľa čl. 19 ods. 2 a 3 Ústavy SR **„každý má právo na ochranu pred neoprávneným zasahovaním do súkromného a rodinného života a zároveň každý má právo na ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe“**. Podľa čl. 21 Ústavy SR **„obydlie je nedotknuteľné. Nie je dovolené doň 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. Spôsob vykonania domovej prehliadky ustanoví zákon. Iné zásahy do nedotknuteľnosti obydlia 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“.** Podľa čl. 22 Ústavy SR **„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“.**

V tejto spojitosti možno spomenúť Nález Ústavného súdu SR, sp. zn. II. ÚS 1/97, podľa ktorého **„účelom Ústavou SR priznaného práva na súkromie je nielen poskytnúť ochranu práv priznaných podľa § 11 a nasl. zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov (ďalej v texte len „OZ“), ale zároveň aj zabrániť štátnym orgánom ako 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 SR. Týmto ustanovením sa nezaručuje absolútna ochrana súkromného a rodinného života, ale priznáva sa len ochrana pred neoprávneným zasahovaním do súkromného a rodinného života. **Ústava SR teda umožňuje také zásahy do súkromného a rodinného života, ktoré sú oprávnené.**

Listina v čl. 7 ods. 1 ustanovuje, že **„nedotknuteľnosť osoby a jej súkromia je zaručená, obmedziť ju možno iba v prípadoch ustanovených zákonom“**. Čl. 10 ods. 2 Listiny každému zaručuje ochranu pred neoprávneným zasahovaním do súkromného a rodinného života. Čl. 13 Listiny poskytuje ochranu listovému tajomstvu. **„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“.**

Samostatnými osobitnými právnymi predpismi sa rozumejú primárne zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov (ďalej len „TP“), zákon č. 166/2003 Z. z. o ochra-

[13] ŠIMOVČEK, I., 2017. Zákonné limity zabezpečovania informácií dôležitých pre trestné konanie. In: Zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou konanej dňa 23. marca 2017 s názvom Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní. Praha: Leges, 2017, s. 48.

ne 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 je zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.[14] Charakter osobitného zákona v zmysle ustanovenia § 119 ods. 2 TP má aj zákon č. 1/2014 Z. z. o organizovaní verejných športových podujatí v znení neskorších predpisov. Podľa ustanovenia § 21 tohto zákona **„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 tohto zákona".**

Podľa § 10 ods. 21 TP „sa informačno-technickými prostriedkami 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".

Podľa § 2 ods. 1 písm. a), b), c) 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) „sa informačno-technickými prostriedkami 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".

V tejto súvislosti treba uviesť, že pojem informačno-technický prostriedok nie je „terminus technicus" pre označenie prostriedkov využívaných orgánmi štátu na zasahovanie do súkromia osoby. Uvedený pojem je definovaný výlučne v právnom poriadku Slovenskej republiky. Ani právna úprava Českej republiky, ktorá je z historického hľadiska najbližšou právnou úpravou, neobsahuje tento pojem. Za informačno-technický prostriedok sa často chybne označuje napr. inštitút (dôkazný prostriedok) odpočúvania a zaznamenávania telekomunikačnej prevádzky alebo vyhotovovanie obrazových, zvukových a iných záznamov. Ako vyplýva z uvedených definícií, informačno-technický prostriedok je technické zariadenie určené na získavanie informácií, a nie činnosť. Takáto kategorizácia je absolútne nesprávna a dochádza k nej na základe nesprávnej interpretácie definície informačno-technických prostriedkov.[15]

Zjednodušene možno informačno-technické prostriedky definovať ako prostriedky využívané utajovaným spôsobom, ktorými štátny orgán zasahuje do súkromia osôb bez ich predchádzajúceho súhlasu pri:

- vyhľadávaní, otváraní, skúmaní a vyhodnocovaní poštových zásielok a iných dopravovaných zásielok,
- odpočúvaní a zaznamenávaní telekomunikačnej prevádzky,

[14] Škoda len, že tento zákon neobsahuje výslovne také ustanovenie, ako ho obsahoval predchádzajúci zákon o ochrane osobných údajov, ktorý v ustanovení § 15 ods. 7 uvádzal, že „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".

[15] ALÁČ, M., 2015. Získavanie informácií na spravodajské účely a na účely trestného konania. Bratislava: C. H. Beck, 2015, s. 54.

– vyhotovovaní a využívaní obrazových, zvukových, obrazovo-zvukových záznamov alebo iných záznamov.

Ako už bolo uvedené informačno-technické prostriedky sa používajú utajovaným spôsobom, teda bez toho, aby o ich použití mali dotknuté osoby vedomosť. Toto predstavuje základ, s ktorým súvisí samotná podstata informačno-technických prostriedkov, a súčasne je to dôvod, pre ktorý sú uvedené prostriedky tak významné pre trestné konanie. V opačnom prípade, ak by dotknuté osoby vedeli o tom, že ich komunikácia a iné aktivity sú zaznamenávané, pravdepodobne by svoje aktivity obmedzovali, kontakty prerušili tak, aby sa nerealizovala žiadna protiprávna činnosť, prípadne by posilnili krycie legendy takýchto činností a kontaktov. Takáto vedomosť dotknutých osôb o použití informačno-technických prostriedkov by následne smerovala k zmareniu účelu ich používania a pre trestné konania by sa zrejme nezískali objektívne poznatky o skutočnej povahe realizovaných aktivít a o povahe konkrétnej činnosti, kontaktov a pod.[16]

Na záver možno uviesť, že použitím informačno-technických prostriedkov sa výrazným spôsobom zasahuje do základných ľudských práv dotknutých osôb, a to do práva na súkromie, a z tohto dôvodu sú nevyhnutné limity ich uplatňovania. Zároveň sa požaduje, aby existoval dostatočný ako i efektívny systém garancií ochrany práv pred zásahmi, ktoré sú nezákonné, neprimerané a neodôvodnené. Garanciu ochrany práv by mala zabezpečovať tá právna úprava, ktorá použitie takýchto zásahov umožňuje. Na tieto účely je zameraná celková úprava podmienok, za ktorých sa konkrétny inštitút môže využiť, stanovuje sa okruh trestných činov, pri ktorých je ich možné nariadiť, fázy konania, v ktorých je možné inštitút vykonávať, stanovený je subjekt oprávnený rozhodnúť o ich použití, písomná forma príkazu, jeho odôvodnenie, možnosti využitia zistených informácií, úprava spôsobu kontroly dodržiavania zákonnosti pri ich využívaní a v neposlednom rade sú upravené možnosti informovania dotknutých osôb.

2. Limity uplatňovania informačno-technických prostriedkov podľa zásad trestného konania

Základnou úlohou trestného konania je zistiť, či sa stal trestný čin, zistiť jeho páchateľa a rozhodnúť o jeho potrestaní. Tomu korešponduje aj pôsobenie orgánov činných v trestnom konaní a súdov, ako aj iných subjektov trestného konania pri upevňovaní zákonnosti, uskutočňovanie výchovy občanov v duchu dôsledného zachovávania zákonov a pravidiel občianskeho spolužitia a čestného plnenia povinností voči sebe navzájom, voči štátu a spoločnosti a preventívne pôsobenie. Takýto cieľ je možné naplniť len v tom prípade, ak trestné konanie vychádza z určitých vyšších princípov a pravidiel, ktoré sa prierezovo a dôsledne aplikujú počas trestného konania. Ide o tzv. základné zásady trestného konania, ktoré sa chápu ako pramene, východiskové body nielen trestného konania, ale aj trestného práva procesného ako celku, a ich správne formulovanie je nezanedbateľným aspektom nielen pri aplikácií TP, ale aj pri jeho vypracovávaní a schvaľovaní, ako aj pri jeho ďalších zmenách.[17]

Základné zásady trestného konania predstavujú tie vedúce právne idey, ktorým toto postavenie priznáva zákon. Na základných zásadách je vybudovaný celý trestný proces, celá organizácia trestného konania, rozdelenie funkcií v trestnom konaní, teda aj všetky systémové a štrukturál-

[16] PERHÁCS, Z., PERHÁCSOVÁ, A., 2013. Právna úprava používania informačno-technických prostriedkov (2. časť). In: Justičná revue: časopis pre právnu prax, 2013, č. 5, s. 708.

[17] MUSIL, J., KRATOCHVÍL, V., ŠÁMAL, P., a kol., 2007. Kurs trestního práva. Trestní právo procesní. 3. přeprac. vyd. Praha: C. H. Beck, 2007, s. 106.

ne trestno-procesné vzťahy. Bez samotného pochopenia významu základných zásad trestného konania nemožno porozumieť jednotlivým ustanoveniam TP a správne ich aplikovať v praxi.[18]

Vzhľadom na tieto skutočnosti možno teda uviesť, že použitie informačno-technických prostriedkov musí byť v súlade so základnými zásadami trestného konania. To znamená, že limitácia uplatňovania informačno-technických prostriedkov je daná aj podľa základných zásad trestného konania. Za základné zásady trestného konania, ktoré limitujú uplatňovanie informačno-technických prostriedkov možno považovať **zásadu stíhania len zo zákonných dôvodov a zákonným spôsobom, zásadu primeranosti a zdržanlivosti, vyhľadávaciu zásadu a zásadu zistenia skutkového stavu veci, o ktorom nie sú dôvodné pochybnosti.**

Zásada stíhania len zo zákonných dôvodov a zákonným spôsobom je obsiahnutá v ustanovení § 2 ods. 1 TP, podľa ktorého nikto nemôže byť stíhaný ako obvinený inak než zo zákonných dôvodov a spôsobom, ktorý ustanovuje tento zákon. Uvedená zásada limituje uplatňovanie použitie informačno-technických prostriedkov tým, že **zásah do súkromia dotknutej osoby je možný len na základe zákona a spôsobom, ktorý je v súlade so zákonom**. Taktiež uvedená zásada limituje uplatňovanie informačno-technických prostriedkov tým, že **príkaz alebo návrh na použitie informačno-technických prostriedkov, predstavujúci zásah do práva na súkromie musí byť náležitým spôsobom odôvodnený** napr. podľa § 108 ods. 4 TP „...Príkaz na vydanie zásielok podľa odseku 2 sa musí odôvodniť", podľa § 114 ods. 2 TP „Príkaz na vyhotovenie 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...", podľa § 115 ods. 3 TP „Príkaz na odpočúvanie a záznam telekomunikačnej prevádzky sa musí vydať písomne a odôvodniť aj skutkovými okolnosťami, a to osobitne na každú účastnícku stanicu alebo zariadenie...", podľa § 116 ods. 2 TP „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...,zisťovanie a oznamovanie týchto údajov môže trvať najviac šesť mesiacov, tento čas môže v prípravnom konaní na písomný a odôvodnený návrh prokurátora sudca pre prípravne konanie predĺžiť vždy o ďalšie dva mesiace, a to aj opakovane...".

Zásada primeranosti a zdržanlivosti predstavuje jednu z nových procesných zásad, ktorá je upravená v ustanovení § 2 ods. 2 TP, podľa ktorého 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. Výrazom limitov uplatňovania informačno-technických prostriedkov v prípade zásady primeranosti a zdržanlivosti je **obmedzenie rozsahu trestných činov, v prípade ktorých možno použiť informačno-technické prostriedky** napr. podľa § 114 ods. 1 TP „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, možno vyhotoviť obrazový, zvukový alebo obrazovo-zvukový záznam...", podľa § 114 ods. 2 TP „...Vyhotovenie obrazových, zvukových alebo obrazovo-zvukových záznamov spojených s priamym vstupom do obydlia 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 me-

[18] IVOR, J., POLÁK, P., ZÁHORA, J., 2017. Trestné právo procesné I. Bratislava: Wolters Kluwer, 2017, s. 51.

dzinárodná zmluva...“, podľa § 114 ods. 7 TP „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 príjmu z trestnej činnosti alebo pre iný úmyselný trestný čin, o ktorom na konanie zaväzuje medzinárodná zmluva.“, podľa § 115 ods. 1 TP „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 a záznam telekomunikačnej prevádzky...“, podľa § 115 ods. 5 TP „V trestnom konaní pre iný úmyselný trestný čin, ako je uvedený v odseku 1, môže vydať príkaz na odpočúvanie a záznam telekomunikačnej prevádzky predseda senátu...“, podľa § 116 ods. 1 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, možno vydať príkaz na zistenie a oznámenie údajov o telekomunikačnej prevádzke...“.

Ďalším výrazom limitov uplatňovania informačno-technických prostriedkov prostredníctvom zásady primeranosti a zdržanlivosti je aj samotné vyjadrenie v konkrétnych ustanoveniach TP **kedy a za akých podmienok možno uplatniť informačno-technické prostriedky**[19] napr. v § 108 ods. 1 TP „Ak je na objasnenie skutočností závažných pre trestné konanie nevyhnutné zistiť obsah nedoručených telegramov, listov alebo iných zásielok...“, v § 108 ods. 2 TP „...ak je na objasnenie skutočností závažných pre trestné konanie nevyhnutné zistiť jej obsah.“, v § 114 ods. 1 TP „...možno vyhotoviť obrazový, zvukový alebo obrazovo-zvukový záznam, ak možno dôvodne predpokladať, že ním budú zistené skutočnosti významné pre trestné konanie.“, v § 114 ods. 2 TP „...Vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov spojených s priamym vstupom do obydlia je prípustné len v trestnom konaní o zločine...“, v § 115 ods. 1 TP „...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.“, v § 115 ods. 2 TP „...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 obydlia, ktorý však musí najneskôr do 24 hodín od jeho vydania potvrdiť sudca pre prípravné konanie...“, v § 115 ods. 5 TP „V trestnom konaní pre iný úmyselný trestný čin, ako je uvedený v odseku 1, môže vydať príkaz na odpočúvanie a záznam telekomunikačnej prevádzky predseda senátu, pred začatím trestného stíhania alebo v prípravnom konaní sudca pre prípravné konanie na návrh prokurátora iba so súhlasom užívateľa odpočúvaného alebo zaznamenávaného telekomunikačného zariadenia.“, v § 116 ods. 1 TP „...možno vydať príkaz na zistenie a oznámenie údajov o telekomunikačnej prevádzke, ktoré sú predmetom telekomunikačného tajomstva, alebo na ktoré sa

[19] ZÁHORA, J., 2018. Uplatňovanie zásady primeranosti a zdržanlivosti pri využívaní informačno-technických prostriedkov v trestnom konaní v Slovenskej republike. In: Časopis pro právní vědu a praxi, 2018, roč. 26, č. 1, s. 33 – 35.

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 sťažené". Uplatnením zásady primeranosti a zdržanlivosti, ako limitu použitia informačno-technických prostriedkov, je aj **požiadavka ich subsidiárneho použitia**, a to vtedy, ak „nemožno sledovaný cieľ dosiahnuť inak alebo ak by bolo jeho dosiahnutie iným spôsobom podstatne sťažené". Konkrétne je to v prípade podľa § 115 ods. 1 druhá veta Trestného poriadku, podľa ktorého jednou z kumulatívnych podmienok vydania príkazu na odpočúvanie a záznam telekomunikačnej prevádzky je podmienka „ak nemožno sledovaný cieľ dosiahnuť inak alebo ak by bolo jeho dosiahnutie iným spôsobom podstatne sťažené", ako aj v prípade podľa § 116 ods. 1 posledná veta Trestného poriadku, podľa ktorého je taktiež jednou z kumulatívnych podmienok vydania príkazu na oznámenie údajov o telekomunikačnej prevádzke taká istá podmienka.

Vyhľadávacia zásada a zásada zistenia skutkového stavu veci, o ktorom nie sú dôvodné pochybnosti je obsiahnutá v § 2 ods. 10 TP, podľa ktorého orgány činné v trestnom konaní postupujú tak, aby bol zistený skutkový stav veci, o ktorom nie sú dôvodné pochybnosti, a to v rozsahu nevyhnutnom na ich rozhodnutie. V zmysle zásady oficiality orgány činné v trestnom konaní s rovnakou starostlivosťou objasňujú okolnosti svedčiace proti obvinenému, ako aj okolnosti, ktoré svedčia v jeho prospech, a v oboch smeroch vykonávajú dôkazy tak, aby umožnili súdu spravodlivé rozhodnutie. Dôkazy obstarávajú z úradnej povinnosti. V tejto spojitosti možno spomenúť aj ustanovenie § 1 TP, podľa ktorého „Trestný poriadok upravuje postup orgánov činných v trestnom konaní a súdov tak, aby trestné činy boli náležite zistené a ich páchatelia podľa zákona spravodlivo potrestaní, pričom treba rešpektovať základné práva a slobody fyzických osôb a právnických osôb."

Zásada zistenia skutkového stavu veci, o ktorom nie sú dôvodné pochybnosti limituje uplatňovanie informačno-technických prostriedkov, v tom zmysle, že **k použitiu informačno-technických prostriedkov by malo dôjsť až v takom prípade, keď zistený skutkový stav veci dostatočne odôvodňuje použitie takých prostriedkov**, ktoré invazívnym spôsobom zasahujú do práva na súkromie, čím sa rozumejú zásahy prostredníctvom informačno-technických prostriedkov. Takéto odôvodnenie by sa malo premietnuť aj do samotných návrhov a rovnako do príkazov na použitie informačno-technických prostriedkov. Z tejto základnej zásady možno odvodiť aj limit, že **informačno technický prostriedok možno použiť vtedy, ak je to nevyhnutné na zistenie skutkového stavu veci, o ktorom nie sú pochybnosti, a to v rozsahu nevyhnutnom na ich rozhodnutie**. Uvedená zásada limituje uplatňovanie informačno-technických prostriedkov aj v tom zmysle, že **ak použitím informačno-technických prostriedkov sa zistil skutkový stav veci, o ktorom nie sú dôvodné pochybnosti, a to v rozsahu nevyhnutnom na ich rozhodnutie, tak použitie informačno-technických prostriedkov by sa malo ukončiť**. Rovnako však je potrebné spomenúť, že uvedená zásada v sebe zahŕňa nielen pochybnosti o zistení skutkového stavu, ale zároveň pochybnosti o možnosti obstarania a vykonania ďalších dôkazov, ktoré by tento skutkový stav, resp. vykonané dokazovanie zmenili.

Z vyššie uvedeného teda vyplýva, že **k použitiu informačno-technických prostriedkov by malo dôjsť, až v tom prípade, keď prokurátor resp. sudca vzhľadom na doposiaľ zistený skutkový stav veci nadobudne presvedčenie, ktoré by malo byť premietnuté v odôvodnení návrhu resp. príkazu, že je potrebné použiť informačno-technické prostriedky**. Možno vychádzať z premisy, že informačno-technické prostriedky predstavujú prostriedok „ultima ratio", čo znamená, že štátne orgány by sa k použitiu takéhoto invazívneho prostriedku mali uchýliť až vtedy, keď predošle dôkazné prostriedky sa javili ako nedostačujúce resp. nepostačujúce a súčasný

skutkový stav veci si to vyžaduje. To znamená, že k takýmto zásahom do garantovaných ľudských práv nemôže dochádzať svojvoľne a bezohľadne, ale až po ich dôkladnom zvážení.

Vyhľadávacia zásada úzko súvisí so zásadou zistenia skutkového stavu veci, o ktorom nie sú dôvodné pochybnosti a rovnako je vyjadrená v ustanovení § 2 ods. 10 TP. V zmysle uvedenej zásady, **orgány činné v trestnom konaní sú povinné objasňovať jednak okolnosti svedčiace proti obvinenému a jednak aj okolnosti svedčiace v prospech obvineného**, nakoľko orgány činné v trestnom konaní sú povinné obstarávať dôkazy na zistenie skutkového stavu veci. Limity uplatňovania informačno-technických prostriedkov v zmysle vyhľadávacej zásady možno vidieť v tom, že úlohou orgánov činných v trestnom konaní nie je preukázať vinu, ale zistiť skutkový stav veci, a zároveň preukázať, že jednotlivé skutkové okolnosti, ktoré tvoria mozaiku pravdepodobného priebehu skutkového stavu veci, stoja na reálnom základe a vzájomne do seba zapadajú. Až následne orgány činné v trestnom konaní majú skutkový stav veci nezávisle posúdiť, bez ohľadu na vonkajšie vplyvy, a až na takomto základe prijať adekvátne rozhodnutia. Je potrebné uviesť, že je nielen v rozpore so zmyslom trestného konania v právnom štáte, ale priamo i protizákonné, ak predstavitelia orgánov činných v trestnom konaní vnímajú svoju rolu iba ako činiteľov, ktorí majú dokázať vinu a takto úspešne uzatvárať prípady, čo sa bude dobre vynímať v oficiálnych štatistikách. Takéto vnímanie poslania orgánov činných v trestnom konaní je taktiež v rozpore so základnými zásadami trestného konania, ktoré sú priamo záväzné. Na záver je potrebné dodať, že dôsledné dodržiavanie zásad uvedených v ustanovení § 2 ods. 10 TP je vecou osobnej zodpovednosti a nevyhnutnej miery zdravého idealizmu vloženého do inak pragmatického prístupu k veci u každého jednotlivého predstaviteľa orgánov činných v trestnom konaní.[20]

3. Limity uplatňovania informačno-technických prostriedkov podľa judikatúry ESĽP

Limity uplatňovania informačno-technických prostriedkov možno pozorovať aj v obsahu relevantnej judikatúry ESĽP. Ochrana ľudských práv a možné zásahy štátnych orgánov do takýchto práv totiž boli a neustále sú imanentnou súčasťou posudzovania a rozhodovania ESĽP.

Vo svojej skoršej judikatúre súd považoval tieto práva za absolútne, t. zn. zasadzoval sa za absolútnu ochranu týchto práv. Postupom času, najmä vplyvom rozvoja organizovaného zločinu, ktorý začal ohrozovať Európu, súd pripustil, že zásahy do týchto práv sú možné za striktného splnenia určitých podmienok. ESĽP vo svojom rozhodnutí z roku 1968 pod názvom „Belgický jazykový prípad“[21] považoval právo na súkromie, právo na ochranu rodinného života, právo na ochranu komunikovaných skutočností za tak závažné, že ich považoval za absolútne práva, do ktorých sa akýkoľvek zásah nepripúšťa a štátne orgány za žiadnych okolností nemajú možnosť a ani oprávnenie do nich zasahovať. Avšak už v roku 1978 súd vo svojom rozhodnutí[22] konštatoval, že určité zásahy do práva na súkromie sú možné, no musia spĺňať požiadavky uvedené v čl. 8 ods. 2 Dohovoru.[23] Uvedeným prelomovým rozhodnutím súd pripustil, že právo na ochranu súkromia je právom relatívnym.

[20] KOLESÁR, J., 2010. Perspektívy dokazovania v trestnom konaní s dôrazom na znalecké dokazovanie. Prievidza: Citicom, 2010, s. 17 – 18.

[21] Rozsudok ESĽP z 23. júla 1968 „Belgický jazykový prípad“.

[22] Rozsudok ESĽP zo 6. septembra 1978 vo veci Klass vs. Nemecko.

[23] TITTLOVÁ, M., 2016. Kritické zhodnotenie trestnoprávnej úpravy odpočúvania a záznamu telekomunikačnej prevádzky. In: Justičná revue: časopis pre právnu prax, 2016, roč. 68, č. 6–7, s. 750.

ESĽP pri posudzovaní prípadov týkajúcich sa použitia prostriedkov, ktoré zasahujú do garantovaných ľudských práv, kladie osobitý dôraz na podmienku súladu so zákonom, teda zlučiteľnosť vnútroštátnej právnej úpravy s garanciou práv podľa čl. 8 Dohovoru. V zmysle ustálenej judikatúry ESĽP uvedená podmienka je vyjadrená implicitne v požiadavke, **aby príslušný zákon, ktorý predstavuje zákonný podklad pre opatrenia zasahujúce do súkromia dotknutých osôb, bol takýmto osobám dostatočne prístupný, aby mohli predvídať dôsledky jeho aplikácie a súčasne aby bol zlučiteľný s princípmi právneho štátu**. Neznamená to však, že „predvídateľnosť" má znamenať, že osoba bude spôsobilá predvídať, že štátne orgány voči nej využívajú tajné opatrenia na jej sledovanie. Ide o požiadavku, aby vnútroštátna úprava bola dostatočne jasná a zrozumiteľná, aby osoba vedela predvídať za akých okolností a za akých podmienok je možné použiť voči nej takéto opatrenia. ESĽP zároveň zdôraznil, **potrebu adekvátnych a účinných záruk voči zneužitiu**, čo je odrazom limitov využitia takýchto prostriedkov každého jednotlivého štátu. Z judikatúry ESĽP v súvislosti s možnými zásahmi do práv garantovaných v čl. 8 Dohovoru vyplýva, že **ak majú byť tieto zásahy prípustné a ospravedlniteľné, je nutné striktné a jasné stanovenie limitov použitia prostriedkov**, ktorými je možné do nich zasiahnuť.

Možno teda povedať, že ustanovenia čl. 8 Dohovoru, podľa ktorých možno zasiahnuť za istých okolností do práva na súkromie, neskôr dotvorila judikatúra ESĽP, na ktorú sa často odvoláva aj Ústavný súd Slovenskej republiky.

Vzhľadom na skutočnosť, že závažnosť možných zásahov štátu do súkromia je mnohokrát spojená s ťažko napraviteľnými následkami, ESĽP posudzuje právo na súkromie vo všetkých prípadoch veľmi citlivo. Pri jednotlivých prípadoch kladie veľký dôraz na posudzovanie kvality relevantnej vnútroštátnej úpravy daného štátu a preto právo na súkromie vykladá judikatúrou vo vzťahu ku každému riešenému prípadu osobitne. V každom prípade sa posudzuje oprávnenosť zásahov do práva na súkromie (nielen prostredníctvom informačno-technických prostriedkov) a skúma sa, či daný skutkový stav možno „ratio materiae" považovať za súčasť práva na súkromie. ESĽP mnohokrát vyslovil porušenie článku 8 Dohovoru, práve z dôvodu nedostatočnej podrobnosti príslušných zákonov. Vývoj názorov ESĽP na možnosti zásahov do súkromia použitím aj informačno-technických prostriedkov možno sledovať na nasledovných jednotlivých rozhodnutiach:

Prípad Marcks proti Belgicku[24] z roku 1970. Sudca si v uvedenom prípade vyložil právo na súkromie nasledovne: Osoba a jeho rodina by nemala byť vystavená prehliadkam a vypočúvaniam v prostredí domova, výsluchom, nasadzovaniu skrytých odpočúvacích prístrojov (špicľovaniu), nahrávaniu telefonických rozhovorov alebo ich prerušovaním – stručne celej škále fašistických a komunistických inkvizítorských praktík takých, ako boli zriedkavo známe, prinajmenej v západnej Európe, od období náboženskej intolerancie a útlaku až pokým (ideológia nahradila náboženstvo) sa znovu nestali prevládajúcimi v mnohých krajinách medzi dvoma svetovými vojnami a neskôr.

Prípad Klass proti Nemecku[25] z roku 1978. Ide prelomovým judikát, v ktorom ESĽP povolil možnosť sledovania podozrivých osôb a využiť voči nim prostriedky tajného dohľadu. V uvedenom prípade súd pripustil, že zásahy do práva na súkromie (v uvedenom prípade išlo o o zásah prostredníctvom informačno-technických prostriedkov – odpočúvanie a záznam telekomunikačnej prevádzky) sú prípustné a ospravedlniteľné, avšak len vtedy, ak spĺňajú podmienky čl. 8 ods. 2 Dohovoru. ESĽP vyžaduje reštriktívnu interpretáciu predmetného článku a presvedčivosť preukázania nevyhnutnosti použitia takýchto invazívnych prostriedkov do súkromia. Pod-

[24] Rozsudok ESĽP z 13. júna 1970 vo veci Marckx vs. Belgicko.
[25] Rozsudok ESĽP zo 6. septembra 1978 vo veci Klass vs. Nemecko.

ľa ESĽP prostriedky tajného dohľadu môžu byť voči jednotlivcom použité a opodstatňujú ich dve okolnosti: technický pokrok zaznamenaný vo vývoji špionážnych prostriedkov a následne aj v prostriedkoch kontrašpionážneho dohľadu a druhou okolnosťou je rozmach terorizmu v Európe. Uvedené okolnosti zapríčiňujú, že demokratické zriadenia sa ocitajú v ohrození. V uvedenom prípade teda súd pripustil, že existencia právnej úpravy, ktorou sa umožňuje uplatnenie tajného dohľadu nad poštovými zásielkami a telekomunikáciami za výnimočných podmienok je v demokratickej spoločnosti nevyhnutná v záujme národnej bezpečnosti alebo na predchádzanie zločinnosti.

Prípad Malone proti Spojenému kráľovstvu[26] z roku 1984. V uvedenom prípade sa nepodarilo britskej vláde preukázať pred ESĽP, že jej právomoc odpočúvať telefonické rozhovory má jasný, zrozumiteľný a predvídateľný zákonný podklad na nasadenie uvedeného prostriedku. Podľa súdu nebola splnená základná podmienka, aby možné zásahy do práva na súkromie boli obmedzené iba na základe zákona, pričom podľa jeho skoršej judikatúry sa vyžaduje, aby zákon bol občanom dostatočne prístupný, sformulovaný s dostatočnou presnosťou, aby umožnil občanovi prispôsobiť svoje konanie, aby bol občan schopný odhadnúť podmienky a okolnosti za ktorých jeho konanie poskytne štátnym orgánom oprávnenie k zásahu do jeho garantovaných práv. V Spojenom kráľovstve nebol dostatočne jasne určený rozsah a spôsob, ktorým bolo uskutočňované rozhodnutie úradov rozhodujúcich o využití odpočúvania. Možné zásahy do garantovaných práv neboli upravené jasným zákonom, ale celou radou neprehľadných právnych predpisov a princípmi common law.

Prípad Mersch a ďalší proti Luxembursku[27] z roku 1985. ESĽP stanovil, že úroveň podrobností, s akou majú byť vo vnútroštátnom zákone definované podmienky a okolnosti, kedy môže byť zásah štátu použitý, má poskytovať iba všeobecnú pravdepodobnosť týchto okolností, aby jedinec vedel, v akých situáciách môže byť jeho telefónny hovor odpočúvaný. Nikdy nie možnosť jedinca vopred varovať na možnosť odpočúvania v danej konkrétnej situácii.

Prípad Valenzuela Contreras proti Španielsku[28] z roku 1998. ESĽP v uvedenom prípade konštatoval, že požiadavka predvídateľnosti zákona znamená v oblasti monitorovania telefonických rozhovorov to, že vo vnútroštátnom práve musia byť jednoznačne stanovené záruky stanovujúce rozsah pre uváženie príslušných orgánov a spôsob, ktorým má byť monitorovanie uskutočnené, aby tak jasne limitovali uváženie orgánov štátu pri aplikácii týchto prostriedkov.

Prípad Kruslin proti Francúzsku[29] z roku 1990. V uvedenom prípade ESĽP posudzoval súlad francúzskeho zákonného podkladu pre odpočúvanie. Francúzsky trestný zákon obsahoval nasledovné ustanovenie: „Vyšetrujúci sudca použije v súlade so zákonom všetky vyšetrovacie prostriedky, ktoré považuje za užitočné k nájdeniu pravdy". Francúzske súdy si predmetné ustanovenie vykladali ako zmocňujúce na nariadenie odpočúvania. Podľa ESĽP predmetné ustanovenie bolo v rozpore s Dohovorom, z dôvodu absencie záruk proti svojvoľnému zneužitiu poskytnutej právomoci, čím nebola splnená požiadavka existencie primeraných opatrení proti zneužitiu, ktorá by mala stanoviť okruh činov, pri ktorých je možné takýto prostriedok využiť, dobu trvania a pod.

Prípad Rotaru proti Rumunsku[30] z roku 2000. ESĽP posudzoval, či zákon umožňujúci zásah do práva na súkromie je pre osoby dostupný a predvídateľný. Súd stanovil minimálne požiadav-

[26] Rozsudok ESĽP zo 2. augusta 1984 vo veci Malone vs. Spojené kráľovstvo.
[27] Rozsudok ESĽP z 10. mája 1985 vo veci Mersch a ďalší vs. Luxembursko.
[28] Rozsudok ESĽP zo 30. júla 1998 vo veci Valenzuela Contreras vs. Španielsko.
[29] Rozsudok ESĽP z 24. apríla 1990 vo veci Kruslin vs. Francúzsko.
[30] Rozsudok ESĽP zo 4. mája 2000 vo veci Rotaru vs. Rumunsko.

ky na záruky, ktoré by mali byť stanovené vo vnútroštátnom zákone tak, aby zabránili možnému zneužitiu. Zákon podľa ESĽP musí upravovať vymedzenie trestných činov, pri ktorých je možné odpočúvanie použiť (musí ísť o závažnú trestnú činnosť, v žiadnom prípade nesmie ísť o „každý" trestný čin), vymedzenie skupín osôb, ktoré môžu byť odpočúvané, procedúru posudzovania, využívania a ukladania dát získaných odpočúvaním, záruky proti získaniu dát z odpočúvania inými osobami, či inému zneužitiu (dohľad súdu alebo zakotvenie inej nezávislej kontroly), ako aj podmienky, podľa ktorých majú byť výsledky z odpočúvania vymazané či inak zničené.

Prípad Liberty a ďalší proti Spojenému Kráľovstvu[31] z roku 2008. ESĽP v uvedenom prípade preskúmaval vnútroštátnu právnu úpravu a dospel k záveru, že nebola dostatočne jasná, neposkytovala primeranú ochranu proti zneužitiu, priznávala štátnym orgánom taký rozsah a spôsob výkonu zachytávania a odpočúvania telekomunikácie, ktorá poskytovala širokú mieru ich voľnej úvahy. Predovšetkým neupravovala vo verejnosti dostupnej podobe žiadnu selekciu, odovzdávanie, uchovávanie a zničenie zachyteného materiálu, ako to vyžaduje skoršia judikatúra súdu.

Prípad Kirov proti Bulharsku z 2008.[32] V uvedenom prípade sa ESĽP zaoberal požiadavkou existencie ex post notifikačného mechanizmu v právnej úprave Bulharska. Súd skonštatoval, že sťažovateľ, ktorý sa dozvedel o odpočúvaní, nemal možnosť získať žiadne 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", a boli zničené ešte pred skončením trestného konania proti nemu na základe interného predpisu ministra vnútra. Súd v uvedenom prípade skonštatoval, že bulharská vnútroštátna úprava jednoznačne preukazuje absenciu akejkoľvek „a posteriori" kontroly, či už automatickej alebo na základe žiadosti dotknutej osoby a osoby nepožívajú minimálne záruky proti svojvoľným zásahom do ich práv.

Prípad Kvasnica proti Slovenskej republike[33] z roku 2009. Premetom sťažnosti bolo posudzovanie či došlo k zásahu do práva na súkromie sťažovateľa, ktorý pred súdom tvrdil, že zo strany štátnych orgánov došlo k takému zásahu do jeho telefonickej komunikácie, ktorý nebol v súlade so slovenskými zákonmi, ale predovšetkým nešlo o zásah, ktorý by bol v demokratickej spoločnosti nevyhnutný. Sťažovateľ taktiež namietal porušenie čl. 6 Dohovoru, keďže v danom čase neexistovali zákonné pravidlá, ktoré by určovali vecnú príslušnosť súdov vo vzťahu k agende odpočúvania a poukazoval na nesúlad realizovaných opatrení voči nemu s platnou právnou úpravou, ako aj jej kvalitu, predovšetkým na nedostatočný spôsob upravenia záruk proti zneužitiu. Okolnosti prípadu boli preverované zo strany inšpekcie ministerstva vnútra, ktorá na tento účel zriadila komisiu odborníkov, tí ale nezistili žiadne porušenia právnych predpisov v uvedenom prípade p. Kvasnicu. ESĽP napriek tomu poukázal na množstvo pochybení zo strany štátnych orgánov, pokiaľ ide o dodržanie právnych predpisov v sťažovateľovom prípade. Súd uviedol, že v sťažovateľovom prípade neboli splnené všetky zákonné podmienky, najmä že 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 hovorov medzi sťažovateľom ako advokátom a jeho trestne stíhanými klientmi, že zásah obmedzil nedotknuteľnosť jeho obydlia, súkromný charakter korešpondencie iba v rozsahu, ktorý bol nevyhnutný. Z uvedených dôvodov ESĽP vyslovil porušenie čl. 8 Dohovoru.

[31] Rozsudok ESĽP z 1. júla 2008 vo veci Liberty a ďalší vs. Spojené kráľovstvo.
[32] Rozsudok ESĽP z 22. mája 2008 vo veci Kirov proti Bulharsku.
[33] Rozsudok ESĽP z 9. júna 2009 vo veci Kvasnica proti Slovenskej republike.

V tejto súvislosti je treba uviesť, že ESĽP naďalej pokračuje v posudzovaní jednotlivých prípadov, v ktorých malo prísť zo strany štátnych orgánov k zásahu do súkromia prostredníctvom použitia prostriedkov na utajené získanie informácií, pričom každý prípad posudzuje prísne individuálne, ale na druhej strane v súlade so zovšeobecnenými doteraz judikovanými požiadavkami na limity (podmienky) zásahov do súkromia takýmito prostriedkami tak, ako je to uvedené v predchádzajúcom texte.

Záver

Na základe skutočností uvedených v príspevku možno konštatovať, že slovenské právne prostredie vytvára vo všeobecných, ale aj v špeciálnych právnych predpisoch dostatok limitov pre legálne, legitímne a proporcionálne používanie informačno-technických prostriedkov v trestnom konaní, tak ako to vyplýva z relevantných ustanovení medzinárodnej a nadnárodnej úpravy, vrátane judikatúry ESĽP. Existujúca národná právna úprava nie je úplne ideálna, ale aj tak je v súlade s požiadavkami vyplývajúcimi z judikatúry ESĽP, ktorá sa vzťahuje na zásahy do súkromia občanov. Predovšetkým ide o splnenie požiadavky predvídateľnosti použitia zásahov do súkromia takýmito prostriedkami, požiadavky existencie adekvátnych a účinných záruk proti zneužitiu takýchto prostriedkov, ako aj požiadavky striktnosti a jasnosti stanovenia právnych limitov použitia týchto prostriedkov. Napriek tomu nie je možné v jednotlivých prípadoch úplne vylúčiť, aby v procese realizácie informačno-technických prostriedkov a v procese nakladania s informáciami získanými takýmito postupmi nedochádzalo k porušeniu, či obchádzaniu, niektorých limitov. To už ale nie je ani tak otázka právnej úpravy, ako skôr otázka jej aplikácie.

Literatúra

ALÁČ, M., 2015. Získavanie informácií na spravodajské účely a na účely trestného konania. Bratislava: C. H. Beck, 2015, 184 s. ISBN 978-80-89603-32-9

FRIDRICH, B., a kol., 2013. Ústavné garancie ľudských práv. Bratislava: PraF UK, 2013, 270 s. ISBN 978-80-7160-338-2

IVOR, J., POLÁK, P., ZÁHORA, J., 2017. Trestné právo procesné I. Bratislava: Wolters Kluwer, 2017, 526 s. ISBN 978-80-8168-593-4

KLÍMA, K., a kol., 2007. Encyklopedie ústavního práva. Praha: ASPI, 2007, 776 s. ISBN 978-80-7357-295-2

KOLESÁR, J., 2010. Perspektívy dokazovania v trestnom konaní s dôrazom na znalecké dokazovanie. Prievidza: Citicom, 2010, 176 s. ISBN 978-80-89433-00-1

MUSIL, J., KRATOCHVÍL, V., ŠÁMAL, P., a kol., 2007. Kurs trestního práva. Trestní právo procesní. 3. přeprac. vyd. Praha: C. H. Beck, 2007, 1166 s. ISBN 978-80-7179-572-8

PERHÁCS, Z., PERHÁCSOVÁ, A., 2013. Právna úprava používania informačno-technických prostriedkov (1. časť). In: Justičná revue: časopis pre právnu prax, 2013, roč. 65, č. 4, s. 542 – 555. ISSN 1335-6461

PERHÁCS, Z., PERHÁCSOVÁ, A., 2013. Právna úprava používania informačno-technických prostriedkov (2. časť). In: Justičná revue: časopis pre právnu prax, 2013, roč. 65, č. 5, s. 698 – 711. ISSN 1335-6461

SVÁK, J., 2006. Ochrana ľudských práv (z pohľadu judikatúry a doktríny štrasburských orgánov ochrany práva). II. rozšírené vydanie. Bratislava: Eurokódex, 2006, 1116 s. ISBN 80-88931-51-7

ŠIMOVČEK, I., 2017. Zákonné limity zabezpečovania informácií dôležitých pre trestné konanie. In: ZÁHORA, J. (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. Praha: Leges, 2017, s. 44 – 52. ISBN 978-80-7502-206-6

TITTLOVÁ, M., 2016. Kritické zhodnotenie trestnoprávnej úpravy odpočúvania a záznamu telekomunikačnej prevádzky. In: Justičná revue: časopis pre právnu prax, 2016, roč. 68, č. 6–7, s. 748 – 762. ISSN 1335-6461

ZÁHORA, J., 2018. Uplatňovanie zásady primeranosti a zdržanlivosti pri využívaní informačno-technických prostriedkov v trestnom konaní v Slovenskej republike. In: Časopis pro právní vědu a praxi, 2018, č. 1, s. 29 – 39. ISSN 1210-9126

Informačno-technické prostriedky – vybrané aplikačné problémy v praxi

Information-technical Tools – Selected Application Problems in Practice

Marek Kordík[1]

Abstrakt: *Uvedený príspevok sa zaoberá aktuálnymi aplikačnými problémami na úseku použitia informačno-technických prostriedkov. Súčasná aplikačná prax v spojení so stavom legislatívy a vedecko-technickým pokrokom prináša nové výzvy, s ktorými sa v každodennej praxi orgány činné v trestnom konaní stretávajú. Jeden zo súčasných vypuklých problémov je fakt, že sa stiera rozdiel medzi informačno-technickým prostriedkom a operatívno-pátracím prostriedkom. Práve na uvedené problémy poukazuje tento príspevok.*

Abstract: *This paper deals with current application problems in the area of using information- technical tools. Current application practice, coupled with legislation and scientific and technological progress, brings new challenges that law enforcement agencies encounter in their daily practice. One of the emerging problems is the fact that the difference between the information technical tools and the operative-search methods is blurred. This is the topic that the contribution points out.*

Kľúčové slová: *informačno-technický prostriedok, operatívno-pátrací prostriedok, vyhotovovanie obrazových, zvukových a obrazovo-zvukových záznamov, prostriedky nástrahovej techniky.*

Keywords: *interception, trap techniques, search and detecting techniques, recording.*

Informačno-technický prostriedok vs. operatívno-pátrací prostriedok

Informačno-technický prostriedok je definovaný *expressis verbis* výlučne v § 10 ods. 21 zákona č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov (ďalej len „Trestný poriadok) pre účely trestného stíhania ako *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* a v § 2 ods. 1 Zákona č. 166/2003 Z. z. o ochrane pred odpočúvaním v znení neskorších predpisov (ďalej len „Zákon o ochrane pred odpočúvaním") pre účely postupu mimo trestné stíhanie ako *elektrotechnické, rádiotechnické, 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.

Prvým problémom aplikačnej praxe je dlhodobý neúspech hľadania pevnej hranice, kedy je nevyhnutné postupovať pri použití informačno-technického prostriedku v zmysle ustanovení

[1] Mjr. JUDr. Marek Kordík, LL.M., PhD., Úrad kriminálnej polície Prezídia Policajného zboru, Račianska 45, 832 23 Bratislava, e-mail: marek.kordik@minv.sk.

Trestného poriadku a kedy ešte „postačuje" postup podľa Zákona o ochrane pred odpočúvaním postupom v tzv. „operatívnej rovine". Je potrebné zdôrazniť, že účel použitia informačno-technického prostriedku podľa § 36 zákona č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov o PZ[2] je v reálnej praxi veľmi podobný ak nie totožný s účelom stanoveným v Trestnom poriadku podľa § 114 až § 116 Trestného poriadku v spojení s § 199 Trestného poriadku, ktorý stanovuje povinnosť orgánov činných v trestnom konaní bezodkladne začať trestné stíhanie, ak existuje podozrenie zo spáchania trestného činu a postupovať pri získavaní informácii dôležitých pre trestné konanie ďalej v zmysle predpisu *lex specialis*, ktorým je v tomto prípade Trestný poriadok. Ďalší postup podľa Zákona o PZ v spojení so Zákonom o ochrane pred odpočúvaním, v takýchto prípadoch znamená nezákonný zásah do súkromia dotknutej osoby a rezultuje v nemožnosť využitia takejto informácie ako dôkazu v trestnom konaní, čo potvrdzuje dlhodobo aj súdna prax,[3] tento postup je navyše aj v rozpore so znením článku 8 ods. 2 Dohovoru o ochrane ľudských práv a základných slobôd publikovaného pod oznámením Federálneho ministerstva zahraničných vecí Českej a Slovenskej Federatívnej Republiky č. 209/1992 Zb. (ďalej len „Dohovor").[4]

Druhý problém aplikačnej praxe súvisí s najviac problematickým informačno-technickým prostriedkom vyhotovovania obrazových, obrazovo-zvukových a zvukových záznamov. Problém nastáva najmä v prípade posúdenia, či určité technické riešenie používané na odhaľovanie a dokumentovanie trestnej činnosti je informačno-technický prostriedok na vyhotovenie a uchovanie obrazu, zvuku, alebo ich kombinácie a je teda potrebné postupovať pri jeho použití len so súhlasom súdu, či už podľa Trestného poriadku alebo podľa Zákona o ochrane pred odpočúvaním, alebo je povinnosť sem zahrnúť aj operatívno-pátrací prostriedok, ktorý by mohol spadať napr. pod sledovanie osôb a veci alebo použitie prostriedkov nástrahovej techniky ako prostriedkov operatívno- pátracej činnosti, ktorý je pre operatívne účely upravený v § 38a a § 39 Zákona o PZ.

Pri interpretácii uvedených ustanovení, vzhľadom na neexistenciu súdnej praxe v tejto veci, je potrebné vychádzať z relevantných rozhodnutí k výkladu § 113 a § 114 Trsteného poriadku a v primeranej miere ich aplikovať.

Skutočnosť, že v praxi dochádza k prelínaniu informačno-technických prostriedkov s operatívno-pátracími prostriedkami konštatujú i súdy, ich vzájomný pomer sa pokúsil naznačiť Krajský súd v Trnave, keď konštatoval, že sledovanie osôb alebo vecí s použitím tohto informačno-technického prostriedku podľa § 113 ods. 4 Tr. por. a tiež i vyhotovovanie obrazových,

[2] Boj proti terorizmu, v boji proti legalizácii príjmov z trestnej činnosti a financovaniu terorizmu pri odhaľovaní trestnej činnosti a financovaniu terorizmu organizovanej v spojení s cudzinou a organizovanej trestnej činnosti a financovaniu terorizmu súvisiacej s nedovolenou výrobou, držaním a rozširovaním omamných a psychotropných látok, jedov, prekurzorov a jadrových materiálov, s falšovaním a pozmeňovaním peňazí, známok a cenných papierov, pri odhaľovaní iných zločinov, pri poskytovaní ochrany a pomoci ohrozenému svedkovi a chránenému svedkovi podľa osobitného predpisu, pri operatívnej ochrane legalizanta a agenta pri odhaľovaní daňových únikov a nezákonných finančných operácií, pri odhaľovaní úmyselných trestných činov podľa druhého a tretieho dielu ôsmej hlavy druhej časti zákona č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov (ďalej len Trestný zákon), za ktoré možno uložiť trest odňatia slobody s hornou hranicou najmenej dva roky, alebo iných úmyselných trestných činov, ktorých stíhanie upravuje medzinárodná zmluva, ktorou je Slovenská republika viazaná, a pri zisťovaní ich páchateľov a pátraní po nich.

[3] Uznesenie Ústavného súdu Slovenskej republiky (ďalej len „ÚS SR") I. ÚS 274/05-49, Nález ÚS SR PL. ÚS 10/2014, Uznesenie Najvyššieho súdu Slovenskej republiky Rozsudok (ďalej len NS SR) 2 Tdo 24/2013, Uznesenie NS SR 3 Tdo 4/2014 a ďalšie.

[4] V zmysle čl. 8 ods. 2 Dohovoru: 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.

zvukových alebo obrazovo-zvukových záznamov podľa § 114 Tr. por. predstavuje v samotnej podstate rovnaký zásah do základných práv a slobôd, najmä do oblasti práva na súkromie. Obe citované procesnoprávne ustanovenia stanovujú pre taký zásah, vykonaný v podobe vydania príkazu, formálnu podmienku vedenia trestného stíhania pre úmyselný trestný čin, ako i materiálnu podmienku spočívajúcu v dôvodnom predpoklade, že týmto sledovaním a vyhotovovaním záznamov majú byť a budú zistené skutočnosti významné pre trestné konanie. V oboch prípadoch zákon vyžaduje na takýto postup súdne povolenie v podobe príkazu vydaného sudcom pre prípravné konanie, pričom oba takéto príkazy možno vydať výlučne na návrh orgánov činných v trestnom konaní, a to za situácie, že v oboch prípadoch podania návrhov zákon vyžaduje identický spôsob ich odôvodnenia. Preto je skutočne vecou polície, ktorý z týchto inštitútov Trestného poriadku si vyberie na dosiahnutie legitímne sledovaného účelu a o vydanie ktorého príkazu aj požiada sudcu konajúceho v štádiu prípravného konania, nakoľko oboma spôsobmi je možné dosiahnuť sledovaný cieľ, ktorým je dokumentovanie páchania trestnej činnosti, odhalenie jej miesta a páchateľov.[5]

Z uvedeného Najvyšší súd ako dovolací súd, vyvodil, že postup podľa § 114 ods. 2 Tr. por. je špeciálnym vo vzťahu k postupu podľa § 113 Tr. por., pričom procesný postup podľa § 113 ods. 4 Tr. por. (sledovanie so súčasným použitím ITP) možno použiť len v prípade, ak nepôjde o trestné činy spadajúce do katalógu trestných činov vymenovaných v ustanovení § 114 ods. 1, ods. 2 Tr. por. a sledovanie nebude spojené so vstupom do obydlia. Inými slovami, ak je potrebné vykonať sledovanie spojené s použitím ITP (§ 113 ods. 4 Tr. por.) so vstupom do obydlia s tým, že pôjde o niektorý z trestných činov taxatívne uvedených v ustanovení § 114 ods. 1, ods. 2 Tr. por. musí sa postupovať podľa špeciálneho ustanovenia a to podľa ustanovenia § 114 Tr. por.[6]

Najvyšší súd ďalej zdôraznil, že je pochopiteľné, že v rámci postupu podľa § 114 Tr. por., napríklad pri použití kamery na zaznamenávanie obrazu i zvuku dochádza k sledovaniu objektov a osôb v širšom zmysle, čo je logickým dôsledkom činnosti označeného technického zariadenia. Použitie ITP na vyhotovovanie obrazových záznamov v sebe vždy zahŕňa i sledovanie. Samotný charakter toho ktorého prostriedku dopredu predurčuje jeho aplikáciu. Postup podľa § 113 Tr. por. možno označiť ako tzv. „in move" a teda sledovanie v pohybe, naproti tomu postup podľa § 114 Tr. por. je určený prioritne na stacionárne „sledovanie" ako tzv. „steady" procesný prostriedok.[7] Uvedené rozlíšenie, ktoré použil Najvyšší súd nie je v praxi veľmi použiteľné a navyše je aj technickými možnosťami prekonané.[8]

M. Deset uvádza, že utajovaný spôsob realizácie sledovania osôb a vecí smeruje k získaniu neskreslených, záujmami dotknutých subjektov neovplyvnených informácií a poznatkov o osobách a veciach, čo je zásadný element pre ich využiteľnosť v trestnom konaní a pre význam (dôkaznú hodnotu), ktorú v trestnom konaní môžu nadobudnúť. Je zrejmé, že ak by dotknuté osoby mali v konkrétnom čase a mieste vedomosť o tom, že ich činnosť, aktivity, operácie s vecami, ich stav a povaha boli takýmto spôsobom sledované, svoju činnosť by modifikovali tak, aby sa vyhli prípadnému trestnému postihu, aby sa tieto aktivity a operácie javili ako súladné (aprobované) s právom (napr. na základe vytvorenej krycej legendy) tak, aby vyvracali podozrenia odôvodňujúce použitie inštitútu sledovania osôb a vecí voči nim. Práve utajený spôsob realizácie sledovania osôb a vecí smeruje k dosiahnutiu účelu použitia tohto prostriedku, ktorý by bol vedomosťou dotknutých osôb o tomto použití zrejme zmarený. Prirodzene, že nielen spôsob realizácie ale aj samotná povaha sledovania osôb a vecí ako prostriedku operatívno-pátracej činnos-

[5] Uznesenie KS TT 5 To/68/2014 zo dňa 15. 1. 2015.
[6] Uznesenie NS SR 6 Tdo/31/2016 zo dňa 14. 9. 2016.
[7] Uznesenie NS SR 6 Tdo/31/2016 zo dňa 14. 9. 2016.
[8] Uznesenie NS SR 6 Tdo/31/2016 zo dňa 14. 9. 2016.

ti naznačujú, že jeho výkonom sa spravidla veľmi intenzívne zasahuje do oblasti ľudských práv a základných slobôd garantovaných nielen na ústavnej úrovni, ale aj vo viacerých dokumentoch európskej či medzinárodnej povahy. Okrem celého radu osobnostných práv je možné spomenúť tiež právo na ochranu súkromia a rodinného života, právo na zachovávanie tajomstva prepravovaných správ, právo na ochranu prejavov súkromnej povahy a pod. So zreteľom na korelácie medzi záujmom štátu na boji proti najzávažnejším formám kriminality a ľudskými právami jednotlivcov zohráva trestno-procesná úprava (podmienky a možnosti využitia inštitútu sledovania osôb a vecí v konkrétnych prípadoch, jej povaha a garancie, ktoré sa pomocou nej vytvárajú) veľmi dôležitú úlohu.[9]

Samozrejme, že sledovanie osôb a vecí, je svojou povahou iným prostriedkom ako vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov či odpočúvanie a záznam telekomunikačnej prevádzky, pretože ide prostriedok operatívno-pátracej činnosti, ale keďže aj pri tomto prostriedku sa môžu použiť informačno-technické prostriedky, ktorými sa zasahuje do súkromia, právna úprava sledovania, ktorá ich použitie umožňuje, najmä garancií práva na súkromie, by mala byť porovnateľná s právnou úpravou, ktorá upravuje tieto informačno-technické prostriedky.[10]

Samozrejme, že sledovanie osôb a vecí, podobne ako použitie agenta, je svojou povahou iným prostriedkom ako vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov či odpočúvanie a záznam telekomunikačnej prevádzky, pretože ide prostriedok operatívno-pátracej činnosti, ale keďže aj pri tomto prostriedku sa môžu použiť informačno-technické prostriedky, ktorými sa zasahuje do súkromia, právna úprava sledovania, ktorá ich použitie umožňuje, najmä garancií práva na súkromie, by mala byť porovnateľná s právnou úpravou, ktorá upravuje tieto informačno-technické prostriedky. Okruh trestných činov, pri ktorých sa takéto sledovanie umožňuje, by preto mal byť stanovený oveľa užšie, napríklad tak, ako je tomu pri vyhotovovaní obrazových, zvukových alebo obrazovo-zvukových záznamov.[11]

V zmysle všeobecného ustanovenia § 69 ods. 2 Zákona o PZ o získavaní informácii je možné využívať technické zariadenia a prostriedky na monitorovanie a záznam služobného úkonu, pokiaľ sa tento služobný úkon vykonáva na mieste verejne prístupnom, t. j. dokumentácie, ktorá má slúžiť v operatívnom procese na vylúčenie alebo potvrdenie určitej informácie. Uvedené ustanovenie je však problémové v dvoch smeroch. Jednak expressis verbis nerieši, či sa služobným úkonom rozumie aj použitie operatívno-pátracích prostriedkov, ako je sledovanie osôb a veci a taktiež nedáva odpoveď na otázku, či pod túto úpravu spadá aj situácia, kedy sa služobný

[9] Deset, M. Vybrané aspekty sledovania osôb a veci v trestnom konaní; In: Zborník príspevkov z medzinárodnej vedeckej konferencie organizovanej dňa 18. 10. 2017 Katedrou trestného práva a kriminológie Právnickej fakulty Trnavskej univerzity v Trnave s názvom „Informačno-technické prostriedky a prostriedky operatívno-pátracej činnosti získavania informácií dôležitých pre trestné konanie“, Leges, Praha, 2017, ISBN 978-80-7502-260-8, s. 356.

[10] Deset, M. Vybrané aspekty sledovania osôb a veci v trestnom konaní; In: Zborník príspevkov z medzinárodnej vedeckej konferencie organizovanej dňa 18. 10. 2017 Katedrou trestného práva a kriminológie Právnickej fakulty Trnavskej univerzity v Trnave s názvom „Informačno-technické prostriedky a prostriedky operatívno-pátracej činnosti získavania informácií dôležitých pre trestné konanie“, Leges, Praha, 2017, ISBN 978-80-7502-260-8, s. 360.

[11] Deset, M. Vybrané aspekty sledovania osôb a veci v trestnom konaní; In: Zborník príspevkov z medzinárodnej vedeckej konferencie organizovanej dňa 18. 10. 2017 Katedrou trestného práva a kriminológie Právnickej fakulty Trnavskej univerzity v Trnave s názvom „Informačno-technické prostriedky a prostriedky operatívno-pátracej činnosti získavania informácií dôležitých pre trestné konanie“, Leges, Praha, 2017, ISBN 978-80-7502-260-8, s. 360–361.

úkon, ktorý sa síce vykonáva vo verejnom priestore monitoruje a uchováva, avšak *utajovaným spôsobom.*[12]

Používanie *Vyhotovovanie obrazových, zvukových a obrazovo-zvukových záznamov* ako informačno-technického prostriedku v rámci činnosti PZ je upravené výlučne v § 36 Zákona o PZ a má úplne odlišné podmienky od úpravy § 69 ods. 2 Zákona o PZ a § 38 a 39 Zákona o PZ, pričom pri jeho používaní je ďalej potrebné postupovať v režime Zákona o ochrane pred odpočúvaním. V rámci odbornej diskusie existujú názory, že Ustanovenie § 69 ods. 2 Zákona o PZ nie je možné vykladať ako úpravu informačno-technického prostriedku vyhotovovania obrazových, zvukových a obrazovo-zvukových záznamov. *Ide len o všeobecnú úpravu spracúvania získaných informácií Policajným zborom z verejne prístupných priestranstiev a časti a predstavuje právne zakotvenie činností, ktoré Policajný zbor nevyhnutne vykonáva. Súčasne ide o ustanovenie predstavujúce presah do ochrany osobných údajov podľa zákona č. 18/2018 Z. z. o ochrane osobných údajov, ktorá nadväzuje na ods. 1, cit. paragrafu*[13] Toto ustanovenie nijakým spôsobom neupravuje, či hore uvedený postup ma charakter informačno-technického prostriedku, alebo operatívno-pátracieho prostriedku.[14]

Uvedené ustanovenie § 69 ods. 2 Zákona o PZ rozoznáva zaznamenávanie a vyhotovovanie 2 druhov záznamov:

1. Zvukové, obrazové, alebo iné záznamy z miest verejne prístupných a
2. Zvukové, obrazové alebo iné záznamy o priebehu služobnej činnosti, alebo služobného zákroku.

Zaznamenávanie obrazu, zvuku, ich kombinácie, alebo inej formy zaznamenávania pri používaní operatívno-pátracieho prostriedku je možné zaraďovať pod bod 1 a v tomto zmysle ho aj vykladať. Ide len o použitie záznamovej techniky na monitorovanie a zaznamenanie priebehu služobného úkonu.

Záver

Z naznačených rozhodnutí vyplýva že dôkazný prostriedok sledovanie osôb a vecí podľa § 113 Trestného poriadku je obsahovo podobným a v niektorých prípadoch dokonca identickým dôkazným prostriedkom ako vyhotovovanie obrazových záznamov. Vzhľadom na množstvo výkladových nejasností, ktoré sú spojené s aplikáciou týchto dvoch dôkazných prostriedkov bude de lege ferenda nevyhnutné, aby zákonodarca prijal takú právnu úpravu, ktorá odstráni akékoľvek pochybnosti pri ich používaní.[15] Z tohto pohľadu by sa ako najvhodnejšie riešenie javilo včlenenie ustanovenia § 113 Trestného poriadku do ustanovenia § 114 Trestného poriadku s tým, že tak sledovanie osôb a veci ako aj sledovanie prostredníctvom vyhotovovania obrazo-

[12] Odôvodnenosť tejto interpretácie je analogická úprava § 113 ods. 11 Trestného poriadku, avšak rovnaký problém pretrváva vo vzťahu k otázke, aký je pomer § 113 ods. 4 prvá veta Trestného poriadku a § 113 ods. 11 Trestného poriadku, pričom odborná diskusia na túto tému chýba.

[13] Dôvodová správa k novele č. 490/2001 Z. z. www.rokovania.sk/File.aspx/Index/Mater-Dokum-26293., dostupné dňa 1. 9. 2018.

[14] Súčasne je potrebné zdôrazniť, že toto ustanovenie s použitím § 69 ods. 1 Zákona o PZ, umožňuje interpretáciu, že je možné získať aj iné informácie z verejne dostupných priestranstiev (odhodené, opustené, voľne dostupné), ktoré samé osebe netvoria súčasť postupu sledovania osôb a veci, avšak svojou povahou ide o „náhodne získanú vec resp. informáciu pri plnení služobnej úlohy" (napr. odfotený odhodený bankový výpis, výpis hovorov). Podmienkou ďalšieho použitia takejto veci resp. získanej informácie ako dôkazu v trestnom konaní je skutočnosť, že bola získaná vyhotovením záznamu z verejného priestranstva.

[15] Šamko, P. Sledovanie osôb a vecí – aplikačné problémy, Právne listy, dostupné na: http://www.pravnelisty.sk/clanky/a553-sledovanie-osob-a-veci-aplikacne-problemy.; dňa 4. 4. 2019.

vých záznamov by malo upravovať jedno ustanovenie s rovnakými obsahovými podmienkami pre jeho použitie. Bohužiaľ ani jedno z rozhodnutí neodpovedalo na otázku, ako je potrebné vykladať ustanovenie § 113 ods. 11 Trestného poriadku k ustanoveniu § 113 ods. 4, resp. § 114 Trestného poriadku pričom táto argumentácia by bola primeranej miere použiteľná aj pre upresnenie výkladu a vzťahu § 38 a § 39 s ustanovením § 69 ods. 2 Zákona o PZ.

Uvedený príspevok nemal ambíciu dať odpovede na aplikačné problémy používania informačno-technických prostriedkov a operatívno-pátracích prostriedkov a taktiež nedáva systémové návrhy riešení, ktorý by sa mali uplatniť. Úlohou príspevku bolo poukázať na súčasné aplikačné problémy vyplývajúce z toho, že použitie informačno-operatívnych prostriedkov nie je formalizované do takej miery ako použitie informačno-technických prostriedkov. Jednotlivé odvetvové zákony poskytujú len rámcové definície jednotlivých podmienok používania, dokumentovania používania a kontroly používania informačno-operatívnych prostriedkov v rámci spravodajskej činnosti je ponechaná na rozhodnutie vedúcich predstaviteľov spravodajských služieb a bezpečnostných zborov, ktorí túto problematiku upravia v interných predpisoch. Podrobnejšiu úpravu ustanovuje iba Trestný poriadok.[16] Súčasne je potrebné zdôrazniť, že určitý vklad neobsahujú ani komentáre použiteľné pre túto oblasť.[17]

Príspevok sa snažil poukázať na skutočnosť, že pravdepodobne dospel čas na zásadnú zmenu úpravy Zákona o PZ, ktorá by mala pokrývať nasledovné okruhy:

1. Definovať operatívno-pátrací prostriedok, jeho jednotlivé druhy a jeho pomer/resp. vzťah k informačno-technickému prostriedku podľa Zákona o ochrane pred odpočúvaním.
2. Definovať oprávnenia policajta pri používaní operatívno-pátracích prostriedkov v operatívnej rovine.
3. Definovať jasné hranice operatívneho používania informačno-technických prostriedkov
4. Nahradiť slovné spojenie vyhotovovanie obrazových, zvukových, alebo zvukovo-obrazových záznamov iným termínom, ktorý by neevokoval, že sa jedná o informačno-technický prostriedok, na použitie ktorého sa vzťahuje Zákon o ochrane pred odpočúvaním.

Potreba uvedených zmien z pohľadu činností kriminálnej polície spočíva najmä v odstránení pochybností a zvýšeniu právnej istoty policajtov, ktorí vykonávajú uvedené činnosti a zasahujú tým do práv a slobôd dotknutých osôb.

Literatúra

Deset, M. Vybrané aspekty sledovania osôb a veci v trestnom konaní; In: Zborník príspevkov z medzinárodnej vedeckej konferencie organizovanej dňa 18. 10. 2017, Leges, Praha, 2017, ISBN 978-80-7502-260-8,

Dôvodová správa k novele č. 490/2001 Z. z. www.rokovania.sk/File.aspx/Index/Mater-Dokum-26293., dostupné dňa 1. 9. 2018,

[16] Aláč, M. Získavanie informácií na spravodajské účely a na účely trestného konania. Bratislava: C. H. Beck. 2015. s. 119. In: Hruška, R., Žuffa, M. Niekoľko poznámok k inštitútom operatívno-pátracej činnosti; Zborník príspevkov z medzinárodnej vedeckej konferencie organizovanej dňa 18. 10. 2017 Katedrou trestného práva a kriminológie Právnickej fakulty Trnavskej univerzity v Trnave s názvom „Informačno-technické prostriedky a prostriedky operatívno-pátracej činnosti získavania informácií dôležitých pre trestné konanie", Leges, Praha, 2017, ISBN 978-80-7502-260-8, s. 348.

[17] Porovnaj Napr. Tittlová, M. Zákon o ochrane súkromia pre neoprávneným použitím informačno-.technických prostriedkov (zákon o ochrane pred odpočúvaním) – Komentár, Wolters Kluwer, 2017, ISBN 978-80-8168-717-4, Bratislava, s. 10 – 34; alebo Tittlová, M., Medelský, J. Zákon o Policajnom zbore. Komentár, Wolters Kluwer, Bratislava, ISBN 978-80-8168-577-4, Bratislava, komentár k § 69.

Hruška, R., Žuffa, M. Niekoľko poznámok k inštitútom operatívno-pátracej činnosti; Zborník príspevkov z medzinárodnej vedeckej konferencie organizovanej dňa 18. 10. 2017, Leges, Praha, 2017, ISBN 978-80-7502-260-8,

Nález ÚS SR PL. ÚS 10/2014,

Rozsudok NS SR 2 Tdo 24/2013,

Šamko, P. Sledovanie osôb a vecí – aplikačné problémy, Právne listy, dostupné na: http://www.pravnelisty.sk/clanky/a553-sledovanie-osob-a-veci-aplikacne-problemy.; dňa 4. 4. 2019,

Tittlová, M., Zákon o ochrane súkromia pre neoprávneným použitím informačno-technických prostriedkov (zákon o ochrane pred odpočúvaním) – Komentár, Wolters Kluwer, 2017, ISBN 978-80-8168-717-4, Bratislava,

Tittlová, M., Medelský, J. Zákon Policajnom zbore – Komentár, Wolters Kluwer, Bratislava, ISBN 978-80-8168-577-4, Bratislava, komentár k § 69,

Uznesenie KS TT 5 To/68/2014 zo dňa 15. 1. 2015,

Uznesenie NS SR 3 Tdo 4/2014,

Uznesenie NS SR 6 Tdo/31/2016 zo dňa 14. 9. 2019,

Uznesenie I. ÚS 274/05-49.

K praktickým poznatkom vyplývajúcim zo Zákona o ochrane pred odpočúvaním a Trestného poriadku[1]

Practical Knowledge Related to the Law about Protection from Interception and Code of Criminal Procedure

Ján Šanta[2]

Abstrakt: *V predmetnom príspevku sa jeho autor po úvodných teoretických východiskách k odpočúvaniu a záznamu telekomunikačnej prevádzky zaoberá spoločnými a rozdielnymi znakmi tohto procesného postupu podľa § 115 Trestného poriadku a podľa zákona č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov. Dôraz pritom autor kladie na pojem „súčasné" vedenie trestných konaní, pričom dochádza k záveru a nejednotnej praxi v tomto smere.*

Abstract: *In the article, the author is initially focusing on theoretical approaches to interception and recording of telecommunication services and then elaborates on differences and similarities of this procedure according to § 115 of Code of Criminal Procedure and according to law no. 166/2003 Col. concerning the protection of privacy from unauthorised use of information – technical tools. The main emphasis is put on "current" conducting of criminal process, and he comes to the conclusion that the practices in this area differ from each other.*

Kľúčové slová: *telekomunikačná prevádzka, odpočúvanie, záznam, súčasne, oznámenie údajov, ochrana pred odpočúvaním*

Keywords: *telecommunication service, interception, record, current, announcement of information, protection from interception*

Úvod

Ústava SR v čl. 22 ods. 2 zaručuje tajomstvo správ podávaných telefónom, telegrafom alebo iným podobným zariadením. Ochrana sa týka správ súkromného aj verejného charakteru. Ochrana súkromia zahŕňa predmet telekomunikačného tajomstva, a to obsah prenášaných informácií, údaje komunikujúcich strán, osobné údaje fyzickej osoby, prevádzkové údaje a lokalizačné údaje. Výnimkou sú prípady, kedy je podľa zákona, v tomto prípade Trestného poriadku, možné použitie informačno-technických prostriedkov – odpočúvania a záznamu telekomunikačnej prevádzky.

Odpočúvanie a záznam telekomunikačnej prevádzky (§ 115 a 116 TP) je trestno-procesný inštitút, ktorý umožňuje prenos obsahu komunikácie a prepravovaných údajov k určitej účastníckej adrese do zariadení oprávnených subjektov.

Predmetom odpočúvania a záznamu telekomunikačnej prevádzky je utajeným spôsobom odpočúvať a zaznamenávať telefónne hovory medzi účastníkmi telekomunikačnej prevádzky prostredníctvom elektronickej komunikačnej siete a túto komunikáciu archivovať s cieľom zis-

[1] Príspevok je podporený Agentúrou na podporu výskumu a vývoja na základe Zmluvy č. APVV-15-0740 Návody a nástroje na efektívnu elimináciu protiprávnych konaní v spojení s možnou insolvenciou/Guidelines and tools for effective elimination of unlawful acts in relation with potential insolvency.

[2] JUDr. Ján Šanta PhD., LL.M., MBA, prokurátor Úradu špeciálnej prokuratúry GP SR, Akadémia Policajného zboru v Bratislave, e-mail: jan.santa@genpro.gov.sk.

tenia obsahu telekomunikačnej prevádzky prebiehajúcej v konkrétnej forme a v aktuálnom čase, resp. v budúcnosti.

Odpočúvaním sa rozumie utajené a účelové vnímanie komunikácie medzi účastníkmi telekomunikačnej prevádzky, ktoré je sprostredkované tretej osobe.

Záznamom sa rozumie najmä proces, pri ktorom sa komunikácia medzi účastníkmi prevádzky zachycuje na príslušný nosič, ktorý umožní archivovanie a reprodukovanie obsahu komunikácie.

Pri odpočúvaní a zaznamenávaní telekomunikačnej prevádzky sa môže použiť len taký informačno-technický prostriedok, ktorým sa okamžite identifikuje koncové telekomunikačné zariadenie použité na odpočúvanie a zaznamenávanie telekomunikačnej služby, a ktorý neumožní vymazanie údajov identifikujúcich toto zariadenie ani vymazanie času odpočúvania a zaznamenávania telekomunikačnej služby.[3]

Telekomunikačnou prevádzkou je prenos uskutočňovaný prostredníctvom telekomunikačného zariadenia. Telekomunikačné zariadenie je technické zariadenie na vysielanie, prenos, smerovanie, príjem, prepojenie alebo spracovanie signálov a informácií vo forme obrazu, zvuku alebo dát prostredníctvom vedení, rádiovými, optickými alebo inými elektromagnetickými prostriedkami, ako aj pridružené prostriedky (§ 3 ods. 1 zákona č. 610/2003 Z. z. o elektrotechnických komunikáciách). Pôjde predovšetkým o prenos signálu telefónom, telefaxom, mobilným telefónom vrátane posielania SMS, vysielačky, pageru alebo elektronickou poštou (e-mailom).[4]

Dôsledná ochrana súkromia jednotlivca pri odpočúvaní vyžaduje existenciu primeraných a účinných záruk, ktoré sa skladajú najmä zo zodpovedajúcich právnych predpisov a účinnej kontroly ich dodržiavania. S prihliadnutím na utajený charakter odpočúvania, o ktorom dotknutá (odpočúvaná) osoba nemá vedomosť a nemôže tak uplatňovať svoje práva, vystupuje do popredia nevyhnutnosť určenia hraníc zásahu do týchto práv tak, aby odpočúvanie bolo v súlade so zákonom Z týchto dôvodov je nevyhnutná taká právna úprava odpočúvania, ktorá zodpovedá požiadavkám vyplývajúcim predovšetkým z medzinárodných zmlúv o ľudských právach a základných slobodách, ktorými je Slovenská republika viazaná, a zákona č. 460/1992 Zb. Ústava Slovenskej republiky v znení neskorších predpisov. Uvedené vyžaduje pri odpočúvaní dôsledné skúmanie podmienok zásahu, a to najmä do práva na súkromie. Pri tomto postupe verejná moc musí rešpektovať pravidlá fungovania právneho štátu. Zároveň pri odpočúvaní sa musí postupovať tak, aby sa nadmerne neobmedzila právna ochrana jednotlivca. V tejto súvislosti možno zvýrazniť, že ak právna úprava má pôsobiť preventívne, musí byť dostatočne zrozumiteľná, jednoznačná a adresná, aby nevznikali pochybnosti o právach a povinnostiach účastníkov dotknutých vzťahov všeobecne, preto je potrebné precizovať úpravu v predmetnej oblasti, a to nielen v záujme právnej istoty, ale najmä reálnej ochrany individuálnych práv jednotlivca.[5]

Podstatne menej ako v rámci trestného konania sa analyzuje a hodnotí právna úprava podmienok použitia inštitútu vyhotovovania obrazových, zvukových a obrazovo-zvukových záznamov mimo rámca trestného konania, teda v neprocesnej rovine (a prelínanie týchto postupov). Ide o použitie na základe ustanovení osobitných predpisov, vrátane najmä ustanovení zákona o ochrane pred odpočúvaním.

Podstata tohto inštitútu, bez ohľadu na rovinu použitia a bez ohľadu na ich právny základ, však ostáva stále rovnaká. Tak v rovine procesnej, ako aj v rovine neprocesnej ide o prostried-

[3] Čentéš, J. a kol.: Trestné právo procesné. Všeobecná časť. Šamorín: Heuréka, 2016, s. 306.

[4] Ivor, I. a kol.: Trestné právo procesné. Druhé, doplnené a prepracované vydanie. Bratislava: Iura Edition, 2010, s. 405.

[5] Čentéš, J.: Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. Bratislava: C. H. Beck, 2013, s. 1.

ky, ktoré rovnako intenzívne zasahujú so oblasti ľudských práv (pritom v rovine neprocesnej možno hovoriť ešte o intenzívnejšom zásahu, keďže sa pohybujeme mimo rámca trestného konania, mimo akýchkoľvek trestných šetrení). V oboch prípadoch ide o prostriedky, ktoré majú rovnako povahu inštitútov moderných, ofenzívnych a spravodajsky (teda utajene) využívaných, čo je priamo zákonný znak týchto prostriedkov. Aj napriek tomu sú právne úpravy ich použitia v rovine procesnej a v rovine neprocesnej v niektorých oblastiach odlišné. Zaujímavosťou je, že v rovine neprocesnej by sme predpokladali, že právna úprava možností ich použitia je prísnejšia a striktnejšia, keďže sa stále pohybujeme mimo trestného konania, mimo konkrétnych trestnoprocesných šetrení. A prirodzene, takto by sme predpokladali, že v rovine procesnej budú možnosti ich využitia o niečo širšie, keďže spravidla je už podané trestné oznámenie, začaté trestné stíhanie a prípadne aj vznesené obvinenie voči konkrétnej osobe. Aj napriek tomuto predpokladu v niektorých aspektoch tomu tak nie je, resp. je tomu presne naopak.[6]

K niektorým právnym východiskám odpočúvania a záznamu telekomunikačnej prevádzky

Podľa § 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**. 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.

Spomínanými informačno-technickými prostriedkami sa v zmysle § 10 ods. 21 Trestného poriadku 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 dovolávať povinnosti mlčanlivosti podľa osobitných zákonov.

Samotný procesný inštitút odpočúvania a záznamu telekomunikačnej prevádzky je upravený v § 115 Trestného poriadku. Z jednotlivých jeho odsekov relevantnými v nadväznosti na tento príspevok sú najmä jeho odseky 1, 2, 5, 11 a predovšetkým § 115 ods. 7 Trestného poriadku, podľa ktorých 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 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 spôso-

[6] Záhora, J. a kol.: Obrazové a zvukové záznamy v trestnom konaní. Bratislava: Wolters Kluwer, 2018, s. 69 – 77.

bom podstatne sťažené. 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 zničiť; to neplatí, ak ide o informácie, ktoré sa vzťahujú na vec, v ktorej advokát nezastupuje obvineného ako obhajca. 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 obydlia, 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. V trestnom konaní pre iný úmyselný trestný čin, ako je uvedený v odseku 1, môže vydať príkaz na odpočúvanie a záznam telekomunikačnej prevádzky predseda senátu, pred začatím trestného stíhania alebo v prípravnom konaní sudca pre prípravné konanie na návrh prokurátora iba so súhlasom užívateľa odpočúvaného alebo zaznamenávaného telekomunikačného zariadenia.

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.

Ustanovenia odsekov 1 až 10 sa rovnako vzťahujú na údaje, ktoré sú v reálnom čase prenášané prostredníctvom počítačového systému.

Nakoniec východiskovou právnou úpravou pre objasnenie ďalej uvedených aplikačných problémov sú § 2 ods. 1, 7, § 3 ods. 1, 2, § 4 ods. 1 a § 7 ods. 2 zákona č. 166/2003 Z. z. v platnom znení o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním).

Podľa týchto ustanovení informačno-technickými prostriedkami na účely tohto zákona sú najmä elektrotechnické, rádiotechnické, fototechnické, optické, mechanické, chemické a iné prostriedky a zariadenia alebo ich súbory používané utajeným spôsobom na vyhľadávanie, otváranie, skúmanie a vyhodnocovanie poštových zásielok a iných dopravovaných zásielok, získavanie obsahu správ prenášaných prostredníctvom elektronických komunikačných sietí vrátane odpočúvania telefónnej komunikácie, vyhotovovanie obrazových, zvukových, obrazovo-zvukových alebo iných záznamov.

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; informačno-technické prostriedky možno v pôsobnosti Slovenskej informačnej služby a Vojenského spravodajstva použiť aj mimo územia Slovenskej republiky v rozsahu úloh podľa osobitných predpisov. 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. Údaje získané informačno-technickými prostriedkami možno použiť výlučne na dosiahnutie účelu pri plnení úloh štátu, ktoré spĺňajú podmienky podľa odseku 1. Informačno-technické prostriedky možno použiť iba na základe predchádzajúceho písomného súhlasu zákonného sudcu (ďalej len „súhlas") len na nevyhnutný čas, najdlhšie však na šesť 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 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.

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.

Aplikačná prax – poznatky, problémy, riešenia

V aplikačnej praxi orgánov činných v trestnom konaní a súdov sa vyskytli viaceré aplikačné problémy súvisiace s danou problematikou, z ktorých boli viaceré vyriešené, niektoré z nich však zostávajú otvorené. Jedným z aktuálnych nevyriešených aplikačných problémov je aplikácia citovaného **ustanovenia § 115 ods. 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, teda o zločine, korupcii, trestných činoch extrémizmu, trestnom čine zneužívania právomoci verejného činiteľa, trestnom čine legalizácie príjmu z trestnej činnosti alebo pre úmyselný trestný čin, o ktorom na konanie zaväzuje medzinárodná zmluva.

Obdobná procesná situácia vzniká v súvislosti s **§ 114 ods. 7 Trestného poriadku, podľa ktorého 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 príjmu z trestnej činnosti alebo pre iný úmyselný trestný čin, o ktorom na konanie zaväzuje medzinárodná zmluva.

Na tomto mieste je potrebné zdôrazniť, že Trestný poriadok nepoužíva pojem „trestné stíhanie“, ako vyššiu fázu postupu podľa Trestného poriadku, ale pojem „trestné konanie“. Podľa § 10 ods. 15 Trestného poriadku trestné konanie 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 alebo právoplatnosti rozhodnutia orgánu činného v trestnom konaní vo veci samej.

Rôznosť právnych názorov teda vyvoláva pojem „súčasné“ vedenie trestného konania v dvoch, či viacerých veciach pre zákonom vymedzené, citované, trestné činy, na ktorom sa doposiaľ nezjednotilo ani trestnoprávne kolégium Najvyššieho súdu SR v rámci opakovaného hlasovania. Z uvedeného dôvodu aj v rámci rozhodovacej činnosti Najvyššieho súdu SR existujú úplne protikladné rozhodnutia, ktoré viedli priam k absurdnej právnej situácii tiež v konkrétnej trestnej veci dozorovanej autorom tohto príspevku.

Najvyšší súd SR vo svojom uznesení **1 To 8/2014 z 29. 10. 2014** priamo poukazuje na rozpornosť rozhodovania NS SR a uvádza, že v rozsudku NS SR sp. zn. **2 To 5/2011 zo 7. 2. 2012** je zmieňované prvostupňové súdne rozhodnutie, v zmysle ktorého **nebolo možné** ako dôkaz

v tomto konaní použiť prepisy zvukových záznamov z inej trestnej veci a takéto prepisy mohli predstavovať len kriminálnu informáciu pre orgány činné v trestnom konaní.

Konkrétne Najvyšší súd SR v uvádzanom rozsudku sp. zn. 2 To 5/2011 uviedol, že pôvodné príkazy sudcu pre prípravné konanie Špecializovaného trestného súdu na odpočúvanie a záznam telekomunikačnej prevádzky (§ 115 ods. 2 Trestného poriadku) a na vyhotovenie obrazovo-zvukových záznamov (§ 114 ods. 2 Trestného poriadku) boli vydané 8. júna 2007 vo veci trestného stíhania začatého podľa § 199 ods. 1 Trestného poriadku pre podozrenie z korupcie prokurátora Okresnej prokuratúry P. B. pri výkone jeho funkcie uznesením zo 4. júna 2007. Takto boli zabezpečené dôkazné informácie vo vzťahu ku skutkom v bodoch 1a/, 1b/ a 2/ výroku napadnutého rozsudku (vo vzťahu ku skutkom 1a/ a b/ sa začalo trestné stíhanie uznesením z 28. augusta 2007, a vo vzťahu ku skutku v bode 2/ uznesením z 2. októbra 2007. Prvé z vyššie uvedených troch trestných stíhaní, začaté 4. júna 2007 bolo zastavené 21. augusta 2008. Ďalší príkaz na odpočúvanie, ako aj príkaz na vyhotovenie obrazovo-zvukových záznamov bol vydaný sudcom pre prípravné konanie Špecializovaného trestného súdu 27. septembra 2009, a to vo veci trestného stíhania pre skutky v bode 1a/ a 1b/, ktoré sa začalo uznesením z 28. augusta 2007. Takto bol zabezpečený záznam zo 17. októbra 2007 (skutok v bode 3/ výroku o vine napadnutého rozsudku). Trestné stíhanie pre skutok v bode 3/ sa potom začalo uznesením z 24. októbra 2007, následne boli na základe už uvedeného príkazu z 27. septembra 2007 zabezpečené záznamy z 26. a 29. októbra 2007 a zo 6. novembra 2007 (ku skutku v bode3/).

Obvinenie bolo potom pre všetky skutky dotknuté napadnutým rozsudkom vznesené 11. marca 2009 (vrátane skutku, ktorého sa týka oslobodzujúca časť výroku napadnutého rozsudku).

Okrem situácie po 28. auguste 2007, týkajúcej sa časti záznamov ku skutku v bodoch 1a/ a 1b/ a záznamov ku skutku v bode 3/ výroku o vine napadnutého rozsudku (skutky v bode 1a/ a 3/ sú čiastkovými útokmi toho istého pokračovacieho trestného činu, resp. by boli, ak by u skutku v bode 3/ išlo o trestný čin), neboli splnené podmienky pre použitie zabezpečených informácií ako dôkazu, keďže išlo o záznamy získané podľa § 114 Trestného poriadku v inej trestnej veci, ako je tá, v ktorej boli dotknuté záznamy na základe súdneho príkazu vyhotovené, pričom neboli splnené podmienky podľa § 114 ods. 7 Trestného poriadku. K tomu je ešte potrebné uviesť, že vzhľadom ku kritériám § 122 ods. 10 Trestného zákona, a to jednak spôsobu spáchania a jednak času spáchania činov (skutkov) je vylúčené, aby u skutkov podľa uznesenia o začatí trestného stíhania zo 4. júna 2006, skutku uvedeného v oslobodzujúcej časti výroku rozsudku (trestné stíhanie začaté uznesením zo 7. septembra 2007) a skutku v bode 2/ odsudzujúcej časti výroku rozsudku išlo o čiastkové útoky toho istého pokračovacieho trestného činu (teda ani keby bolo dokázané spáchanie týchto činov obžalovaným ako trestných činov).

Čo sa týka požiadavky súčasného vedenia trestného konania v zmysle § 114 ods. 7 a § 115 ods. 7 Trestného poriadku, súd prvého stupňa ju v odôvodnení napadnutého rozsudku interpretuje, podľa tohto právneho názoru NS SR, nesprávne.

Odôvodnenie rozsudku uvádza, že slovo „súčasne", uvedené v dotknutých ustanoveniach je potrebné správne vzťahovať k okamihu použitia výsledku týchto procesných inštitútov a nie k okamihu k ich vykonávania.

V tejto otázke sa však súd prvého stupňa, podľa NS SR, mýli. 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.

Zároveň platí, že podľa takéhoto výkladu by informácie získané na základe príslušných príkazov z 8. júna 2007, vydaných v pôvodnom konaní, nemohli byť v súdnom konaní v prejednávanej veci použité, nakoľko toto konanie bolo zastavené 21. augusta 2008 (čo aj odôvodnenie rozsudku konštatuje a tým fakticky neguje svoj skôr uvedený výklad dotknutých ustanovení).

V konečnom dôsledku súd prvého stupňa slovo „súčasne" vykladá ako súčasné vedenie trestného konania (ako konania podľa Trestného poriadku), teda nie konania občiansko-právneho, správneho alebo iného.

K tomu NS SR ďalej uvádza, že Trestný poriadok upravuje postup v trestnom konaní (§ 1 Trestného poriadku) a nie v občiansko-súdnom, správnom, či inom konaní. Je evidentne nadbytočné, aby trestno-procesný predpis ustanovoval podmienky pre dôkazné použitie podľa jeho úpravy v určitej veci zabezpečených informácií v inej veci s určením kritéria, že musí ísť o iné trestné (teda nie občianske súdne, správne alebo iné) konanie. Termín „súčasne" by však nezapadal ani do tejto konštrukcie.

Jediným vecne odôvodneným východiskom, ktoré je možné použiť pri výklade zákonnej požiadavky „súčasného vedenia trestného konania v inej trestnej veci" (s príslušnou právnou kvalifikáciou činu) je, podľa tohto názoru NS SR, 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.

Dotknutá informácia je však vždy použiteľná mimo procesne (operatívne), resp. ako informačný podklad pre následný procesný postup s jeho už aj dôkaznou relevanciou (§ 199 ods. 2 Trestného poriadku).

Platí teda, podľa tohto právneho názoru NS SR, nasledovné:

Dôkazné informácie zabezpečené postupmi podľa priatej hlavy prvej časti Trestného poriadku sa môžu zásadne použiť len v trestnej veci, v ktorej bol príslušný postup vykonaný na základe príkazu predsedu senátu alebo sudcu pre prípravné konanie.

Výnimkou z tejto zásady je súčasne vedenie trestného konania v inej trestnej veci v zmysle § 113 ods. 9, § 114 ods. 7, § 115 ods. 7, § 117 ods. 12 a § 118 ods. 7 Trestného poriadku (vždy musí ísť o konanie pre trestný čin uvedený v odseku jeden toho ktorého ustanovenia).

Súčasným vedením trestného konania v inej trestnej veci 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, prostredníctvom agenta, alebo porovnaním údajov v informačných systémoch).

Inou trestnou vecou sa rozumie trestné konanie (aj pred začatím trestného stíhania) pre iný skutok ako trestný čin. Takým činom je na účel aplikácie vyššie uvedených ustanovení potrebné chápať aj pokračovací trestný čin v celom súhrne jeho čiastkových útokov (§ 122 ods. 10 a ods. 13 Trestného zákona). Pre možnosť dôkazného použitia zabezpečenej informácie vo vzťahu ku všetkým čiastkovým útokom toho istého pokračovacieho trestného činu teda postačuje vedenie trestného konania pre niektorý z jeho čiastkových útokov.

V ustanovení § 117 ods. 12 Trestného poriadku absentuje explicitné vyjadrenie podmienky súčasného vedenia trestného konania v inej veci. Z hľadiska výkladovej systematiky je však zrejmé, že na „externé" dôkazné použitie informácií zabezpečených agentom sa tiež vzťahuje jed-

notný a z rovnakého princípu odvodený normatívny model riešenia dotknutej otázky, ktorý pokrýva všetky inštitúty upravené v piatej hlave prvej časti Trestného poriadku.

Na dôvažok najvyšší súd uvádza, že vypustenie požiadavky súčasného vedenia trestného konania (úpravou vyššie uvedených ustanovení) bolo súčasťou vládneho návrhu na zmenu Trestného poriadku, ktorá viedla ku jeho novelizácii zákonom č. 262/2011 Z. z. (s účinnosťou od 1. septembra 2011). V príslušnej obsahovej časti však návrh nebol Národnou radou Slovenskej republiky akceptovaný, čo síce nezohráva z pohľadu súdneho výkladu platného a účinného zákona rozhodujúci význam, táto okolnosť je však legitímnou súčasťou interpretačných podkladov vo vzťahu k dotknutým ustanoveniam.

V Týchto súvislostiach je vhodné tiež pripomenúť, že do práva na súkromie možno zasiahnuť len v odôvodnených prípadoch a na základe zásad legality, legitimity a proporcionality.

Legálny zásah znamená, že štát môže do práva na súkromie zasiahnuť iba na základe a v medziach zákona, pričom skúma, či k zásahu do súkromia došlo v súlade s platnými právnymi predpismi.

Legitimita zásahu znamená, že do práva na súkromie možno zasiahnuť len vtedy, keď je to v záujme štátu z dôvodov ochrany národnej bezpečnosti, verejnej bezpečnosti, predchádzania nepokojov a zločinnosti, ochrany zdravia a morálky, zabezpečenia hospodárskeho blahobytu krajiny a v záujme jednotlivcov z dôvodu ochrany ich práva slobôd.

Proporcionalita zásahu znamená, že k nemu možno prikročiť len vtedy, keď je to nevyhnutné a sledovaný cieľ nemožno dosiahnuť miernejšími prostriedkami a iba v duchu požiadaviek kladených na demokratickú spoločnosť vyznačujúcu sa pluralizmom a toleranciou.

Aby bolo možné v súlade s ustanovením § 2 ods. 12 Trestného poriadku 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 republike 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 pre odpočúvaním,
- príkaz alebo súhlas na použitie informačno-technických prostriedkov je riadne odôvodnený, obsahuje všetky stanovené náležitosti a bol vydaný príslušným súdom a sudcom,
- použitie informačno-technických prostriedkov bolo vykonané v súlade s vydaním príkazom,
- dôkaz získaný použitím informačno-technických prostriedkov je použiteľný v trestnom konaní z hľadiska kvality, obsahu a úplnosti.

Na druhej strane však Najvyšší súd SR, okrem iného a na rozdiel od citovaného rozhodnutia NS SR, vo svojom rozhodnutí **3 To 2/2011 z 21. 9. 2011** konštatuje, že záznam z telekomunikačnej činnosti vo veci, v ktorej konal, bol vykonaný na základe rozhodnutia príslušného súdu a sudcu, spôsobom, ktorý je v súlade s príslušnými ustanoveniami Trestného poriadku a rešpektuje vyššie spomenutí princípy. Tento záznam je preto potrebné považovať za dôkaz získaný zákonným spôsobom.

V ustanovení § 115 ods. 7 Trestného poriadku sa uvádza, že v inej trestnej veci, ako je tá, v ktorej sa odpočúvanie a záznam telekomunikačnej prevádzky vykonal, možno záznam použiť ako dôkaz len vtedy, ak sa súčasne aj v tejto veci vedie trestné konanie pre trestný čin uvedený v odseku 1 § 115 Trestného poriadku. V ods. 7 § 115 Trestného poriadku sú teda upravené podmienky na použitie tohto inštitútu ako dôkazu v inej trestnej veci.

Podľa názoru tohto senátu NS SR však slovo „súčasne" je potrebné správne vzťahovať až k okamžiku použitia výsledkov odposluchu, a nie už k okamihu vykonávania odposluchu.

Bolo by nelogické, pokračuje ďalej NS SR, aby zákonným spôsobom vykonaný odposluch a záznam telekomunikačnej prevádzky, ktorý vo veci, v ktorej bol nariadený, mohol byť vykonaný aj pred začatím trestného stíhania, ale v inej veci by mohol byť použitý len v tom prípade, ak by už v dobe vykonávania tohto odposluchu bolo v tejto inej veci vedené trestné stíhanie a nič by v tomto prípade nebránilo, aby bol súčasne nariadený odposluch 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. Na základe vyššie uvedeného NS SR neakceptoval odvolaciu námietku obžalovaného a uzatvoril, že použitie záznamu z odposluchu telekomunikačnej prevádzky v posudzovanej trestnej veci bolo ako dôkaz použité v súlade so zákonom.

Kazuistika

Úplná protichodnosť takéhoto rozhodovania sa, inter alia, prejavila aj v konkrétnej trestnej veci dozorovanej autorom tohto príspevku, právne kvalifikovanej ako trestný čin machinácie pri verejnom obstarávaní a verejnej dražbe podľa § 266 ods. 1, 2 písm. c), ods. 3 písm. a) Trestného zákona.

Špecifikum tejto trestnej veci, z hľadiska obsahu spracovanej témy, spočívalo v tom, že pôvodné odpočúvanie a záznamy boli vykonané podľa citovaného zákona č. 166/2003 Z. z. v platnom znení o ochrane pred odpočúvaním, **pre korupčnú trestnú činnosť**. V rámci tohto odpočúvania boli úplne detailne **zistené skutočnosti o spáchaní trestného činu machinácií pre verejnom obstarávaní a verejnej dražbe podľa § 266 ods. 1, 2 písm. c), ods. 3 písm. a) Trestného zákona, o ktorom však vtedy trestné konanie vedené nebolo**. Po zistení skutočnosti o dôvodnom podozrení o spáchaní tohto trestného činu vyšetrovateľ bezodkladne začal trestné stíhanie a zároveň bolo bezodkladne začaté odpočúvanie telekomunikačnej prevádzky podľa § 115 Trestného poriadku. Postupom podľa § 115 Trestného poriadku však na rozdiel od postupu podľa citovaného zákona č. 166/2003 Z. z. v platnom znení, relevantné dôkazy zistené neboli. Aj z uvedených dôvodov, teda konštatujúc, že sa súčasne neviedli obe trestné konania, prvostupňový súd nevyhovel dôkaznému návrhu prokurátora na dokazovanie zvukovým záznamom podľa § 270 ods. 2 Trestného poriadku a obžalovaných spod obžaloby prokurátora podľa § 285 písm. a) Trestného poriadku oslobodil. Prvostupňový súd svoje rozhodnutie odôvodnil v podstate tým, že v súlade s existujúcou judikatúrou, okrem iného, aj v súlade rozsudkom NS SR sp. zn. 2 To 5/2011, bol súdom prijatý záver, že ide o dôkaz získaný v inej trestnej veci, pričom v tejto konkrétnej veci, za ktorú bola podaná obžaloba, sa v čase odpočúvania a zaznamenávania telekomunikačnej činnosti na základe vyššie uvedeného súhlasu sudcu tohto súdu, neviedlo trestné stíhanie. Z uvedeného dôvodu preto prepisy zvukových záznamov, získané na základe vyššie uvedeného súhlasu sudcu tohto súdu, nebolo možné ako dôkaz v tomto konaní použiť. Uvedené prepisy zvukových záznamov mohli predstavovať len kriminálnu informáciu pre orgány činné v trestnom konaní, ale neboli, podľa súdu, použiteľné ako dôkazy v tejto trestnej veci. Pokiaľ ide o argumentáciu prokurátora v rámci jeho záverečného vyjadrenia, že platná judikatúra (vrátane citovaného rozhodnutia Najvyššieho súdu SR) sa vzťahuje iba na dôkazy získané v inej veci podľa Trestného poriadku, a nie na dôkazy získané postupom podľa osobitného zákona, súd uviedol, že tento názor prokurátora je z pohľadu súdu nesprávny, a to z dôvodu, že podľa § 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. Z tohto je zrejmé a nesporné, že či už dôkazy získané podľa tohto (Trestný poriadok) alebo podľa osobitného zákona (zák. č. 166/2003 Z. z. o ochrane pred odpočúvaním) musia byť získané zákonným spôsobom, lebo len tak možno prijať záver, že boli získané zákonným spôsobom, a to predovšetkým z pohľadu toho, že boli získané v konaní a spôsobom zameraným na zistenie konkrétnych skutočností, ktoré zistené majú byť a na ktoré bol súhlas alebo príkaz vydaný, teda na to, na čo bol príkaz určený a čo ním malo byť zistené. Akceptovanie názoru prokurátora, podľa súdu, by malo vo všeobecnosti za následok, že ak by sa v konkrétnej prejednávanej trestnej veci neviedlo trestné stíhanie už v čase, kedy v inej trestnej veci boli odpočúvaním zistené skutočnosti dôležité pre konanie v prejednávanej veci, mohlo by dôjsť k tomu, že akékoľvek skutočnosti významné pre trestné konanie v prejednávanej veci zistené kedykoľvek a kdekoľvek by následne boli používané ako dôkazy v prejednávanej veci, čo by bolo v rozpore so základnom požiadavkou, aby zásahy do Ústavou Slovenskej republiky a medzinárodno-právnymi dokumentmi chránených práv a slobôd fyzických osôb, realizovaných orgánmi štátu, boli vždy realizované len na zistenie tých konkrétnych skutočností, ktoré takýmto zásahom majú byť zistené, iba v nevyhnutnom rozsahu, len na nevyhnutnú dobu, za prísneho dodržania základných atribútov existujúceho zásahu z pohľadu ich legality, legitimity a proporcionality.

S takýmito právnymi závermi súdu sa nestotožňujem z nasledujúcich dôvodov.

Objektívnou skutočnosťou v danej trestnej veci je fakt, že k najdôležitejším dôkazom, z ktorých vyplýva objektívne zistený skutkový stav obžalobou, a teda pravdivý obraz zmanipulovaného verejného obstarávania, a zároveň k dôkazom usvedčujúcim, patria práve tie zvukové záznamy, ktoré, ako to už bolo konštatované, súd odmietol vykonať. Je pravdou, že tieto záznamy boli vykonané podľa zákona č. 166/2003 Z. z. v platnom znení o ochrane pred odpočúvaním, na rozdiel od vyššie uvedeného právneho názoru súdu však považujem tieto záznamy za zákonne vykonateľný a použiteľný dôkaz podľa § 119 ods. 2 Tr. por., podľa ktorého za dôkaz môže slúžiť všetko, čo môže prispieť na náležité objasnenie veci a čo sa získalo z dôkazných prostriedkov podľa tohto zákona (Trestného poriadku) alebo **podľa osobitného zákona**.

Inkriminované, súdom na hlavnom pojednávaní nevykonané zvukové záznamy, boli podľa môjho názoru pred hlavným pojednávaním vykonané zákonne podľa osobitného zákona, najmä v súlade s jeho § 3 ods. 1, 2 a § 7 ods. 2.

Podľa týchto ustanovení, ako to už bolo uvedené, informačno-technický prostriedok možno použiť 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 základné právo alebo sloboda obmedziť len v nevyhnutnom rozsahu a nie dlhšie, ako je to nevyhnutné na dosiahnutie zákonom uznaného cieľa, na ktorý slúži. Údaje získané informačno-technickými prostriedkami možno použiť výlučne na dosiahnutie účelu pri plnení úloh štátu, ktoré spĺňajú podmienky podľa odseku 1 (§ 3 ods. 1, 2).

Ak sa majú informácie získané 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 (§ 7 ods. 2).**

Najmä z poslednej vety citovaného zákona v spojitosti s uvádzaným ustanovením § 119 ods. 2 Tr. por. je zrejmé, že zákonný dôkaz v trestnom konaní možno získať aj podľa iného zákona ako

podľa Trestného priadku, t. j. aj podľa spomínaného zákona č. 166/2003 Z. z. v platnom znení o ochrane pred odpočúvaním, pričom kritériá zákonnosti vykonania a získania takého dôkazu sú uvedené v tomto osobitnom zákone. Za daných okolností preto na uvedený postup nemožno použiť kritériá zákonnosti podľa § 115 ods. 7 Tr. por., t. j. okrem iného aj súčasné vedenie trestného konania vo viacerých veciach, ale kritériá zákonnosti najmä podľa citovaného § 7 ods. 2 zákona č. 166/2003 Z. z. v platnom znení. Týmto kritériom použitia ITP ako dôkazu v trestnom konaní aj v inej veci je zákonná možnosť použitia ITP aj v tejto inej veci, čomu žalovaný pôvodný zločin machinácií pri verejnom obstarávaní a verejnej dražbe podľa § 266 ods. 1, ods. 3 písm. a) Tr. zákona vyhovuje a pritom sa nemusia súčasne viesť viaceré trestné konania.

Ak by súd tento, podľa môjho názoru, dôkaz pripustil a vykonal ho na hlavnom pojednávaní podľa § 270 ods. 2 Tr. por., potom by zistil objektívny priebeh manipulácie tohto verejného obstarávania obžalovanými tak, ako bol popísaný v obžalobe.

Práve v týchto súvislostiach, t. j. ak je spôsobom uvedeným v obžalobe preukázaná objektívna pravda, teda skutočné manipulovanie tejto verejnej súťaže obžalovanými, do pozornosti súdu je potrebné alternatívne dať aj tzv. Radbruchovu formulu, podľa ktorej sudca, ktorý by mal aplikovať zákon hrubo porušujúci spravodlivosť ako všeobecnú rovnosť, musí vychádzať z tejto spravodlivosti a náplň zákona ignorovať ako bezprávne právo. Teda pokiaľ je rozpor so spravodlivosťou extrémny tak ako v tomto prípade, potom má sudca povinnosť rozhodnúť contra legem a v súlade s prirodzeno-právnou teóriou práva a nie len v zmysle právneho pozitivizmu, musí hľadať objektívnu pravdu a rozhodnúť v súlade s ňou spravodlivo.

Konštatujem však, že tento postup má byť alternatívny, pretože prioritne, postupujúc podľa § 119 ods. 2 Tr. por. v spojitosti najmä s citovanými § 3 ods. 1, 2 a § 7 ods. 2 zákona č. 166/2003 Z. z. v platnom znení o ochrane pred odpočúvaním, mal súd vyhovieť návrhu prokurátora na vykonanie dôkazov podľa § 270 ods. 2 Tr. por. v celom rozsahu, v dôsledku čoho by v kontexte aj iných vykonaných dôkazov rozhodol objektívne, zákonne a spravodlivo odsudzujúcim a nie oslobodzujúcim rozsudkom.

Najvyšší súd SR rozhodujúci o odvolaní pod sp. zn. **1 To 8/2014** z **29. 10. 2014** vyhovel odvolaniu prokurátora, zrušil napadnutý rozsudok a túto vec vrátil súdu prvého stupňa, aby ju v potrebnom rozsahu znova prejednal a rozhodol. NS SR k dôvodom takéhoto svojho rozhodnutia, okrem iného uviedol, že s poukazom na existujúcu judikatúru, okrem iného aj na rozsudok Najvyššieho súdu SR sp. zn. 2 To 5/2011, bol súdom prvého stupňa prijatý záver, že ide o dôkaz získaný v inej trestnej veci, pričom v tejto konkrétnej veci, za ktorú bola podaná obžaloba sa v čase odpočúvania a zaznamenávania telekomunikačnej činnosti na základe vyššie uvedeného súhlasu sudcu tohto súdu, neviedlo trestné stíhanie. Podľa názoru súdu prvého stupňa z uvedeného dôvodu preto prepisy zvukových záznamov získané na základe vyššie uvedeného súhlasu sudcu tohto súdu nebolo možné ako dôkaz v tomto konaní použiť, ale uvedené prepisy zvukových záznamov mohli predstavovať len kriminálnu informáciu pre orgány činné v trestnom konaní, ale nie sú použiteľné ako dôkazy v tejto trestnej veci.

Súd prvého stupňa svojou argumentáciou nepresvedčil odvolací súd o dôvodnosti jeho právneho názoru, ktorým odmietol vykonať ako dôkaz oboznámenie prepisov zvukových záznamov. Podľa názoru odvolacieho súdu, pôvodný súhlas sudcu spĺňa všetky materiálne i formálne podmienky, ktorú skutočnosť nespochybňuje ani súd prvého stupňa. Pri označenom súhlase príslušný sudca konal v súlade s ustanoveniami 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.

Podľa § 7 ods. 2 zákona o ochrane pred odpočúvaním, ak sa majú informácie získané použitím informačno-technického prostriedku použiť ako dôkaz v trestnom konaní, vyhotoví or-

gán 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.

V analyzovanej trestnej veci bolo vedené trestné stíhanie pre zločin, a teda informácie získané použitím informačno-technického prostriedku podľa zákona č. 166/2003 Z. z. v znení neskorších predpisov, sa môžu použiť ako dôkaz v trestnom konám, pretože to umožňuje ustanovenie § 115 ods. 1 Tr. por. S poukazom na ustanovenie § 119 ods. 2 Tr. por. malo teda byť úlohou súdu prvého stupňa vykonať všetky dostupné dôkazy v predmetnej trestnej veci a tieto následne vyhodnotiť v súlade s ustanovením § 2 ods. 12 Tr. por. Súd prvého stupňa na podporu svojho procesného postupu poukazoval aj na rozsudok Najvyššieho súdu SR sp. zn. 2 To 5/2011, pričom na tomto mieste Najvyšší súd SR poznamenal, že existujú aj iné rozhodnutia súvisiace s prejednávanou problematikou, ako napríklad rozhodnutie Najvyššieho súdu Slovenskej republiky sp. zn. 3 To 2/2011 zo dňa 21. septembra 2011, s presne opačnou právnou argumentáciou.

V súvislosti s aplikáciou judikatúry v rozhodovacej činnosti všeobecných súdov Najvyšší súd SR primárne pripomenul, že podľa ustanovenia § 2 ods. 3, ods. 4 zákona č. 385/2000 Z. z. v znení neskorších predpisov, sudca je pri výkone svojej funkcie nezávislý a pri rozhodovaní viazaný len Ústavou Slovenskej republiky, ústavným zákonom, medzinárodnou zmluvou podľa čl. 7 ods. 2 a ods. 5 Ústavy Slovenskej republiky a zákonom.

Právny názor Ústavného súdu Slovenskej republiky obsiahnutý v jeho rozhodnutí vydanom v konaní podľa čl. 125 ods. 1 Ústavy Slovenskej republiky, na základe návrhu súdu, je pre súd záväzný. Za podmienok ustanovených osobitnými predpismi je sudca viazaný aj právnym názorom, ktorý vyslovil vo svojom rozhodnutí súd vyššieho stupňa.

Na základe tejto argumentácie NS SR uvedenej v jeho uznesení sp. zn. 1 To 8/2014 z 29. 10. 2014, prvostupňový súd naopak, v porovnaní s pôvodným svojim oslobodzujúcim rozsudkom, páchateľov odsúdil za žalovaný trestný čin machinácii pri verejnom obstarávaní a verejnej dražbe podľa § 266 ods. 1, 2 písm. c), ods. 3 písm. a) Trestného zákona, akceptujúc zákonnosť postupu podľa zákona č. 166/2003 Z. z. v platnom znení o ochrane pred odpočúvaním, ako aj zákonnosť postupu podľa § 115 Trestného poriadku.

Paradoxne však na základe odvolania obžalovaných podaných proti tomuto odsudzujúcemu rozsudku, Najvyšší súd SR v inom zložení senátu, pod sp. zn. **4 To 2/2016 z 23. 11. 2017** zrušil tento naposledy uvádzaný odsudzujúci prvostupňový rozsudok a vrátil súdu prvého stupňa, aby ju v potrebnom rozsahu znova prejednal a rozhodol.

V tomto svojom rozhodnutí NS SR, okrem iného uviedol, že záznamy telekomunikačnej prevádzky, ktorých prepisy boli v tomto konaní použité ako jediný usvedčujúci dôkaz, boli zadovážené za účelom získania skutočností významných pre trestné konanie vedené pre trestnú činnosť žiadnym spôsobom nesúvisiacu s trestnou činnosťou obžalovaných, pre ktorú na nich bola podaná obžaloba v tomto konaní, a to v období pred začatím trestného stíhania v tejto trestnej veci.

NS SR tiež zdôraznil, že rešpektovanie zákonnosti pri vykonávaní dôkazov nie je abstraktnou a formalistickou požiadavkou, ale má základný význam pre spravodlivosť trestného procesu, dôsledkom čoho je, že dôkaz získaný nezákonným spôsobom nemožno brať do úvahy bez toho, aby súčasne došlo k poškodeniu riadneho výkonu spravodlivosti. Uvedené, podľa tohto názoru NS SR, vyplýva z ustanovenia § 2 ods. 1 Tr. por., v zmysle ktorého nikto nemôže byť stíhaný ako obvinený inak než zo zákonných dôvodov a spôsobom, ktorý ustanovuje tento zákon. Zákon-

nosť dôkazu predpokladá, že bol získaný z prameňa, ktorý stanovuje alebo pripúšťa zákon, a zabezpečený a vykonaný procesným subjektom k tomu zákonom oprávneným, a to v zodpovedajúcom štádiu trestného konania a postupom, ktorý je v súlade s právnymi predpismi. Vzhľadom na okolnosti prejednávaného prípadu súd tiež poznamenal, že okrem zákonnosti dôkazu je potrebné rozlišovať tzv. procesnú použiteľnosť dôkazu (prípustnosť dôkazu), pri ktorej ide v zásade o zákonný dôkaz, ktorý však vzhľadom k určitým okolnostiam nemôže byť použitý v ďalšom priebehu konania a nie je možné z neho vychádzať pri ustaľovaní skutkového stavu veci.

Skutočnosti zodpovedá, že v súčasnosti existujú k prejednávanej problematike prípustnosti použitia záznamov telekomunikačnej prevádzky ako dôkazu v inej trestnej veci, ako je tá, v ktorej sa odpočúvanie vykonalo a záznam vyhotovil, protichodné rozhodnutia Najvyššieho súdu SR. Odlišnosti vo výklade podmienok použitia inštitútu odpočúvania a záznamu telekomunikačnej prevádzky ako dôkazu v inej trestnej veci, vyjadrených v § 115 ods. 7 Tr. por., najmä rozdielne chápanie obsahu pojmu „súčasne vedené trestné konanie," doposiaľ zjednocujúcim stanoviskom trestnoprávneho kolégia Najvyššieho súdu Slovenskej republiky neboli odstránené. Zároveň však treba dodať, že ani jedno z výkladovými rozdielnosťami dotknutých rozhodnutí najvyššieho súdu nemá povahu judikátu.

V kontexte prejednávanej veci je, podľa tohto právneho názoru jedného zo senátov NS SR určujúce vymedzenie podmienok použitia záznamu telekomunikačnej prevádzky ako dôkazu v inej veci než je tá, v ktorej bol získaný, ktoré je obsiahnuté v § 115 ods. 7 Tr. por. Uvedené ustanovenie Trestného poriadku určuje, že 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. Z citovaného ustanovenia, podľa NS SR, vyplýva, že Trestný poriadok spája možnosť použitia záznamu telekomunikačnej prevádzky ako dôkazu v inej trestnej veci s existenciou ďalšieho trestného konania. Pritom už samotná voľba výrazových prostriedkov, ktorými zákonodarca špecifikoval podmienky, za akých možno pristúpiť k použitiu záznamu telekomunikačnej prevádzky ako dôkazu aj v tomto ďalšom konaní, zároveň, s ohľadom na ich jazykový výklad, nenecháva žiaden priestor pre pochybnosti o tom, že toto ďalšie trestné konanie musí spĺňať dve podmienky.

Musí byť vedené pre niektorý z trestných činov, ktoré sú Trestným poriadkom taxatívne vymenované v ustanovení § 115 ods. 1, a zároveň musí byť vedené v rovnakom čase ako trestné konanie, v rámci ktorého k získaniu tohto dôkazného prostriedku došlo. Slovo „súčasne," použité v dikcii ustanovenia § 115 ods. 7 Tr. por., vyjadrujúceho podmienky použitia záznamu telekomunikačnej prevádzky v inej trestnej veci ako je tá, v ktorej bol vyhotovený, tak nepochybne vyjadruje práve časovú súvislosť trestného konania, v rámci ktorého bolo odpočúvanie vykonané a záznam vyhotovený, a trestného konania, v ktorom sa má tento záznam použiť ako dôkaz. Vecná súvislosť týchto konaní, daná právnou kvalifikáciou trestných činov, pre ktoré majú byť za účelom naplnenia podmienok ustanovenia § 115 ods. 7 Tr. por. vedené, totiž vyplýva už z odkazu na odsek 1 tohto ustanovenia Trestného poriadku, a teda nevyžaduje prítomnosť slova „súčasne," ktoré by sa takto javilo byť nadbytočným. Pritom požiadavka na súčasné vedenie trestného konania v trestnej veci, v ktorej záznam telekomunikačnej prevádzky síce nebol vyhotovený, ale má byť ako dôkaz použitý, sa musí, podľa názoru NS SR, logicky vzťahovať už na okamih získania tohto dôkazu, teda na okamih realizácie odpočúvania a vyhotovenia záznamu telekomunikačnej prevádzky, respektíve už na okamih vydania príkazu na odpočúvanie a záznam telekomunikačnej prevádzky. Za zákonný totiž možno považovať len dôkaz, ktorý bol zákonným spôsobom nielen vykonaný, ale v súlade so zákonom už aj získaný, preto výklad, v zmysle ktorého pre zákonnosť a prípustnosť použitia záznamu telekomunikačnej prevádzky v inej trestnej veci, než je tá, v ktorej bol príkaz na odpočúvanie a záznam telekomu-

nikačnej prevádzky vydaný, stačí, aby v čase jeho použitia bolo stále vedené aj trestné konanie, v ktorom sa odpočúvanie a záznam telekomunikačnej prevádzky vykonali, nemá žiadne opodstatnenie. Vykonanie, hoci aj toho istého, dôkazu totiž prebieha v každej trestnej veci samostatne, a teda aj zákonnosť jeho realizácie podmieňujú konkrétne procesné postupy, zvolené súdom v tej-ktorej veci. Fázou dokazovania, v ktorej dochádza k prieniku trestných konaní a ktorá je teda spoločná pre všetky trestné konania, v ktorých sa konkrétny dôkaz používa, je získanie dôkazu. Časová súvislosť trestných konaní, požadovaná zákonom ako podmienka prípustnosti použitia dôkazu získaného v jednom trestnom konaní aj v ďalšom trestnom konaní, sa potom zákonite musí odvíjať práve od tejto fázy dokazovania. Uvedený prístup je navyše aj v súlade s požiadavkou na reštriktívny výklad podmienok zásahov do základných práv a slobôd. Rovnako, uvažujúc v kontexte požiadaviek stanovených Trestným poriadkom v § 115 ods. 1 na aplikáciu inštitútu odpočúvania a záznamu telekomunikačnej prevádzky, nemožno ani z hľadiska systematického a teleologického výkladu pripustiť, aby sa v jednej trestnej veci na použitie tohto zabezpečovacieho prostriedku vyžadovalo splnenie konkrétnych, zákonom presne špecifikovaných podmienok, obmedzujúcich jeho uplatnenie len na zistenie tých konkrétnych skutočností, ktoré takýmto zásahom majú byť zistené, len v nevyhnutnom rozsahu, len na nevyhnutnú dobu a za prísneho rešpektovania kritérií legality, legitimity a proporcionality, a v inej trestnej veci bolo možné stotožniť sa s použitím výsledkov takéhoto zásahu do Ústavou Slovenskej republiky i medzinárodno-právnymi dokumentmi chránených práv a slobôd fyzických osôb, realizovaného v čase, keď sa zo strany orgánov činných v trestnom konám o existencii možnosti (s)páchania určitého, čo do podstaty skutku aspoň rámcovo identifikovaného činu, ani len neuvažovalo. Účelom inštitútu odpočúvania a záznamu telekomunikačnej prevádzky nie je preventívne zisťovanie skutočností, ktoré by potenciálne mohli byť významnými pre trestné konanie v nejakej veci a ich následné použitie ako dôkazov v akomkoľvek trestnom konaní, ale existenciou dôvodného predpokladu podmienené zistenie konkrétnych skutočností významných pre trestné konanie vedené v konkrétnej trestnej veci.

Konštatované vedie, podľa tohto názoru NS SR, k jednoznačnému záveru o prípustnosti použitia záznamu telekomunikačnej prevádzky ako dôkazu v trestnom konaní vedenom v inej trestnej veci než je tá, v ktorej došlo k jeho vyhotoveniu, len v prípade, že, použijúc dikciu ustanovenia § 115 ods. 7 Tr. por., trestné konanie v tejto inej trestnej veci bolo vedené už v čase vykonania odpočúvania a vyhotovenia záznamu telekomunikačnej prevádzky.

Kľúčovým pre posúdenie prípustnosti použitia záznamu telekomunikačnej prevádzky ako dôkazu v trestnom konaní vedenom v inej trestnej veci než je tá, v ktorej došlo k vydaniu príkazu na odpočúvanie a záznam telekomunikačnej prevádzky, bude preto určenie okamihu začatia trestného konania v tejto inej trestnej veci. Trestné konanie je Trestným poriadkom v § 10 ods. 15 definované ako konanie podľa tohto zákona. Prakticky to znamená, že v trestnom konaní vedenom v prejednávanej trestnej veci by prichádzalo do úvahy použitie ako dôkazu tých záznamov telekomunikačnej prevádzky, ktoré boli v rámci konania, v ktorom bol vydaný príkaz na odpočúvanie a záznam telekomunikačnej prevádzky, vyhotovené v čase od podania trestného oznámenia v prejednávanej trestnej veci, či v čase od zistenia trestného činu príslušným orgánom činným v trestnom konaní.

Niet, podľa tohto názoru NS SR, pochybností o tom, že informácie získané použitím informačno-technických prostriedkov, realizovaným na základe príkazu (súhlasu) zodpovedajúceho po formálnej i obsahovej stránke uvedeným požiadavkám (v posudzovanom prípade podľa § 3 a § 4 zákona o ochrane pred odpočúvaním), predstavujú dôkazný prostriedok získaný zákonným spôsobom. Tento záver platí v plnom rozsahu aj pre záznamy telekomunikačnej prevádzky, o ktoré ide v prejednávanej veci. Nie vždy však zákonným spôsobom získaný dôkazný pros-

triedok možno v ďalšom, najmä súdnom, či v dokonca inom trestnom konaní použiť ako dôkaz na preukazovanie viny páchateľa (napríklad nemožno na hlavnom pojednávaní prečítať výpoveď svedka z prípravného konania učinenú pred vznesením obvinenia, pretože táto nebola už v prípravnom konaní vykonaná kontradiktórne, a podobne). Odpočúvanie a zaznamenávanie telefonickej prevádzky predstavuje v každom prípade závažný zásah do ústavného práva na súkromie osoby, preto pripustenie použitia informácií v trestnom konaní, vo vzťahu ku ktorému boli prostredníctvom týchto informačno-technických prostriedkov získané takpovediac náhodne, bez vzťahu k v ňom prejednávanej trestnej veci, či aspoň vedomia existencie možnosti ich potenciálneho získania, vyplývajúceho z poznatku o vedení trestného stíhania v takej veci, ako dôkazu, teda aj v inej forme než v podobe kriminálnej informácie, ktorou nepochybne sú, keďže v prípade, keď sa v určitej trestnej veci ešte trestné stíhanie nevedie, povedú evidentne práve tieto informácie k vôbec vytvoreniu podozrenia zo (s)páchania trestného činu v tejto veci, by bolo bezprecedentným zaznávaním významu (Ústavou Slovenskej republiky i celým radom medzinárodno-právnych dokumentov poskytovanej) ochrany tohto základného práva fyzických osôb na jednej strane v prospech zľahčenia postupu orgánov činných v trestnom konaní na strane druhej. Na záver o zákonnosti dôkazu sa z hľadiska jeho zadováženia vyžaduje nielen splnenie formálnych podmienok upravených Trestným poriadkom, ale aj naplnenie materiálnych, t. j. obsahových podmienok. To znamená, že použitý dôkazný prostriedok na vykonanie, prípadne získanie dôkazu musí byť zameraný na zistenie takých skutočností, na ktoré, aj s ohľadom na podmienky a dôvody jeho použitia, môže byť zameraný a použitý. Na podklade uvedeného, osobitne majúc na zreteli požiadavku na rešpektovanie princípu právnej istoty, je žiaduce posudzovať okamih prípustnosti použitia záznamov telekomunikačnej prevádzky získaných v trestnom konaní vedenom pre jednu trestnú vec ako dôkazu v inej trestnej veci s ohľadom na začatie trestného stíhania ako toho určujúceho momentu, ktorý je možné v každom prípade stanoviť s úplnou presnosťou.

Podľa názoru najvyššieho súdu dôkaz, ktorý bol realizovaný v inej trestnej veci, nemôže byť dôkazom v trestnej veci, pre ktorú sa v čase jeho získania ešte neviedlo trestné stíhanie. Ako na to dovolací súd poukázal vyššie, odpočúvaním v inej trestnej veci získané informácie, ešte len vedúce k sformovaniu podozrenia z páchania určitej trestnej činnosti, môžu byť iba podkladom na začatie trestného stíhania, po ktorom následne musia orgány činné v trestnom konaní postupovať pri obstarávaní dôkazov za účelom potvrdenia alebo vyvrátenia nadobudnutého podozrenia v súlade s Trestným poriadkom.

Uvedené platí aj za stavu, že súhlas na odpočúvanie a zaznamenávanie telekomunikačnej služby bol vydaný podľa § 4 ods. 1, § 4a ods. 1 písm. b) s poukazom na § 2 ods. 1 písm. b) zákona o ochrane pred odpočúvaním, a citovaný zákon vo svojom ustanovení § 7 ods. 2 druhá veta výslovne upravuje podmienky použitia takto získaných informácií ako dôkazu v trestnom konaní v inej trestnej veci tak, že 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. Trestný poriadok totiž na rozdiel od zákona o ochrane pred odpočúvaním podrobnejšie upravuje zákonné podmienky odpočúvania a záznamu telekomunikačnej prevádzky, čo je z hľadiska ochrany základných práv a slobôd fyzických osôb v súlade s Ústavou Slovenskej republiky i príslušnými medzinárodno-právnymi dokumentmi ochrany práv a slobôd, ktorými je Slovenská republika viazaná. Z uvedených dôvodov a tiež vzhľadom na všeobecnosť znenia citovaného ustanovenia § 7 ods. 2 zákona o ochrane pred odpočúvaním je pri posudzovaní podmienok prípustnosti použitia informačno-technických prostriedkov, respektíve informácií získaných ich použitím, v súlade s potrebou reštriktívneho výkladu podmie-

nok akýchkoľvek zásahov do základných práv a slobôd nevyhnutné vychádzať zo znenia dotknutých ustanovení Trestného poriadku (§ 115 ods. 7).

Vzhľadom na súčasný stav danej veci, autor príspevku zotrváva len na uvedení tejto rozpornej súdnej argumentácii, ku ktorej doposiaľ neexistuje zjednocujúce stanovisko.

Záver

Na základe zistení uvedených v tomto texte možno prijať tieto závery:

Z hľadiska právnej úpravy a aplikačnej praxe autora tohto príspevku sa v kontexte analyzovanej problematiky javí najproblematickejším znenie a aplikácia § 115 ods. 7 Trestného poriadku, v zmysle 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.

Legitímnymi sú potom otázky, aký praktický dopad má toto ustanovenie na jeho aplikáciu v praxi a či je takáto právna úprava správna, resp. či sú dôvodnými úvahy de lege ferenda o zmene znenia tohto ustanovenia Trestného poriadku.

Ako ukázal skorší obsah tohto príspevku, výklad pojmu súčasné vedenie trestného konania rozdeľuje orgány činné v trestnom konaní a súdy, vrátane senátov Najvyššieho súdu SR, v zásade do dvoch názorových skupín, pričom oba názory majú svoju relatívnu relevanciu. Jedna z názorových skupín sa prikláňa k tomu názoru, že súčasné vedenie trestného konania znamená jeho súčasné vedenie v čase dokazovania týmito dôkazmi (napr. rozhodnutia NS SR sp. zn. 3 To 2/2011, 1 To 8/2014), iná názorová skupina tvrdí, že súčasné vedenie trestného konania znamená viesť toto konanie súčasne v čase vykonávania odpočúvania (napr. rozhodnutia NS SR sp. zn. 2 To 5/2011, 4 To 2/2016).

Za predpokladu, ak by sa mali odpočúvania telekomunikačnej prevádzky najmenej v dvoch veciach vykonávať podľa Trestného poriadku, zastáva autor tohto príspevku ten právny názor, že súčasné vedenie trestného konania znamená jeho vedenie (dokazovanie) v rovnakom čase. Je však potrebné zdôrazniť pojem trestné konanie, a teda, že nejde o trestné stíhanie, čo znamená, že stačí viesť súbežné konania postupom aj podľa § 196 Trestného poriadku. Na druhej strane je potrebné tiež zdôrazniť, že pojem trestné konanie neznamená vykonávanie policajných úkonov podľa Zákona o Policajnom zbore, nejde teda o súčasné vedenie trestného konania a tzv. operatívnych policajných činností.

V prípade situácie, že sa najprv odpočúvanie vykonáva podľa citovaného zákona č. 166/2003 Z. z. v platnom znení o ochrane pred odpočúvaním a potom v nadväznej časovej súvislosti po začatí trestného stíhania podľa § 115 Trestného poriadku, zastáva autor tohto príspevku právny názor, že v intenciách citovaného § 119 ods. 2 Trestného poriadku, sú použiteľné v trestnom konaní aj dôkazy získane odpočúvaním podľa citovaného zákona č. 166/2003 Z. z. v platnom znení, vnímajúc túto procesnú situáciu viac prirodzenoprávne ako prísne formálnoprávne.

Z hľadiska právnych úvah de lege ferenda sa prikláňam k vypusteniu citovaného § 115 ods. 7 a ďalších analogických ustanovení Trestného poriadku. Vychádzam pritom z analogického procesného stavu zodpovedajúceho napr. aj nájdeniu takých rôznych zakázaných látok alebo predmetov pri domovej prehliadke alebo pri prehliadke iných priestorov a pozemkov, ktoré neboli obsahom príslušných príkazov, a napriek tomu po ich nájdení je tento úkon akceptovateľný ako zákonný.

Danú spornú procesnú situáciu by však mala čo najskôr riešiť aktuálna judikatúra Najvyššieho súdu SR.

Literatúra

Čentéš, J. a kol.: Trestné právo procesné. Všeobecná časť. Šamorín: Heuréka, 2016,
Čentéš, J.: Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. Bratislava: C. H. Beck, 2013,
Ivor, I. a kol.: Trestné právo procesné. Druhé, doplnené a prepracované vydanie. Bratislava: Iura Edition, 2010,
Záhora, J. a kol.: Obrazové a zvukové záznamy v trestnom konaní. Bratislava: Wolters Kluwer, 2018.

Posúdenie zásady proporcionality pri zaznamenaní telefonického hovoru

Assessment of the Proportionality Principle for Telephone Calling

Jozef Čentéš[1]

Abstrakt: *Využitie inštitútu odpočúvania je nevyhnutne spojené so zásahom do práva na súkromie. Práve z tohto dôvodu, aby bolo takéto využitie v súlade so zákonom, resp. aby tieto zásahy boli považované za dovolené, musia byť splnené prísne stanovené zákonné požiadavky. V príspevku autor zameriava pozornosť na oprávnené zásahy do práva na súkromie pri odpočúvaní, a to z hľadiska zásad legality, legitimity a najmä proporcionality takéhoto zásahu.*

Abstract: *The use of the interception institute is necessarily linked to interference with the right to privacy. It is for this reason that such use is in accordance with the law. In order for these interventions to be considered lawful, strict legal requirements must be met. In this paper, the author focuses on legitimate interferences of the right to privacy when dealing with interception, in regards to the legal principles, legitimacy and the proportionality of such intervention in particular.*

Kľúčové slová: *právo na súkromie, orgán verejnej moci, zásah, zásada legality, zásada legitimity, zásada proporcionality.*

Key words: *right of privacy, public official, interference, the principle of legality, the principle of legitimacy, the principle of proportionality*

1. Úvod

V prípadoch, v rámci ktorých dochádza k využitiu inštitútu odpočúvania telefonického hovoru dochádza k zásahu do práva na súkromie. Práve z tohto dôvodu, aby bolo takéto využitie v súlade so zákonom, resp. aby tieto zásahy boli považované za dovolené, musia byť splnené prísne stanovené zákonné požiadavky. Kategorickým imperatívom pri posudzovaní zásahu orgánu verejnej moci do práva na súkromie pri odpočúvaní telefonického hovoru je hľadanie spravodlivej rovnováhy medzi potrebami verejného (všeobecného) záujmu a ochranou súkromia fyzickej osoby. Významnú úlohu pri výklade a hodnotení zásahov do práva na súkromie zohrávajú rozhodovacia činnosť Európskeho súdu pre ľudské práva (v minulosti aj Európskej komisie pre ľudské práva) a Ústavného súdu Slovenskej republiky (ďalej len „Ústavný súd"), ktoré precizujú (dotvárajú) právnu úpravu zásahov do práva na súkromie. Podľa tejto rozhodovacej činnosti zásahy do práva na súkromie sa vykladajú v určitej logickej nadväznosti, resp. postupnosti. Predovšetkým sa skúma, či daný **skutkový stav možno ratione materiae považovať za súčasť práva na súkromie**. Po kladnej odpovedi na túto otázku treba skúmať kumulatívne splnenie troch zásad, ktorými sú **legalita**, **legitimita** a **proporcionalita** takéhoto zásahu.[2] Tieto zásahy sa posudzujú v určitej postupnosti. Najskôr sa skúma, či zásah bol legálny (zákonný). V ďalšom sa potom skúma, či bol zásah legitímny, a napokon či bol proporcionálny. Ak sa dospeje k negatívnej odpovedi pri niektorom z týchto zásahov, ďalej sa v skúmaní problematiky nepokračuje a kon-

[1] Prof. JUDr. Jozef Čentéš, PhD., Právnická fakulta, Univerzita Komenského v Bratislave, Katedra trestného práva, kriminológie a kriminalistiky, e-mail: jozef.centes@flaw.uniba.sk.

[2] ČENTÉŠ, J.: Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. Bratislava: C. H. Beck, 2013, s. 38 a nasl. V tomto príspevku sú použité viaceré námety z tejto vedeckej monografie.

štatuje sa porušenie článku 8 Dohovoru o ochrane ľudských práv a základných slobôd (ďalej len „Dohovor“).[3]

2. Zásada legality

Ochrana súkromia jednotlivca, rovnako ako ochrana iných základných práv a slobôd pri odpočúvaní nie je absolútna. Medzinárodné zmluvy a Ústava Slovenskej republiky (ďalej len „Ústava“) umožňujú zásahy do práva na súkromie v prípadoch, ktoré ustanoví zákon. **Legalita zásahu** do práva na súkromie znamená, že orgán verejnej moci môže zasiahnuť do tohto práva iba na **základe zákona** a v **súlade so zákonom**. Z tohto dôvodu napr. záujem štátu na ochrane pred páchaním trestnej činnosti zakladajúci oprávnenosť zásahu do tohto práva musí byť uvedený do rovnováhy so závažnosťou zásahu do tohto práva.

Európsky súd pre ľudské práva uplatňuje článok 8 Dohovoru podľa tézy, že pojmy „právo“ a „zákon“ chápe v materiálnom, a nie formálnom význame.[4] To znamená, že „zákonom“ sa nerozumie iba všeobecne záväzný právny predpis schválený parlamentom, ale aj ďalšie pramene práva vrátane súdnych rozhodnutí a právnej doktríny.[5] Na druhej strane však vyžaduje kvalitu práva, ktoré má byť dostupné a predvídateľné dotknutej osobe a zlučiteľné s princípmi právneho štátu.

V kontexte s Dohovorom je potrebné sa zaoberať kvalitou zákona, ktorý zásah do tohto práva umožňuje. Zákon by smeroval proti výsadnému postaveniu práva, ak by posudzovacia právomoc orgánu verejnej moci pri odpočúvaní nepoznala medze. Preto zákon musí definovať rozsah a podmienky výkonu takejto právomoci dostatočne jasne, s ohľadom na sledovaný legitímny cieľ, aby jednotlivcovi- fyzickej osobe poskytol adekvátnu ochranu proti svojvôli. Z tohto dôvodu je nevyhnutné, aby vnútroštátny zákon poskytoval istú ochranu fyzickej osobe podľa článku 8 Dohovoru aj pri odpočúvaní telefonického hovoru orgánmi verejnej moci.

Podľa rozhodovacej činnosti Európskeho súdu pre ľudské práva požiadavka **„v súlade so zákonom“** vyjadrená v článku 8 ods. 2 Dohovoru vyžaduje v prvom rade, aby dotknuté opatrenie malo základ vo vnútroštátnom práve (v zákone), pretože predstavuje základ zásahu do práva na súkromie.[6] V druhom rade vyžadujú určitú kvalitu zákona, teda, aby bol dostupný dotknutej osobe; aby bol dostatočne jasný, aby poskytol dotknutej osobe zodpovedajúce údaje o okolnostiach a podmienkach, za akých sú orgány verejnej moci oprávnené použiť dotknuté opatrenie. Pri posudzovaní, či je daný takýto „zákonný základ“, je potrebné vziať do úvahy nielen príslušné právne predpisy, ale tiež judikatúru.[7] Európsky súd pre ľudské práva pri tejto požiadavke odkazuje predovšetkým na vnútroštátne právo, pričom tomuto súdu v zásade neprislúcha kontrolovať zákonnosť „delegovaného zákonodarstva“; to prislúcha predovšetkým vnútroštátnym súdom.[8]

---

[3] I. ÚS 274/05 a I. ÚS 117/07. ZÁHORA, J.: Uchovanie počítačových údajov a ochrana súkromia. In: Justičná revue, r. 63, 2011, č. 6–7, s. 904. ČENTÉŠ, J. – LAZAREVA, N.: Legalita, legitimita a proporcionalita odpočúvania a zaznamenávania telekomunikačnej prevádzky. In: 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, s. 183 – 198, konanej dňa 19. januára 2012, Fakulta práva Paneurópskej vysokej školy, Bratislava.

[4] Huvig v. Francúzsko z 24. apríla 1990.

[5] Kopp v. Švajčiarsko z 25. marca 1998.

[6] I. ÚS 117/07.

[7] Huvig v. Francúzsko z 24. apríla 1990. Kruslin v. Francúzsko z 24. apríla 1990.

[8] Campbell v. Spojené kráľovstvo z 25. marca 1992.

V kontexte s dôvernými opatreniami pri odpočúvaní orgánmi verejnej moci, s ohľadom na nedostatok verejnej kontroly a riziko zneužitia moci sa kladie dôraz na dostatočnú presnosť právneho predpisu. Tým sa má dosiahnuť, aby právny predpis predstavoval prostriedok na ochranu pred svojvoľnými zásahmi orgánov verejnej moci do záujmu, ktorému sa priznáva ochrana. Z tohto dôvodu, ak právna úprava priznáva orgánu verejnej moci možnosť úvahy, rozsah a spôsob jej uplatnenia musí tak ustanoviť s dostatočnou jednoznačnosťou, aby sa zabezpečila ochrana garantovaných práv a slobôd. Skúsenosti ale ukazujú, že absolútna presnosť je nedosiahnuteľná a potreba vyhnúť sa prílišnej rigidite a držať krok s meniacimi sa okolnosťami znamená, že mnoho zákonov je nevyhnutne vyjadrených formuláciami, ktoré sú vo väčšom alebo v menšom rozsahu vágne.[9] Európsky súd pre ľudské práva si uvedomuje, že nie vždy je možné v zákone vyjadriť presnú formuláciu ustanovenia zákona, pričom v niektorých prípadoch je účelnejšie používať aj menej určitú formuláciu zákona. Dôležité v takomto prípade bude, aby predvídateľnosť zákona bola zabezpečená rozhodovacou činnosťou súdov.[10] Zákon, ktorý umožňuje voľnú úvahu, nie je sám o sebe nezlučiteľný s požiadavkou predvídateľnosti pod podmienkou, že rozsah voľnej úvahy a spôsob jej vykonania sú dané s dostatočnou jasnosťou, berúc do úvahy legitímny cieľ daného konkrétneho opatrenia, aby bola jednotlivcovi poskytnutá primeraná ochrana proti svojvoľnému zásahu.

Nutnosť dostatočne presnej právnej úpravy možno podporiť rozhodnutiami Európskeho súdu pre ľudské práva, ktorými vyslovil porušenie článku 8 Dohovoru Švajčiarskom, ktorého právna úprava umožnila úradníkovi právneho oddelenia Pošty, ktorý je členom výkonnej moci robiť tajné opatrenia bez dohľadu sudcu;[11] Francúzskom, ktorého právna úprava primerane jasne neurčila rozsah a spôsob uplatňovania takýchto opatrení príslušnými orgánmi,[12] Spojeným kráľovstvom ktorého právna úprava kontroly komunikácie pre policajné účely bola nejasná, predovšetkým nebolo zrejmé, ktorá časť kontroly bola upravená v právnom predpise a ktorá bola ponechaná na voľnej úvahe výkonnej moci[13]; Španielskom, ktorého právna úprava nedefinovala kategórie fyzických osôb, ktoré možno odpočúvať, druh trestných činov, pre ktoré možno odpočúvať a neurčovala časový limit odpočúvania a postup pre vyhotovenie záznamu z odpočúvanie, využitie a možnosť zničenia nahrávok z odpočúvania.[14]

Zákonná úprava zásahu musí byť formulovaná tak, aby nebola popretím chránených práv a tomu musí zodpovedať aj ich interpretácia. Právny predpis musí byť:

a) dostupný,

b) predvídateľný.

Požiadavka **„dostupnosti“** je splnená v prípade verejného publikovania právneho predpisu (zákona) alebo uverejnenia oznámenia o jeho vydaní s určením miesta, kde možno doň nahliadnuť.[15] V podmienkach Slovenskej republiky je táto podmienka splnená spravidla vyhlásením všeobecne záväzného právneho predpisu v Zbierke zákonov Slovenskej republiky uverejnením jeho úplného znenia, ku ktorej majú fyzické osoby prístup. Medzinárodné zmluvy sa vyhlasujú tak, že sa v Zbierke zákonov uverejní oznámenie Ministerstva zahraničných vecí Slovenskej republiky o jej uzavretí obsahujúce jej úplné znenie alebo údaj o tom, kde možno do nej nazrieť, ako aj údaje dôležité na jej vykonávanie, najmä deň nadobudnutia platnosti pre Slovenskú re-

[9] Olsson v. Švédsko z 12. marca 1988.

[10] Gorzelik a ostatní v. Poľsko zo 17. februára 2004.

[11] Kopp v. Švajčiarsko z 25. marca 1998.

[12] Kruslin v. Francúzsko z 24. apríla 1990. K nedostatočnej právnej úprave pozri aj Doerga v. Holandsko z 24. apríla 2004 a Heglas v. Česko z 1. marca 2007.

[13] Malone v. Spojené kráľovstvo z 2. augusta 1984.

[14] Cosme Valenzuela Contreras v. Španielsko z 11. apríla 1997.

[15] Autronic v. Švajčiarsko z 22. mája 1990.

publiku. Táto podmienka môže byť splnená aj v prípade uverejnenia iným spôsobom napr. vo Finančnom spravodajcovi.[16]

V rámci požiadavky **„predvídateľnosti právneho predpisu“** Európsky súdu pre ľudské práva čo do zmyslu a povahy opatrení konštatuje, že článok 8 ods. 2 Dohovoru sa neobmedzuje na odkaz na vnútroštátne právo, ale týka sa aj kvality tohto práva, ktoré by malo byť kompatibilné s princípmi právneho štátu. Vnútroštátne právo musí poskytovať jednotlivcovi ochranu proti arbitrárnemu (svojvoľnému) zásahu do jeho práv, zaručených článkom 8 ods. 1 Dohovoru, a to s prihliadnutím na nedostatok verejnej kontroly a na riziko zneužitia moci. Preto musí dostatočne jasne vo svojich ustanoveniach poskytovať jednotlivcovi náležitú indikáciu podľa okolností a podmienok, za akých je verejná moc zmocnená k zásahu do jeho páva na súkromia v rámci tajných opatrení.[17] Z uvedeného vyplýva, že aj zásah, ktorý má svoj základ v právnej norme, môže za určitých okolností v konkrétnom prípade znamenať porušenie práv garantovaných Dohovorom, resp. Ústavou.[18] Podľa názoru Európskeho súdu pre ľudské práva samotný zákon môže porušovať práva jednotlivca, ak je tento jednotlivec priamo ovplyvnený zákonom pri súčasnom nedostatku konkrétneho prostriedku na jeho uplatňovanie“.[19]

Požiadavka „predvídateľnosti“ nemôže znamenať umožnenie predvídania jednotlivcovi, či a kedy orgány verejnej moci zaznamenajú jeho telefónny hovor. Zákon, ale musí mať dostatočné znenie ustanovení, aby bolo každému zrejmé, za akých okolností a podmienok disponujú orgány verejnej moci oprávnením vykonať tento tajný a potencionálne nebezpečný zásah do práva na súkromie.[20] Podľa Európskeho súdu pre ľudské práva (...) *„požiadavka kvality zákona a predvídateľnosti je formulovaná preto, aby každá osoba mohla – v prípade potreby za pomoci znalých poradcov – prispôsobiť svoje správanie pravidlám ustanoveným v zákone.*“[21] Právna norma sa nemôže považovať za „zákon“ pokiaľ nie je formulovaná s dostatočnou presnosťou tak, aby umožnila jednotlivcovi-fyzickej osobe, ak je to potrebné vo vhodnej rade predvídať rozsah, ktorý je vzhľadom na okolnosti primeraný, a následky, ktoré môže dané konanie spôsobiť.[22]

3. Zásada legitimity

Podľa rozhodovacej činnosti Európskeho súdu pre ľudské práva predmetom skúmania **legitimity zásahu** do práva na súkromie je posúdenie, či opatrenie umožňujúce zásah verejnej moci do tohto práva zodpovedalo niektorému z cieľov taxatívne uvedených v Dohovore. Konkrétne to znamená, že tieto zásahy sa môžu uplatniť len v prípadoch a okolnostiach, ktoré vyplývajú z článku 8 ods. 2 Dohovoru, keďže Ústava výslovne neuvádza prípady, kedy je zásah do práva na súkromie legitímny. Z uvedeného článku Dohovoru vyplýva, že zásah do práva na súkromie je prípustný len vtedy, 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 konštatovať, že ide o relatívne široké spektrum dôvodov pre oprávnený zásah do práva na súkromia. Rozhodovacia činnosť Európskeho súdu pre ľudské práva pri obmedzovaní toh-

[16] Špaček v. Česko z 9. novembra 1999.
[17] Kopp v. Švajčiarsko z 25. marca 1998.
[18] I. ÚS 117/07, III. ÚS 68/2010 a II. ÚS 96/2010.
[19] Klass a ostatní v. Nemecko zo 6. septembra 1978.
[20] Malone v. Spojené kráľovstvo z 2. augusta 2004.
[21] Amann v. Švajčiarsko zo 16. februára 2000, Rotaru v. Rumunsko zo 4. mája 2000.
[22] Olsson v. Švédsko z 12. marca 1988.

to práva prísne limituje podmienky prípustnosti (použiteľnosti) dôkazov získaných obmedzením súkromia a aprobuje len postupy dávajúce dostatočné záruky ochrany základných práv napr. proti ľubovôli, či zneužitiu, pretože v opačnom prípade je vďaka dnešným technologickým možnostiam v stávke samotná demokracia.[23]

Obmedzenie základných práv a slobôd musí okrem iného spĺňať aj limit vzájomnej kolízie týchto práv (t. j. je potrebné ustanoviť kritériá, ktoré určia prioritu jedného práva pred druhým) a legitímny cieľ (t. j. istý verejný záujem na obmedzení). Z hľadiska legitimity zásahu do práva na súkromie sem možno zaradiť predovšetkým nevyhnutnosť danú verejným (všeobecným) záujmom na ochrane spoločnosti pred trestnými činmi a na tom, aby tieto trestné činy boli zistené a ich páchatelia spravodlivo potrestaní.[24] Sledovaný verejný záujem musí byť dostatočne závažný, aby prevážil záujem jednotlivca na nezasahovaní do jeho práv chránených v článku 8 ods. 1 Dohovoru. V iných prípadoch orgán verejnej moci je povinný zdržať sa akýchkoľvek zásahov do výkonu práva na rešpektovanie súkromia.[25]

4. Zásada proporcionality

Zásada proporcionality zásahu do práva na súkromie sa vyvinula na základe najmä súdnej praxe, ktorá ju všeobecne akceptuje. Proporcionalita zásahov do práva na súkromie sa prejavuje v hľadaní a dodržiavaní určitej rovnováhy medzi právami, ktoré sú k dispozícii, a možnosťami výberu konkrétnych prostriedkov smerujúcich k naplneniu sledovaného (legitímneho) cieľa.[26] Pri výbere prostriedkov, verejná moc je limitovaná tým, že zásah do práva na súkromie je možný len vtedy, keď je to nevyhnutné (sledovaný cieľ nemožno dosiahnuť miernejšími prostriedkami), a vykonať ho možno len v duchu požiadaviek kladených na demokratickú spoločnosť vyznačujúcu sa pluralizmom, toleranciou a voľným duchom. Z týchto dôvodov zásah do tohto práva musí zodpovedať naliehavej spoločenskej potrebe a musí byť primeraný sledovanému legitímnemu cieľu a zároveň pri určovaní rozsahu obmedzenia je dôležité zohľadniť podstatu práva, ktoré sa má obmedziť.[27] Preto je vždy dôležité starostlivo zvažovať, ako je zásah intenzívny.[28]

Posúdenie prípustnosti zásahu do súkromnej sféry jednotlivca z hľadiska proporcionality (v širšom slova zmysle) zahŕňa posúdenie:

a) spôsobilosti (vhodnosti),
b) potrebnosti,
c) primeranosti (v užšom zmysle),
d) minimalizácie obmedzenia základného práva.[29]

Pri posúdení **spôsobilosti (vhodnosti)** konkrétneho opatrenia k naplneniu účelu je zisťované, či konkrétne opatrenie je vôbec schopné dosiahnuť sledovaného legitímneho cieľa, ktorým je ochrana iného základného práva, slobody alebo verejného statku (úžitku).[30]

---

[23] Klass a ostatní v. Nemecko zo 6. septembra 1978. Gillan a Quintonová v. Spojené kráľovstvo z 12. januára 2000.

[24] ČENTÉŠ, J. – LAZAREVA, N.: Legalita, legitimita a proporcionalita odpočúvania a zaznamenávania telekomunikačnej prevádzky. In: 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 dňa 19. januára 2012, Fakulta práva Paneurópskej vysokej školy, Bratislava, s. 184.

[25] Primerane pozri I. ÚS 117/07.

[26] ZÁHORA, J. et al.: Obrazové a zvukové záznamy v trestnom konaní. Wolters Kluwer, Bratislava, 2018, s. 23.

[27] I. ÚS 13/00 a III. ÚS 68/2010.

[28] S. a Marper v. Spojené kráľovstvo zo 4. decembra 2008.

[29] ČENTÉŠ, J.: Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. Bratislava: C. H. Beck, 2013, s. 45.

[30] KYJAC, Z.: Použitie informačno-technických prostriedkov v trestnom konaní. Odpočúvanie a záznam telekomunikačnej prevádzky: Wolters Kluwer, Bratislava, 2015, s. 87 a nasl.

Naplnenie proporcionality podľa názoru Ústavného súdu *„vyžaduje primeraný vzťah medzi cieľom (účelom) sledovaným verejnou mocou a použitými opatreniami (prostriedkami). V týchto súvislostiach cieľ (účel) sledovaný verejnou mocou smie byť sledovaný; prostriedky, ktoré verejná moc použije, smú byť použité; použitie prostriedkov na dosiahnutie účelu je vhodné; použitie prostriedkov na dosiahnutie účelu je potrebné a nevyhnutné. Kritérium vhodnosti znamená, že stav, ktorý verejná moc vytvorí zásahom do práva na súkromie, a stav, v ktorom treba sledovaný cieľ vidieť ako uskutočnený, sa nachádzajú vo vzájomnej súvislosti; cieľ musí byť v súlade s použitými prostriedkami. Nevyhnutnosť znamená, že neexistuje iný stav, ktorý štát bez veľkej námahy môže rovnako vytvoriť, ktorý jednotlivca – fyzickú osobu zaťažuje menej a ktorý súvisí so stavom, v ktorom treba sledovaný účel pokladať za uskutočnený. Inými slovami, cieľ nesmie byť dosiahnuteľný rovnako účinným, ale menej zaťažujúcim prostriedkom.“*[31]

Výber prostriedkov pri zásahoch štátu do práva na súkromie je ponechaný na voľnú úvahu orgánu verejnej moci, avšak pri dodržaní limitov spočívajúcich v nevyhnutnosti daných zásahov a v dodržaní princípov a zásad vlastných demokratickej spoločnosti.[32] Pojem „nevyhnutnosti“ v sebe zahŕňa naliehavú spoločenskú potrebu; použité opatrenie musí byť okrem toho primerané povahe legitímneho účelu. Navyše, rozsah obmedzenia použitý verejnou mocou má závisieť nielen od cieľa sledovaného obmedzením, ale aj od druhu obmedzovaného práva; teda či bol nevyhnutný v demokratickej spoločnosti vo vzťahu k jednému alebo viacerým legitímnym cieľom uvedeným v článku 8 ods. 2 Dohovoru. Výsledok posúdenia vzťahu primeranosti medzi namietaným zásahom a sledovanými legitímnymi cieľmi bude závisieť od zistenia, či zásah spočíval v relevantných a dostatočných dôvodoch.[33]

K formulácii *„nevyhnutný v demokratickej spoločnosti“* zaujal názor Ústavný súd, podľa ktorého ju *„možno vysvetliť ako naliehavú spoločenskú potrebu prijať obmedzenie základného práva alebo slobody. Obmedzenie práv a slobôd je nevyhnutné, keď možno konštatovať, že cieľ obmedzenia inak dosiahnuť nemožno. Predpokladom je, že obmedzenie je nutné aj v demokratickej spoločnosti.“*[34] Podľa Európskeho súdu pre ľudské práva slovo „nevyhnutnosť“ znamená, že *„existuje donucujúca spoločenská potreba, že potrebné opatrenia s oprávneným cieľom sa musia uplatniť.“*[35]

Možno zvýrazniť, že odpočúvanie je závažným zásahom do základných práv a slobôd. Z tohto dôvodu je potrebné vziať do úvahy procesné záruky dostupné pre jednotlivca ustanovené vo vnútroštátnej právnej úprave ochrany jeho práv. Pri tomto zásahu je potrebné postupovať v trestnom konaní v súlade so **zásadou primeranosti a zdržanlivosti** (§ 2 ods. 2 Trestného poriadku) podľa ktorej *„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.“*.[36]

Formuláciou tejto základnej zásady zákonodarca sledoval cieľ, ktorým je obmedziť na najnutnejšiu mieru zásahy do ľudských práv a slobôd jednotlivca. Aplikovať možno jednotlivé ustanovenia Trestného poriadku umožňujúce zásah do základných ľudských práv a slobôd primerane, len v miere nevyhnutnej na dosiahnutie účelu trestného konania, zistenia skutkového stavu veci a zabezpečenia dôkazov. Zakotvenie tejto zásady je výrazom humánnosti trestného konania

[31] PL. ÚS 13/2000.
[32] I. ÚS 274/05.
[33] Gillow v. Spojené kráľovstvo z 24. novembra 1986. Pozri aj W. v. Spojené kráľovstvo z 8. júla 1987, A. B. a C. v. Írsko zo 16. decembra 2010.
[34] I. ÚS 33/95 a PL. ÚS 15/98.
[35] Gillow v. Spojené kráľovstvo z 24. novembra 1986.
[36] ČENTÉŠ, Jozef, et al. Trestný poriadok – Veľký komentár. 3. aktualizované vydanie. Eurokódex, Bratislava, 2017. s. 4.

a úcty k základným právam a slobodám.[37] Osobitne je táto zásada ustanovená aj vo všeobecnom ustanovení týkajúceho sa úkonov v trestnom konaní (§ 55 ods. 1 Trestného poriadku): *„Pri vykonávaní úkonov trestného konania musia orgány činné v trestnom konaní, súd a osoby príslušné vykonávať úkony trestného konania zaobchádzať s osobami zúčastnenými na úkone tak, ako to vyžaduje účel trestného konania; vždy sa musí rešpektovať ich dôstojnosť a ich ústavou zaručené základné práva a slobody,"*, ako aj úpravou podmienok na vydanie príkazu na odpočúvanie a záznam telekomunikačnej prevádzky (§ 115 ods. 1 druhá veta Trestného poriadku): *„Príkaz možno vydať, ak nemožno sledovaný účel dosiahnuť inak alebo ak by bolo jeho dosiahnutie iným spôsobom podstatne sťažené" (primerane pozri § 116 ods. 1 druhá veta Trestného poriadku – pozn. autora).*

Zároveň treba mať na zreteli, že všetky základné práva a slobody sa chránia len v takej miere a rozsahu, dokiaľ uplatnením jedného práva alebo slobody nedôjde k neprimeranému obmedzeniu, či popretiu iného práva alebo slobody.

Európsky súd pre ľudské práva v záujme rešpektovania proporcionality zásahu zdôraznil potrebu selektovať z viacerých dostupných možností pre dosiahnutie cieľa možnosť primerane zaručujúcu potrebnú rovnováhu medzi právom jednotlivca na ochranu súkromia a záujmami štátu.[38] Z týchto dôvodov v prípade proporcionality treba zvažovať použitie najšetrnejšieho prostriedku vo vzťahu k zásahu do práva na súkromie (zásada potrebnosti). Posúdenie potrebnosti sleduje analýzu plurality možných normatívnych prostriedkov vo vzťahu k zamýšľanému účelu a ich subsidiaritu z hľadiska obmedzenia Ústavou chránenej hodnoty – základného práva, alebo verejného statku. Ak možno zákonodarcom sledovaného účelu dosiahnuť alternatívnymi normatívnymi prostriedkami je potom ústavne konformný ten, ktorý danú ústavne chránenú hodnotu obmedzuje v miere najmenšej.[39]

V relácii k výkladu ustanovení Dohovoru sa proporcionalita používa ako interpretačný nástroj na obmedzenie právomoci orgánov verejnej moci a na poskytnutie väčšej ochrany autonómie fyzickej osoby. Obdobne podľa Ústavného súdu pri rešpektovaní proporcionality sa vyžaduje, aby sa (...) *„k zásahu prikročilo len vtedy, keď je to nevyhnutné (sledovaný cieľ nemožno dosiahnuť miernejšími prostriedkami) a iba v duchu požiadaviek kladených na demokratickú spoločnosť vyznačujúcu sa pluralizmom, toleranciou a voľným duchom. Výber prostriedkov pri týchto zásahoch štátu do práva na súkromie je ponechaný na voľnú úvahu orgánu verejnej moci, avšak za podmienky dodržania limitov spočívajúcich v nevyhnutnosti daných zásahov a v dodržaní princípov a zásad vlastných demokratickej spoločnosti."*[40]

Posúdenie **primeranosti** (v užšom zmysle), t. j. či ujma na základnom práve nie je neprimeraná vo väzbe na zamýšľaný cieľ, znamená, že opatrenia obmedzujúce základné práva a slobody nesmú, ak ide o kolíziu základného práva či slobody s verejným záujmom, svojimi negatívami dôsledkami prevyšovať pozitíva, ktoré predstavuje verejný záujem na týchto opatreniach.[41] Nevyhnutným predpokladom posúdenia primeranosti je pomerovanie porovnanie) kolízii stojacích ústavných hodnôt. Obsahom tohto pomerovania je posúdenie empirických, systémových, kontextových i hodnotových argumentov. Empirickým argumentom možno chápať faktickú závažnosť javu, ktorý je spojený s ochranou určitého základného práva, resp. verejného dobra;

[37] ČENTÉŠ, J. a kol.: Trestné právo procesné. Všeobecná časť. Šamorín: Heuréka, 2016, s. 59.

[38] Peck v. Spojené kráľovstvo z 28. januára 2003.

[39] MUSIL, J. – ŠVESTKA, J. – HOLLANDER, P.: Bezpečnostní výzvy a omezení základních práv v postmoderní realitě. Právní aspekty situace po 11. září 2011, Masarykova univerzita v Brně, Mezinárodní politologický ústav, Brno, 2002, s. 104 – 105.

[40] Primerane pozri III. ÚS 80/08 a I. ÚS 274/05. Pozri aj Klass a ostaní v. Nemecko zo 6. septembra 1978 a II. ÚS ČR 615/06.

[41] Pl. ÚS ČR 4/94, Pl. ÚS ČR 41/02.

systémový argument znamená zvažovanie zmyslu a zaradenie dotknutého základného práva či slobody v systéme základných práv a slobôd, kontextovým argumentom možno rozumieť ďalšie negatívne dopady obmedzenia jedného základného práva v dôsledku uprednostnenia iného; hodnotový argument predstavuje zvažovanie pozitív v kolízii stojacich základných práv, resp. verejného dobra vzhľadom k akceptovanej hierarchii hodnôt. Poslednou okolnosťou posúdenia prípustnosti zásahu o opodstatnenosti priority verejného dobra pred kolíziou s ním stojacim základným právom je nutnou podmienkou rozhodnutia rovnako využitie všetkých možností minimalizácie obmedzenia tohto základného práva.

Rovnováha verejného záujmu a súkromného záujmu je dôležitým kritériom pre určovanie primeranosti obmedzenia každého základného práva alebo slobody.[42] Podľa názoru Európskeho súdu pre ľudské práva požiadavka primeranosti vyžaduje, aby verejná moc preukázala relevantné a dostatočné dôvody na zásah. V konkrétnej veci Európsky súd pre ľudské práva pri posudzovaní proporcionality zásadu do práv sťažovateľa na súkromie vzal do úvahy obmedzenosť tohto zásahu (odpočúvanie jedného telefónneho hovoru), ktorý mal dostatočný právny základ (§ 88 českého Trestného poriadku), a na druhej strane sledovaný verejný záujem (boj s úplatkárstvom v najvyššej národnej futbalovej súťaži) posúdil ako značný.[43]

Požiadavky, ktoré zo zásady proporcionality vyplývajú dopadajú v prvom rade na demokratického zákonodarcu. V oblasti aplikácie práva dopadajú potom na celú oblasť judiciálnu aj správnu a konečne dopadajú, ako ultima ratio, aj na ústavný prieskum normatívnych i individuálnych právnych aktov Ústavným súdom. Nutnou podmienkou je taktiež využitie všetkých možností minimalizácie obmedzenia práva na súkromie.[44]

Možno zvýrazniť, že aj keď je na vnútroštátnych orgánoch, aby uskutočnili úvodné posúdenie vo všetkých týchto hľadísk a pri tomto posúdení musí byť kompetentným vnútroštátnym orgánom ponechaná určitá miera voľnej úvahy, konečné zhodnotenie toho, či je zásah nevyhnutný na účely jeho súladu s požiadavkami Dohovoru podlieha kontrole zo strany Európskeho súdu pre ľudské práva.[45]

5. Záver

Zásah orgánu verejnej moci do práva na súkromie pri odpočúvaní telefonického hovoru musí byť predvídateľný zákonom, ktorý pre dosiahnutie svojho účelu musí voliť čo najšetrnejšie prostriedky. Zo strany orgánu verejnej moci je prípustný len taký zásah do práva na súkromie pri odpočúvaní, ktorý je legálny (zákonný), legitímny a proporcionálny. Predpokladom naplnenia týchto kritérií je aj existencia systému primeraných a účinných záruk, ktoré sa skladajú najmä zo zodpovedajúcich právnych predpisov a účinnej kontroly ich dodržiavania.

Literatúra

ČENTÉŠ, J. – LAZAREVA, N.: Legalita, legitimita a proporcionalita odpočúvania a zaznamenávania telekomunikačnej prevádzky. In: Zborník príspevkov z celoštátnej konferencie s medzinárodnou účasťou „Aktuálne otázky trestného zákonodarstva“ – pocta akademikovi, Dr. h. c. prof. JUDr. Milanovi Čičovi, DrSc.

[42] PL. ÚS 7/96.

[43] Pastyřík v. Česko z 31. mája 2011.

[44] MUSIL, J. – ŠVESTKA, J. – HOLLANDER, P.: Bezpečnostní výzvy a omezení základních práv v postmoderní realitě. Právní aspekty situace po 11. září 2011, Masarykova univerzita v Brně, Mezinárodní politologický ústav, Brno, 2002, s. 104 – 105. Primerane pozri Pl. ÚS ČR 3/02.

[45] Coster v. Spojené kráľovstvo z 18. januára 2001.

k 80. narodeninám, s. 183 – 198, konanej dňa 19. januára 2012, Fakulta práva Paneurópskej vysokej školy, Bratislava.

ČENTÉŠ, J.: Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. Bratislava: C. H. Beck, 2013, 245 s.

ČENTÉŠ, J. a kol.: Trestné právo procesné. Všeobecná časť. 2. vydanie. Šamorín: Heuréka, 2016, 438 s.

ČENTÉŠ, Jozef, et al.: *Trestný poriadok – Veľký komentár.* 3. aktualizované vydanie. Eurokódex, Bratislava, 2017, 971 s.

KYJAC, Z.: Použitie informačno-technických prostriedkov v trestnom konaní. Odpočúvanie a záznam telekomunikačnej prevádzky. Bratislava: Wolters Kluwer, 2015, 307 s.

MUSIL, J. – ŠVESTKA, J. – HOLLANDER, P.: Bezpečnostní výzvy a omezení základních práv v postmoderní realitě. Právní aspekty situace po 11. září 2011, Masarykova univerzita v Brně, Mezinárodní politologický ústav, Brno, 2002, s. 104 – 105.

ZÁHORA, J.: Uchovanie počítačových údajov a ochrana súkromia. In: Justičná revue, r. 63, 2011, č. 6–7, s. 904 – 913.

ZÁHORA, J. et al.: Obrazové a zvukové záznamy v trestnom konaní. Wolters Kluwer, Bratislava, 2018, 268 s.

Záznam z autokamery ako dôkaz v trestnom konaní[1]

Vehicle Camera Record as the Proof in Criminal Proceedings

Jaroslav Ivor[2]
Eduard Kolla[3]

Abstrakt: *Príspevok analyzuje využitie záznamu z autokamery ako dôkazu v trestnom konaní najmä z pohľadu aktuálnej právnej úpravy: GDPR, Trestný poriadok, Zákon o ochrane osobných údajov, Občiansky zákonník, ktoré určujú podmienky použitia a využitia kamerových informačných systémov. Konštatuje sa absencia špeciálnej právnej úpravy, takže je nevyhnutné pre aplikáciu použiť zásadu účelnosti a zásadu proporcionality. Zároveň sa prezentuje konštrukcia digitálnych vozidlových kamier, jej optický systém a technická stránka využitia záznamu z vozidlových kamier pri rekonštrukcii a analýze dopravných situácií*

Abstract*: The paper analyzes the use of vehicle camera as the proof in criminal proceedings especially from the point of current legal framework: GDPR, Penal Code, The Personal Data Protection Act, Civil Code, which provide the conditions foe the use of the camera information systems. It states the absence of special legal framework, so it is necessary for the application to use the principle of efficiency and the proportionality principle. At the same time what is presented is the the equipment of the digital vehicle cameras, their optical system and technical matters to be used for reconstruction and analysis of traffic situations.*

Kľúčové slová*: autokamera, kamerový systém, GDPR, dôkaz v trestnom konaní, princíp účelnosti, princíp proporcionality, optický záznam, technická rekonštrukcia dopravnej nehody*

Key words*: vehicle camera, camera system, GDPR, the proof in criminal proceedings, principle of efficiency, the principle of proportionality, optical recording, technical reconstruction of traffic accident*

Slovenský Trestný poriadok obsahuje demonštratívny výpočet dôkazných prostriedkov. Od antiky až po súčasnosť základným a najfrekventovanejším dôkazom je nepochybne výpoveď svedka, ktorý má mimoriadny význam pre rozhodnutie vo veci. V trestnoprávnej, ako i kriminalistickej teórii existuje množstvo vymedzení pojmu svedok. Pre naše účely postačí vymedzenie, že je to fyzická osoba, ktorá vnímala okolnosti dôležité pre trestné konanie vlastnými zmyslami (zrak, sluch, čuch, hmat, či chuť) pričom je dôležitá jej schopnosť vnímať, zapamätávať a vypovedať o tom, čo vnímala. Z kriminalistického pohľadu ide v tomto procese o vznik tzv. pamäťových stôp. Teda ako už bolo povedané, zásadný význam má schopnosť vnímania, fixovania, vybavovania a reprodukovania informácií, ktoré sú obsahom pamäťovej stopy. Na pamäťové stopy pôsobí množstvo vplyvov nezávisle od vôle človeka. Je to najmä prostredie, inteligencia, strach, schopnosť zapamätania, zdravotný stav a podobne. Pamäťové stopy sú nedostupné, pokiaľ konkrétna osoba nechce alebo nemôže oznámiť ich obsah, pričom sú definitívne stratené, pokiaľ daná osoba zomrie.

V posledných rokoch je zaznamenávaná u svedkov tendencia z najrôznejších subjektívnych a objektívnych príčin vyhýbať sa svojej zákonnej povinnosti dostaviť sa na výsluch a vypovedať pravdivo o tom, čo mu je známe o trestnom čine, o jeho páchateľovi alebo iných okolnostiach dôležitých pre trestné konanie.

---

[1] Táto práca je podporovaná Agentúrou na podporu výskumu a vývoja na základe zmluvy č. APVV-15-0272.
[2] Dr. h. c. prof. JUDr. Jaroslav Ivor, DrSc., Právnická fakulta UMB Banská Bystrica.
[3] Ing. Eduard Kolla, PhD., Ústav znaleckého výskumu a vzdelávania, Žilinská univerzita v Žiline.

Okrem toho páchanie kriminality v posledných desaťročiach je charakteristické i prejavmi vyplývajúcimi z dynamiky trestnej činnosti Sú to úplne nové druhy kriminality, ktoré vo všetkých krajinách vyvolávajú úsilie po reformách trestnoprocesných predpisov, ktorých obsahom je zavádzanie nových dôkazných prostriedkov, ktoré sú podmienené i rozvojom vedy, techniky a informačných technológií. Nové fenomény zločinnosti predstavujú pre štát mimoriadne silného protivníka, proti ktorému sa doterajšie „tradičné" dôkazné prostriedky policajnej a justičnej práce ukazujú ako príliš mierne a málo efektívne. Trestné konanie musí v mnohých prípadoch prekonávať závažnú prekážku, ktorou sa často stáva stav tzv. dôkaznej núdze.

Rekodifikácia slovenského trestného práva priniesla v tomto smere okrem iného rozšírenie škály demonštratívne vypočítaných dôkazných prostriedkov podľa § 119 ods. 2 Tr. por. o nové, dovtedy typické kriminalistické úkony, ale najmä prípustnosť dôkazu získaného nielen podľa trestného poriadku, ale aj z dôkazného prostriedku podľa osobitného zákona. Takýmto dôkazom je i záznam získaný z monitorovania kamerovým systémom. Kamerový systém, ktorý už svojou inštaláciou pôsobí zároveň preventívne a záznam z neho získaný, poskytujúci informácie o trestnej činnosti najrôznejšieho druhu, sa stáva čoraz frekventovanejším technickým dôkazom i v aplikačnej trestnoprocesnej praxi. Pre označenie záznamu z kamerového systému získaného monitorovaním kriminálne relevantnej udalosti sa preto môže s určitou nadsázkou použiť výraz „nemý svedok".

Aj tento „technický" dôkaz však musí spĺňať všeobecné pravidlá prípustnosti a zákonnosti dôkazu.

Pri hodnotení dôkazov v trestnom konaní priznáva hodnotiaci subjekt každému dôkazu určitú hodnotu z hľadiska jeho prípustnosti, závažnosti a vierohodnosti (pravdivosti). Prípustnosť dôkazov sa označuje aj ako zákonnosť dôkazov. Súčasný Trestný poriadok používa iba termín zákonnosť (§ 2 ods. 12, § 119 ods. 2, § 243 ods. 2). Zákonnosť znamená, že určitý dôkazný prostriedok je prípustný podľa zákona a bol získaný postupom, ktorý je v súlade s právnymi predpismi. Za dôkaz získaný nezákonným spôsobom sa považuje nielen dôkaz, pri ktorom bola nezákonnosť spôsobená, ale aj každý dôkaz získaný na základe takéhoto dôkazu.[4]

V tejto súvislosti sa žiada uviesť niekoľko informácií o podstate, obsahu a vývoji kamerového systému vo všeobecnosti.

Kamerový systém (CCTV – Closed Circuit Television, uzavretý televízny okruh) je využitie kamier na sledovanie priestorov, na zobrazovanie záberov z kamier na monitoroch a archiváciu natočených záberov. Skladá sa z kamier, hardwarového vybavenia a softwaru. Môže byť doplnený aj o mikrofóny, reproduktory a takmer vždy o záznamové médium pre ukladanie zaznamenaných dát. Väčší rozmach kamerového systému vo svete bol zaznamenaný po roku 1980, po roku 2010 sa stal kvalitný kamerový systém i cenovo dostupný pre široké vrstvy obyvateľstva.

Z pohľadu práva pri prevádzkovaní kamerového systému dochádza k spracúvaniu osobných údajov prostredníctvom snímacích zariadení (kamier), ako prostriedkov spracúvania. Osobnými údajmi vo všeobecnosti rozumieme akékoľvek charakteristiky alebo údaje fyzickej osoby, ktoré sú spôsobilé ju určiť a odlíšiť od ostatných osôb. V tomto prípade ide predovšetkým o tvár snímanej osoby, ako i ďalšie biometrické údaje viažúce sa k tejto osobe.

Kamerové systémy zaznamenali za posledné desaťročia prudký rozvoj a to nielen z pohľadu technického, ale i legislatívneho a to najmä s ohľadom na jeho opodstatnenosť, legálnosť a ochranu osobných údajov 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 slovenská právna úprava s ňou bola plne kompatibilná.

[4] Záhora, J. a kol.: Dokazovanie v trestnom konaní. 1. vydanie. Praha: Leges 2013, s. 114.

Prvý slovenský zákon o ochrane osobných údajov (č. 428/2002 Z. z.) medzi osobitné spôsoby získavania osobných údajov podľa § 10 ods. 7 zaradil i monitorovanie osôb v priestore prístupnom verejnosti. Ďalší zákon č. 122/2013 Z. z. okrem iného precizoval inštitút monitorovania prostredníctvom kamerového systému najmä v ustanovení § 15 ods. 7 citovaného zákona.

Zásadná zmena v právnej úprave ochrany osobných údajov nastala v roku 2018, keď dňom 25. 5. 2018 nadobudlo účinnosť v celej EÚ Nariadenie Európskeho parlamentu a Rady 2016/679, ktoré sa prezentuje pod skratkou GDPR (General Data Protection Regulation). Od 25. 5. 2018 je aj na Slovensku účinný nový zákon o ochrane osobných údajov č. 18/2018 Z. z. Okrem iného chcem z GDPR vyzdvihnúť obsah čl. 6, podľa ktorého v prípade monitorovania kamerovým systém sa nesmie **neprimerane** zasahovať do súkromia osôb a tieto zásahy musia byť **primerané** účelu použitia. Slovenský zákon č. 128/2018 Z. z. z veľkej časti iba kopíruje európsku legislatívu, ba naopak vypustil úpravu o monitorovaní kamerovým systémom (s výnimkou všeobecného ustanovenia § 42 ods. 3 písm. c) o využití tohto záznamu ako dôkazu v trestnom konaní, tak ako tomu bolo v predchádzajúcich dvoch zákonoch. Vzhľadom na neustále sa rozširujúci trend využívania kamerových systémov u nás by si táto problematika vyžadovala exaktnejšie a detailnejšie spracovanie.

Slovenská právna úprava však obsahuje viacero ďalších právnych noriem upravujúcich vyhotovovanie obrazových záznamov v súvislosti s ochranou osobných údajov ako napr. Občiansky zákonník (§ 11 až 16), Trestný poriadok (§ 113, 114), Zákon č. 166/2003 Z. z. o ochrane súkromia pred odpočúvaním, Zákonník práce (§ 13 ods. 4), Zákon č. 221/2006 Z. z. o výkone väzby, Zákon č. 483/2001 Z. z. o bankách, Zákon č. 1/2014 Z. z. o organizovaní verejných športových podujatí, aj prostredníctvom využívania kamerových systémov v rôznych špecifických situáciách a pri rôznych podmienkach a režime ich použitia.

Z technického hľadiska ide predovšetkým o tzv. stacionárne kamerové systémy. Tak ako v mnohých iných prípadoch, aj pri využívaní kamerových systémov technický vývoj neustále predbieha legislatívnu úpravu, ktorá v tomto zmysle najmä na Slovensku zaostáva. Osobitne mám na mysli špeciálnu problematiku používania kamerových systémov v automobiloch a využívanie záznamov z ich prevádzky či už v trestnom resp. i priestupkovom konaní ako dôkaz.

Možno súhlasiť so záverom, že Zákon o ochrane osobných údajov ani iný ďalší zákon priamo neupravuje problematiku autokamier.

Úrad na ochranu osobných údajov sa v minulosti snažil vyriešiť tento problém vydaním metodického usmernenia, avšak toto nemá právnu silu zákonnej normy.[5]

S určitou nadsázkou možno na úvod povedať, že autokamera vo vozidle je akýsi tichý spolujazdec a v prípade akejkoľvek kolízie, ktorá môže byť priestupkom alebo trestným činom je zároveň „nemým svedkom". Základnou funkciou autokamery je permanentne monitorovať situáciu pred vozidlom počas jazdy, v niektorých prípadoch i vo vozidle či za vozidlom a vyhotovovať z tejto činnosti príslušný obrazový záznam, ktorý je objektívny, korektný a nespochybniteľný.

Autokamery monitorujú situáciu a udalosti v cestnej premávke, avšak ani Zákon č. 8/2009 Z. z. o cestnej premávke ani Zákon č. 106/2018 Z. z. o prevádzke vozidiel v cestnej premávke vôbec neupravujú problematiku umiestnenia či prevádzku autokamier a využitia záznamov z jej činnosti. Autokamery sa zvyčajne umiestňujú na čelnom skle automobilu resp. na palubnej doske vodiča. Z tohto pohľadu sa umiestnenia autokamery dotýka ustanovenie § 4 ods. 1 písm. i zákona o cestnej premávke, podľa ktorého medzi základné povinnosti vodiča patrí zabezpečiť, aby sa vo výhľadovom poli vodiča nenachádzali premety, ktoré môžu odvádzať po-

[5] Metodické usmernenie č. 3/2013: Kamerové informačné systémy osobných údajov vo vozidlách č. 00063/2016-Op-4.

zornosť od bezpečného vedenia vozidla. Obdobne v metodickom pokyne ministerstva dopravy č. 50/2018 k zákonu o prevádzke vozidiel v cestnej premávke sa uvádza, že „v zornom poli vodiča nesmú byť umiestnené žiadne predmety, ktoré obmedzujú výhľad vodiča všetkými smermi, okrem schválených spätných zrkadiel, označení na umiestnenie na skle vozidla (diaľničné známky, kontrolná nálepka technickej a emisnej kontroly alebo kontroly originality). Teda napríklad navigačné zariadenia či iné technické zariadenia (ako i autokamery) musia z hľadiska umiestnenia spĺňať uvedenú požiadavku, čo však nie je nerealizovateľné. Treba však uviesť poznámku, že pojem „zorné pole" resp. „výhľadové pole" nie je nikde definovaný a stotožňovať ho s pojmom „stieraná plocha" nie je presné a identické.

Inštalácia a prevádzka autokamery je motivovaná najmä ochranou majetku a súvisiacimi právami a povinnosťami vznikajúcimi v podmienkach premávky na pozemných komunikáciách. Účelom vyhotovovania obrazového záznamu z autokamery je najmä získavanie dôkazov o mechanizme vzniku kriminálne relevantnej udalosti a tým aj zodpovednosti za túto udalosť, resp. za spôsobenú škodu alebo inú ujmu. V uvedenej súvislosti však nemožno opomenúť nevyhnutnú mieru náhodne získavaných osobných údajov, ktoré však účelu prevádzkovania autokamery nezodpovedajú.

Z tohto pohľadu treba používanie autokamier analyzovať prostredníctvom právnej úpravy, ktorá rieši ochranu osobných údajov resp. zásahy do osobných práv. Ide najmä o:

a) Nariadenie Európskeho parlamentu a Rady 2016/679 (GDPR) a Zákon o ochrane osobných údajov č. 18/2018 Z. z.
b) Občiansky zákonník (ust. § 11 až 16)
c) Zákonník práce (§ 13 ods. 4).

Autokamera je pojem, ktorý sa žiaľ nevyskytuje v žiadnej legislatívnej úprave, zaznamenávame ho iba v odbornej motoristickej literatúre. Autokameru môžeme vymedziť ako kamerový informačný systém motorového alebo bezmotorového vozidla tvorený kamerou so záznamovým zariadením (vyhotovovanie záznamov) a dátovým úložiskom (uchovávanie záznamov), ktoré spravidla tvoria kompaktný celok.

Vo vozidle je autokamera umiestňovaná spôsobom umožňujúcim monitorovanie situácie pred vozidlom, za vozidlom alebo v jeho interiéri. Navonok autokamera monitoruje vozidlo v premávke na pozemných komunikáciách, teda vyhotovuje záznamy z pohybujúceho sa alebo stojaceho (zaparkovaného) vozidla v priestore verejnosti prístupnom.

Monitorovanie interiéru vozidla sa môže vzťahovať na priestory verejnosti neprístupné (napr. interiér súkromného alebo služobného vozidla) alebo i na priestory prístupné verejnosti (napr. interiér vozidla taxislužby alebo interiér autobusu či trolejbusu). Autokamerou možno označiť i kamerový informačný systém koľajového vozidla, motocykla alebo bicykla.

Pri nepochybne užitočnom a z hľadiska riešenia možnej kolíznej situácie v cestnej premávke efektívneho monitorovania vozidla v premávke na pozemných komunikáciách však súčasne záznam z autokamery zachytáva i náhodných chodcov, vodičov či spolujazdcov iných vozidiel a podobne. V tomto zmysle teda záznam z autokamery okrem hlavného účelu jeho využitia, sekundárne spracúva i osobné údaje dotknutých osôb a je preto dôležité rešpektovať požiadavku neprípustnosti zverejňovania, sprístupňovania a poskytovania záznamu tretím stranám ako aj bezodkladná likvidácia podmienená splnením účelu prevádzky autokamery. Len pre upresnenie, záznam evidenčného čísla motorového vozidla netvorí osobný údaj, ktorý má príslušnú legislatívnu ochranu (čl. 4 ods. 1 GDPR).

Vo vzťahu k spracúvaniu údajov získaných prostredníctvom záznamu z autokamery je potrebné pripomenúť si základnú legislatívnu úpravu tejto problematiky. Na prvom mieste je potrebné prezentovať európske nariadenie o ochrane osobných údajov (GDPR), ktoré však vo svojom

čl. 2 ods. 1 písm. c uvádza, že „toto nariadenie sa nevzťahuje na spracúvanie osobných údajov fyzickou osobou v rámci výlučne osobnej alebo domácej činnosti". Citované nariadenia v čl. 4 podrobne vymedzuje a vykladá relevantné pojmy tohto nariadenia (celkom 26 ustanovení), avšak pojem „osobnej alebo domácej činnosti" tu absentuje. Podobe § 3 ods. 5 písm. a Zákona o ochrane osobných údajov č. 18/2018 Z. z. ustanovuje, že tento zákon sa nevzťahuje na spracúvanie osobných údajov fyzickou osobou v rámci výlučne osobnej alebo domácej činnosti. Teda v slovenskom zákone je iba doslovne prebrané ustanovenie z európskeho nariadenia a taktiež bez výkladu pojmu osobné alebo domáce činnosti.

Zastávam názor, že z hľadiska účelu využívanie záznamu z autokamery bude mať monitorovanie autokamerou umiestnenou v osobnom (služobnom) vozidle charakter osobnej činnosti, pretože je realizované výlučne pre osobnú potrebu majiteľa resp. prevádzkovateľa vozidla v záujme ochrany jeho majetku (vozidla), zdravia a života vodiča a ďalších prepravovaných resp. dotknutých osôb. Tento názor prezentoval vo svojom metodickom usmernení i Úrad na ochranu osobných údajov SR.[6] Z uvedeného vyplýva, že vyňatie prevádzkovania autokamery spod pôsobnosti GDPR a tiež zákona o ochrane osobných údajov je podmienené kumulatívnym splnením nasledujúcich podmienok:

a) autokameru prevádzkuje fyzická osoba,
b) autokamera je prevádzkovaná výlučne v režime osobných činností, čo v praxi znamená, že účelom získavania osobných údajov je ochrana práv a právom chránených záujmov fyzickej osoby, ktorá autokameru prevádzkuje, resp. priebežná dokumentácia situácie v bezprostrednej blízkosti vozidla (pred vozidlom, vo vozidle, za vozidlom) pre prípad potreby preukazovania mechanizmu vzniku dopravnej nehody alebo škodovej udalosti, preukazovania úmyselného či neúmyselného poškodenia parkujúceho vozidla, preukazovanie neoprávneného použitia alebo krádeže vozidla, prípadne iného incidentu v oblasti verejného poriadku a bezpečnosti a preukazovania zodpovednosti za škodu alebo ujmu spôsobenú týmito udalosťami,
c) uchovávanie vyhotovených záznamov zodpovedá priebežnému vyhotovovaniu dokumentácie v určitej časovej slučke (spravidla podľa kapacity úložiska), pričom doba uchovávania takto vyhotovených záznamov nesmie byť v zjavnom rozpore s účelom ich vyhotovenia; v uvedenej súvislosti možno za akceptovateľnú dobu uchovávania považovať maximálne 15 dní, tzn. záznamy nevyužité na účel uvedený v bode b) by mali byť v tejto lehote zlikvidované,
d) vyhotovené záznamy možno využiť len na účely uvedené v bode b) a okrem týchto prípadov nesmú byť sprístupnené alebo poskytnuté tretej strane a nesmú byť nijako zverejnené (napr. na sociálnych sieťach).

Aj pri používaní autokamier za naznačených podmienok v režime tzv. osobných činností však treba mať na pamäti, že záznam z autokamery môže obsahovať aj biometrické údaje (tváre) náhodných osôb vyskytujúcich sa v cestnej premávke. Podľa § 12 ods. 1 Občianskeho zákonníka „... obrazové snímky, obrazové a zvukové záznamy týkajúce sa fyzickej osoby alebo jej prejavov osobnej povahy sa smú vyhotoviť alebo použiť len s jej privolením". Podľa § 13 ods. 1 má fyzická osoba právo domáhať sa „aby sa upustilo od neoprávnených zásahov na ochranu jej osobnosti a aby sa odstránili následky týchto zásahov". V tejto súvislosti teda ani teoreticky ani prakticky nemožno vylúčiť konflikt dvoch záujmov, pričom aj bez ďalšej argumentácie možno vysloviť názor, že bude v zásade prevažovať záujem štátu na preukázaní spáchania trestného činu a usved-

[6] Metodické usmernenie č. 3/2013 Úradu na ochranu osobných údajov SR č. 00063/2016-0p-4, kamerové informačné systémy osobných údajov vo vozidlách.

čení páchateľa nad záujmom inej osoby (najmä páchateľa) na ochranu jeho osobných údajov a teda záznam z monitorovacieho systému bude využiteľný ako dôkaz v trestnom konaní.

Pri stanovení podmienok prevádzky autokamery a využiteľnosti záznamu z nej bude treba dôsledne uplatňovať zásadu účelu a zásadu proporcionality.

Monitorovanie kamerovým systémom za účelom ochrany majetku, zdravia a života nepochybne spĺňa svoj účel len vtedy, pokiaľ prevádzkovateľ autokamery vykonáva záznam za účelom vyhotovenia dôkazného materiálu, aby identifikoval zavinenie nehodovej udalosti a potenciálneho páchateľa 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.

Zásada proporcionality predstavuje posúdenie konfliktu dvoch záujmov. Právo na ochranu osobnosti, osobných údajov na jednej strane a ochrany majetku, zdravia a života prevádzkovateľa autokamery na strane druhej. Toto právo sa prelína i so záujmom spoločnosti na odhalení a potrestaní deliktuálneho konania.

Zásada proporcionality sa v judikatúre (napr. nález ÚS ČR I. ÚS 191/05) posudzuje pri napĺňaní troch kritérií:

- Kritérium vhodnosti určuje, či opatrenie obmedzujúce určité základné právo umožňuje dosiahnuť sledovaný cieľ. V tomto prípade možno priznať, že kamerový systém je prostriedkom, ktorý síce nedokáže zabrániť v dokonaní trestného činu, podstatou jeho činnosti je vyhotoviť záznam takéhoto konania, ktoré následne môže viesť k identifikácii páchateľa a eventuálne k potrestaniu.
- Kritérium potrebnosti porovnáva zvolený prostriedok s inými do úvahy prichádzajúcimi opatreniami. K nehode v cestnej premávke dôjde mnohokrát v extraviláne, bez svedkov, s problémami pri zabezpečení potrebných stôp, kde sa kamerový systém javí ako mimoriadne efektívny prostriedok dokazovania.
- Kritérium porovnania určuje závažnosť oboch v kolízii stojacich práv.

V súvislosti s využívaním autokamier je však potrebné spomenúť i odlišnú situáciu, ktorá nastáva v prípadoch monitorovania interiéru vozidla, v prípade, že je priestorom prístupným verejnosti. V tomto prípade sa totiž uplatňuje iný právny režim, používanie autokamery musí byť v súlade s ustanoveniami Zákona č. 18/2018 Z. z. o ochrane osobných údajov. Pôjde tu o prípady monitorovania interiéru autobusu, trolejbusu, vozidla taxislužby alebo železničného či električkového vagóna. V uvedenej súvislosti je žiadúce mať na zreteli najmä zákonom vymedzený účel spracúvania osobných údajov, splnenie povinnosti zreteľne označiť monitorovaný priestor, využitie vyhotovených záznamov výhradne na účely vymedzené zákonom a likvidácia ostatných (nevyužiteľných) záznamov. V tomto prípade zákon (za splnenia vymedzených podmienok), nepodmieňuje spracúvanie osobných údajov súhlasom dotknutých osôb. V súvislosti s povinnosťou označovať monitorovaný priestor treba poznamenať, že GDPR obsah označenia žiada rozšíriť (v zmysle zásady transparentnosti) aj o účel monitorovania, prevádzkovateľa kamerového systému a kontaktné osoby zodpovednej osoby s cieľom možnosti realizácie svojich práv u dotknutých osôb.

Vo vzťahu k autokamerám je kvôli úplnosti potrebné uviesť i monitorovanie realizované s uplatnením ustanovenia § 13 ods. 4 Zákonníka práce, teda monitorovanie zamestnancov z pozície zamestnávateľa, ktoré sú však spájané s existenciou vážnych dôvodov spočívajúcich v osobitnej povahe jeho činnosti, ako napríklad monitorovanie interiéru služobného vozidla zabezpečujúceho prevoz peňazí, pacientov a podobne.

Ako som už uviedol, výrazným posunom v dokazovaní bola rekodifikácia Slovenského trestného práva účinná od 1. 1. 2006 a to najmä nová úprava § 119 ods. 2 Tr. por., ktorá pripúšťa do konania nielen dôkazy získané z dôkazných prostriedkov podľa trestného poriadku, ale i podľa

osobitného zákona. Takýmto osobitným zákonom je i zákon na ochranu osobných údajov, ktorý vymedzuje zákonné podmienky monitorovania osôb kamerovým systémom. Aj keď špeciálna úprava kamerových systémov umiestnených a prevádzkovaných vo vozidlách (autokamery) absentuje, zastávam názor, že i aplikačná prax už skonštatovala výnimočnosť a efektívnosť využitia záznamov z autokamier v trestnom konaní.

I keď používanie kamerového systému vo vozidlách prudko rastie, firmy s elektronikou ponúkajú celé škály najrôznejších autokamier v rôznej kvalite a v rôznych cenových reláciách, inštalovať autokamery vo vozidle žiaľ v súčasnosti ešte nie je povinnosťou. Aký postup však možno predpokladať pri zaisťovaní záznamu z autokamery pre účely trestného konania:

1. Najčastejším spôsobom bude nepochybne iniciatívne predloženie takéhoto dôkazu orgánom činným v trestnom konaní stranou trestného konania resp. účastníkom dopravnej nehody.
2. Policajt môže požiadať o vydanie veci (záznamu) podľa § 89 ods. 1 Tr. por. Toto ustanovenie vyjadruje povinnosť občanov pomáhať dosiahnutiu účelu trestného konania. Takúto aktivitu však nemožno uplatňovať voči obvinenému, u ktorého treba rešpektovať princíp zákazu sebaobviňovania (nemo tenetur), rovnako tak nemožno postupovať proti osobe, proti ktorej možno dôvodne predpokladať trestné stíhanie.
3. V prípade odmietnutia dobrovoľného vydania veci (záznam z autokamery) je možné realizovať inštitút odňatia veci podľa § 91 ods. 1 Tr. por. Výnimočne v prípade dôvodnosti je možné využiť i inštitúty osobnej prehliadky, domovej prehliadky alebo prehliadky iných priestorov a pozemkov podľa § 99 Tr. por.

Obrazový záznam z autokamery však neposkytuje iba vizuálne zachytenie určitej kriminálne relevantnej udalosti v cestnej premávke. Poskytuje množstvo cenných informácií dôležitých pre trestné konanie najmä z pohľadu zachytenia originálnej situácie, ktorá predchádzala nehode, mechanizmu jej vzniku, jej bezprostrednej príčiny, následkov a ďalších okolností významných pre právne posúdenie nehody najmä z hľadiska zavinenia a kvalifikácie skutku, či už ako priestupku alebo trestného činu. Z tohto pohľadu obrazový záznam z autokamery a jeho podrobná technická analýza znalcom z odboru cestnej premávky je nezastupiteľným zdrojom využiteľných informácií. Z tohto titulu je veľmi vhodné doplniť úvahy o právnom vymedzení použitia a využitia záznamu z autokamery o technický pohľad na problematiku autokamier a možnosti využitia optického záznamu pre potrebu rekonštrukcie nehodového deja.

Použiteľnosť v minulosti najčastejšie používaných metód rekonštrukcie cestných dopravných nehôd je v súčasnej dobe obmedzená: absencia brzdných, alebo šmykových stôp sa stáva štandardom, presný odhad deformačnej energie pomocou syntetickej veličiny EES je viazaný na existenciu známej hodnoty deformačnej energie etalónového vozidla, vyťaženie poľa črepín neumožňuje relevantné určenie nárazovej rýchlosti, ale len oblasti miesta zrážky, apod. Na druhej strane použiteľnosť novej metódy rekonštrukcie DN extrakciou a analýzou nehodových a prednehodových dát zo záznamníka týchto dát (jednotka CDR) je stále obmedzená malou penetráciou trhu vozidlami vybavenými týmto systémom.

Technologický a technický pokrok má však za následok existenciu dodatočného zdroja relevantných informácií o dopravnej nehode – digitálneho videozáznamu zachyteného buď bezpečnostnou kamerou namontovanou v exteriéri a snímajúcou verejné priestory, alebo vozidlovou kamerou umiestnenou v interiéri určitého vozidla. Už z princípu vlastností optického snímania je zrejmé, že vyťaženie takýchto optických digitálnych stôp poskytuje oproti štandardným znaleckým metódam rekonštrukcie dopravných nehôd niekoľko výhod:

– Optický záznam umožňuje priamu rekonštrukciu dopravnej nehody, bez neistôt vyplývajúcich z nepriamych metód – analytik priamo vidí, k čomu pri nehode došlo, nespolieha sa

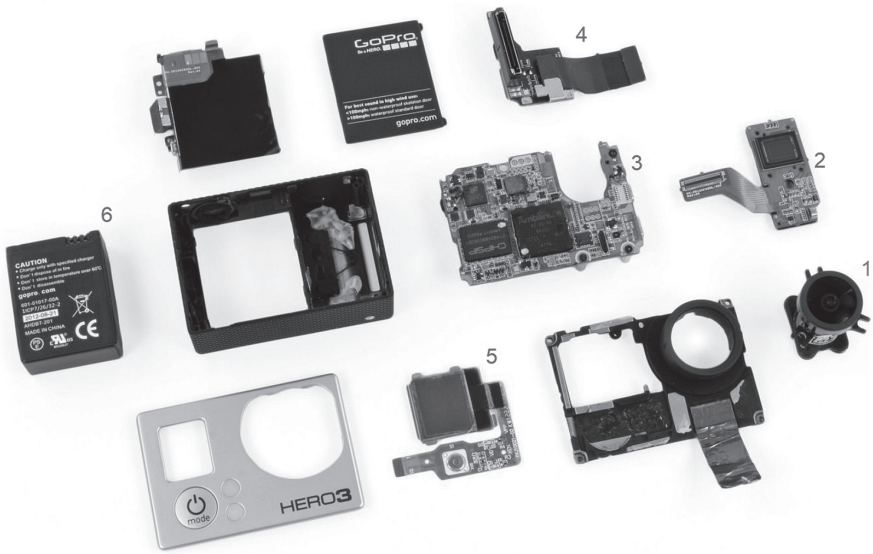
na spätné odvíjanie podmienené technicky prijateľným rozpätím vstupných parametrov (rekonštrukcia DN pomocou nepriamych metód umožňuje výpočet niekoľko technicky prijateľných variantov bez jednoznačnej istoty, ktorý z nich zodpovedal reálnemu deju).

- Optický záznam umožňuje vyťaženie nielen údajov o pohybe vozidla, ale poskytuje aj informáciu o pohybovom vzťahu účastníkov cestnej premávky, t. j. na rozdiel od iných metód umožňuje presnú synchronizáciu pohybu na zázname zachytených účastníkov cestnej premávky. Potom je teda následne možné presne analyzovať kauzalitu danej nehodovej situácie, resp. nekontaktnej, ale nebezpečnej situácie (tzv. near-miss incident).
- Optický záznam umožňuje presnú rekonštrukciu nepriamych stretov – t. j. kolíznych situácií pri ktorých nedošlo ku kontaktu dvoch vozidiel, resp. nekontaktných nebezpečných situácií v cestnej doprave.
- Optický záznam umožňuje presnú rekonštrukciu sériových nehôd, t. j. nehôd pri ktorých došlo ku kontaktu viacerých vozidiel. Náročnosť rekonštrukcie takéhoto druhu nehôd štandardnými metódami narastá zo synchronizačných dôvodov s rastúcim počtom zúčastnených vozidiel exponenciálne až na hranicu pri ktorej rekonštrukciu nie je možné vykonať.

Väčšina metód analýzy dopravných nehôd z videozáznamu je založená na kinematickom princípe, ide o metódy publikované napr. v [1], [2], [3] a [4].

Základné princípy konštrukcie vozidlových kamier

Vozidlové kamery, a to najmä tie používané bežnými účastníkmi cestnej premávky, sú v súčasnej dobe prakticky všetky konštruované ako digitálne kamery (obr. 1). Ide teda o kamery, pri ktorých svetelné lúče dopadajú nie na fotocitlivý film, ale na obrazový senzor. Zjednodušená schéma konštrukcie digitálnej je uvedená na obr. 1.



Obr. 1: Digitálna kamera – všeobecná schéma: 1– šošovka, 2 – zobrazovací senzor (CMOS), 3 – základná doska, 4 – dcérska doska s I/O portami a slotom na SD kartu, 5 – kontrolný LCD panel s predným ovládačom, 6 – zdroj energie (Li-Ion batéria) [5]

Úlohou obrazového senzora (2) digitálnej kamery je konverzia svetla na elektrický náboj, pričom v absolútnej väčšine digitálnych kamier sa používajú dva druhy obrazových senzorov – CMOS (Complementary Metal-Oxide Semiconductor) a CCD (Charged-Coupled Device) [6]. Pri praktickom porovnaní oboch druhov senzorov CCD senzory vyžadujú dodatočné komponenty a logické okruhy pre svoju funkciu a kamery nimi vybavené sú väčšie a komplexnejšie, pričom vo všeobecnosti poskytujú vyššiu obrazovú kvalitu ako CMOS senzory. Naproti pri CMOS senzoroch sú logické okruhy pre spracovanie obrazu integrované v rámci čipu, kamery vybavené CMOS senzormi majú kompaktnejšie rozmery a môžu byť relatívne dlhodobo napájané batériou (6), aj keď v praxi sú často napojené na elektrickú sústavu vozidla. Práve pre svoje kompaktné rozmery sú najviac zastúpené práve v segmenty vozidlových kamier, alebo tzv. akčných kamier (ktoré však rovnako môžu plniť funkciu vozidlových kamier). Každý obrazový senzor digitálnej kamery pozostáva z usporiadaného poľa fotocitlivých obrazových bodov – pixelov, pričo každý pixel premieňa elektromagnetické žiarenie viditeľného spektra (ale väčšinou aj malej časti IR spektra) na digitálny signál, pričom sumár digitálnych signálov zo všetkých pixelov vo výsledku vytvorí digitálny obraz.

Svetlo je prepúšťané na obrazový senzor cez šošovku (1), ktorej úlohou je najmä sústredenie svetla na malú plochu obrazového senzoru. Šošovky vozidlových kamier sú vo väčšine prípadov s ohľadom na požiadavku kompaktných rozmerov pevne spojené s telom kamery a majú pevnú ohniskovú vzdialenosť. Ďalšou typickou charakteristikou šošoviek vozidlových kamier je ich široké zorné pole (typicky cca 140°) a s tým spojené aj značné radiálne skreslenie šošovky. Ide o optické skreslenie šošovky kamery, ktoré spôsobuje, že objekty a predmety, ktoré majú v skutočnosti rovné hrany sa na vyhotovenom obraze javia ako zakrivené. V prípade vozidlových kamier sa potom najčastejšie radiálne skreslenie vyskytuje ako tzv. súdkovitosť, kedy s rastúcou vzdialenosťou rovného objektu od optického stredu obrazu tento objekt nadobúda zakrivenosť konvexného charakteru. Toto skreslenie je ako príklad uvedené na obr. 2. Extrémnym prípadom súdkovitosti je tzv. efekt rybieho oka, ktorý je typický najmä pre akčné kamery. Radiálne skreslenie šošovky kamery predstavuje pre technickú rekonštrukciu a analýzu nehodového deja z videozáznamu vozidlovej (ale aj statickej monitorovacej) kamery problém a je potrebné tento optický jav pri určovaní vzdialeností z videozáznamu zohľadniť a v ideálnom prípade toto skreslenie odstrániť, tak aby videozáznam nadobudol rektilinéarny charakter [7], [8], [9].

Obr. 2: Príklad súdkovitosti šošovky digitálnej kamery – úsečka vyznačuje skutočný tvar nosníka

Súčasťou optického systému vozidlovej kamery je ďalej clona, ktorá reguluje množstvo svetla, ktoré dopadá na obrazový senzor kamery a ktorá spoločne s ohniskovou vzdialenosťou kamery definuje uhol kónusu zväzku svetelných lúčov, ktoré dopadajú na obrazový bod v zobrazovacej rovine. Vozidlové kamery sú spravidla vybavené pevne nastavenou clonou s vysokou hodnotou (od cca f/2,8 po f /1,6).

Nakoniec je súčasťou optického systému vozidlovej kamery aj uzávierka, ktorá reguluje ako a kedy dôjde k prepusteniu svetelných lúčov na obrazový senzor počas expozície, ako aj dĺžku trvania expozície. Rýchlosť uzávierky nie je spravidla u vozidlových kamier nastaviteľná užívateľom, ale je nastavovaná automaticky samotnou kamerou najmä na základe intenzity osvetlenia. Z technického hľadiska sa pri vozidlových kamerách vyskytujú dva druhy konštrukcie uzávierky: globálna uzávierka a valivá uzávierka. Globálna uzávierka prepúšťa svetlo simultánne na všetky pixely obrazového senzoru naraz a tvar snímaného pohybujúceho sa objektu je následne bez deformácie. Valivá uzávierka prepúšťa svetlo na obrazový senzor postupne a to buď horizontálnym spôsobom alebo vertikálnym spôsobom. Keďže svetlo následne nedopadá na obrazový senzor simultánne v jednom časovom okamihu tak potom obraz pohybujúceho sa objektu (napr. cestné vozidlo) má zdeformovaný charakter, napríklad zošikmenie tvaru, kedy sa javí, že dolná časť vozidla „predbieha" hornú časť.

Vytvorený digitálny obraz je uložený na záznamové médium, ktorým je v prípade vozidlových kamier spravidla SD (SDHC, SDXC) karta, alebo microSD (microSDHC, microSDXC) karta. Tieto záznamové karty by mali mať parametre umožňujúce vysokú trvanlivosť pri neustálych prepisoch záznamu, nakoľko videozáznam je spravidla natáčaný v slučke. K permanentnému uloženiu určitého záznamu o určitej dĺžke trvania dochádza spravidla až pri detekcii veľkého zrýchlenia/spomalenia vozidla kvôli nárazu (ak je kamera vybavená G senzorom), alebo manuálne uživateľom. Na rozdiel od statických monitorovacích kamier je spravidla videozáznam pre analytika dostupný vo formáte (napr. avi, mp4, hevc) priamo kompatibilnom s bežnými videoprehrávačmi ako VLC player a MPC HC. V závislosti od kvality záznamového média a veľkosti dátového toku kamery môže pri kombinácií nízkej kvality záznamovej karty a vysokej hodnoty dátového toku dochádzať k vynechávaniu niektorých snímkov záznamu a to buď periodicky, alebo náhodne, čo je potom nutné pri rekonštrukcii a analýze zohľadniť, nakoľko by tento efekt spôsobil prerušenie konštantnosti časového kroku medzi snímkami videozáznamu.

Vozidlové kamery bývajú vybavené samostatným zdrojom energie v podobe Li-Ion alebo Li-Pol batérií, ale na rozdiel od akčných kamier tieto nie sú vysokej kapacity a slúžia skôr ako záložný zdroj. V prípade vozidlových kamier je počítané s tým, že kamera bude napájaná/dobíjaná z elektrickej siete vozidla a to najčastejšie cez 12V napájací adaptér. Čoraz častejšie výrobcovia vozidlových kamier poskytujú a príslušenstvo na trvalú montáž kamery vo vozidle, pričom k zapnutiu kamery a začiatku spustenia záznamu dochádza pri uvedení vozidla do prevádzky vodičom.

Vozidlové kamery sú užívateľom ovládané a nastavované spravidla cez ovládací dotykový panel alebo cez mobilnú aplikáciu, pričom však možnosti nastavenia kamery sú v obmedzenom rozsahu.

Niektoré vozidlové kamery sú vybavené dodatočnými funkciami, ktoré je možné dodatočne vyťažiť pri analýze dopravného deja, napr. GPS senzor, alebo senzor pohybu v zornom poli kamery [10].

Využitie vozidlových kamier pre rekonštrukcii a analýze dopravných situácií

Digitálne vizuálne stopy v podobe digitálnych fotografií z miest dopravných nehôd sú používané v odbore analýzy dopravných nehôd pravidelne. Digitálne fotografie majú v sebe obsiahnutú informáciu o polohe objektov a to minimálne v 2D, t. j. v rovine. Digitálna videostopa zachytávajúca dopravnú situáciu má okrem informácie o polohe objektu v sebe obsiahnutú aj informáciu o čase: videozáznam je vo svojej podstate sekvenčný súbor fotografií s definovaným časovým krokom medzi dvomi po sebe nasledujúcimi snímkami. Tento časový krok je v ideálnom prípade konštantný a je ho možné určiť na základe informácie o snímkovacej frekvencii danej kamery. Táto uvádza počet snímkov, ktorý kamera zaznamená za 1 sekundu. Pre určenie časového kroku medzi dvomi po sebe nasledujúcimi snímkami videozáznamu potom platí jednoduchý vzťah:

$$\Delta t = \frac{1}{f_s}$$

Kde:
Δt (s) – časový krok medzi dvomi po sebe nasledujúcimi snímkami,
f_s (Hz = s^{-1}) – snímkovacia frekvencia kamery, počet snímkov za sekundu (fps – frames per second).

V praxi sa najčastejšie u vozidlových kamier vyskytuje snímkovacia frekvencia 25 Hz, resp. 30 Hz. Vozidlové kamery vyššieho radu majú potom možnosť snímkovacej frekvencie 50 Hz, resp. 60 Hz, čo však samozrejme kladie vyššie nároky na kapacitu úložného priestoru, nakoľko pri rovnakej kvalite a formáte záznamu predstavuje cca dvojnásobný objem digitálnych údajov.

Pri snímkovacej frekvencii 25 Hz je potom časový krok medzi dvomi po sebe nasledujúcimi snímkami 0,04 s. Je teda zrejmé, že ak má analytik dopravných nehôd k dispozícii aj údaj o polohe daného sledovaného objektu záujmu (osobný automobil, motocykel, autobus, apod.) v dvoch po sebe nasledujúcich snímkoch, tak má aj možnosť získať informáciu o priemernej rýchlosti daného objektu medzi týmito snímkami a to na základe jednoduchého kinematického vzťahu:

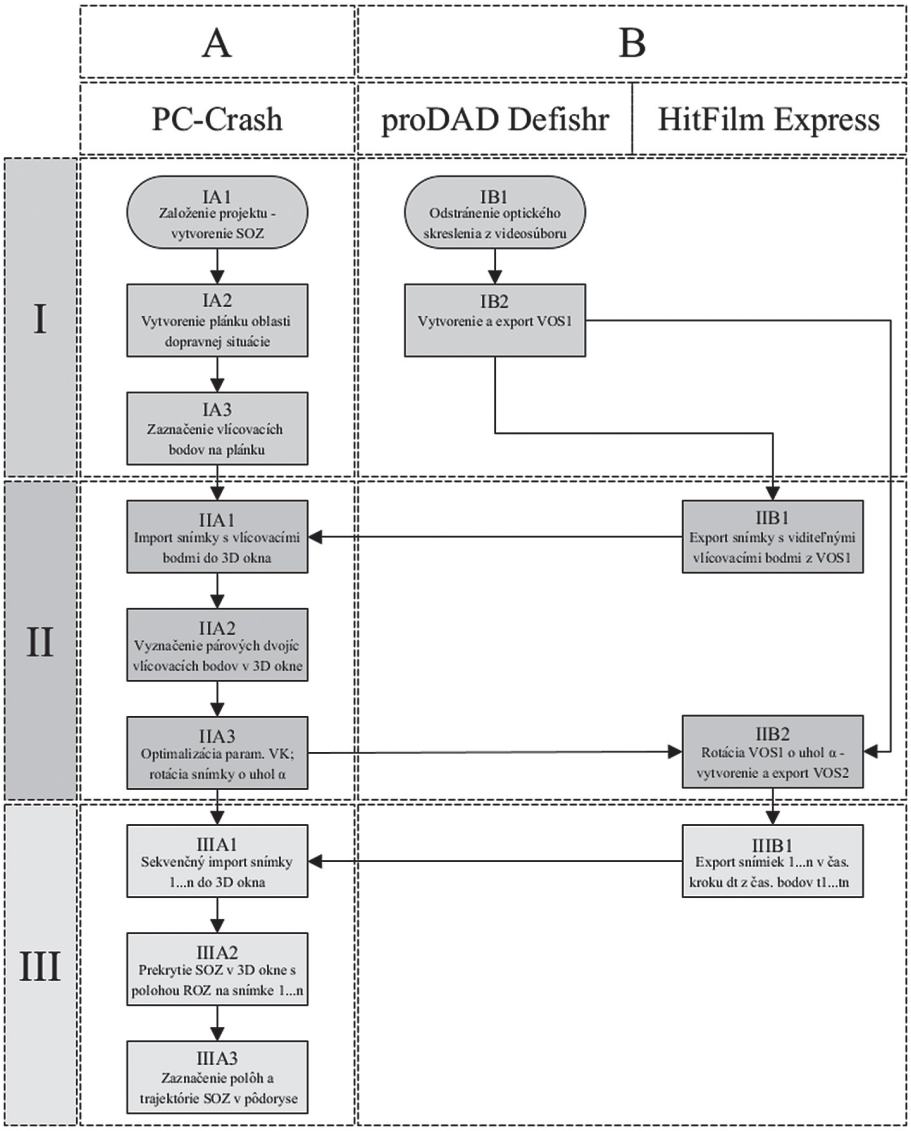
$$v_p = \frac{\Delta s}{\Delta t}$$

Kde:
v_p (m/s) – priemerná rýchlosť objektu záujmu medzi dvomi nasledujúcimi snímkami,
Δs (m) – dráha ktorú prešiel objekt záujmu medzi dvomi po sebe nasledujúcimi snímkami,
Δt (s) – časový krok medzi dvomi po sebe nasledujúcimi snímkami.

V praxi často nie je nutné vyhodnocovať priemernú rýchlosť medzi dvomi nasledujúcimi snímkami videozáznamu (najmä pri pohybe objektu záujmu nízkou rýchlosťou), ale stačí tento údaj vyhodnocovať pre tzv. kľúčové snímky (key frames), napr. pre každý 5 snímok záznamu. V takomto prípade analytik vychádza z údaja polohy objektu záujmu v danom kľúčovom snímku (t. j. v každom 5 snímku záznamu) a použije časový krok, ktorý uplynie medzi každým piatym snímkom záznamu. T. j. pri snímkovacej frekvencii 25 Hz by bol časový krok medzi každým piatym snímkom záznamu 0,2 s ($5/25\ s^{-1} = 0{,}2$ s).

Dôležité je teda potom pre analytika správne určenie polohy objektu záujmu na danom kľúčovom snímku a to z dopravnej situácie zachytenou kamerou v perspektívnom zobrazení. Pre

samotným určením polohy objektu záujmu na danom snímku n musí pritom analytik ešte vykonať kroky ktoré vedú k pripraveniu zdrojového záznamu do stavu použiteľného pre analýzu a to často s použitím špecializovaného softvérového vybavenia. Príklad metódy rekonštrukcie polôh a trajektórie objektov záujmu z videozáznamu s použitím 3 softvérových riešení je uvedený na schéme na obr. 3.



Obr. 3: Bloková schéma rekonštrukcie polohy objektov záujmu na snímkoch 1…n videozáznamu

Vo vyššie uvedenej schéme je logická nadväznosť procesných krokov definovaná vertikálnym aj horizontálnym členením nasledovne:

I. Prípravná fáza slúži na základnú prípravu výpočtu a na prípravu zdrojového videozáznamu do stavu použiteľného pre nasledujúce fázy. V tejto fáze je odstránené radiálne skreslenie videozáznamu tak, aby upravený videozáznam mal rektilineárny charakter.

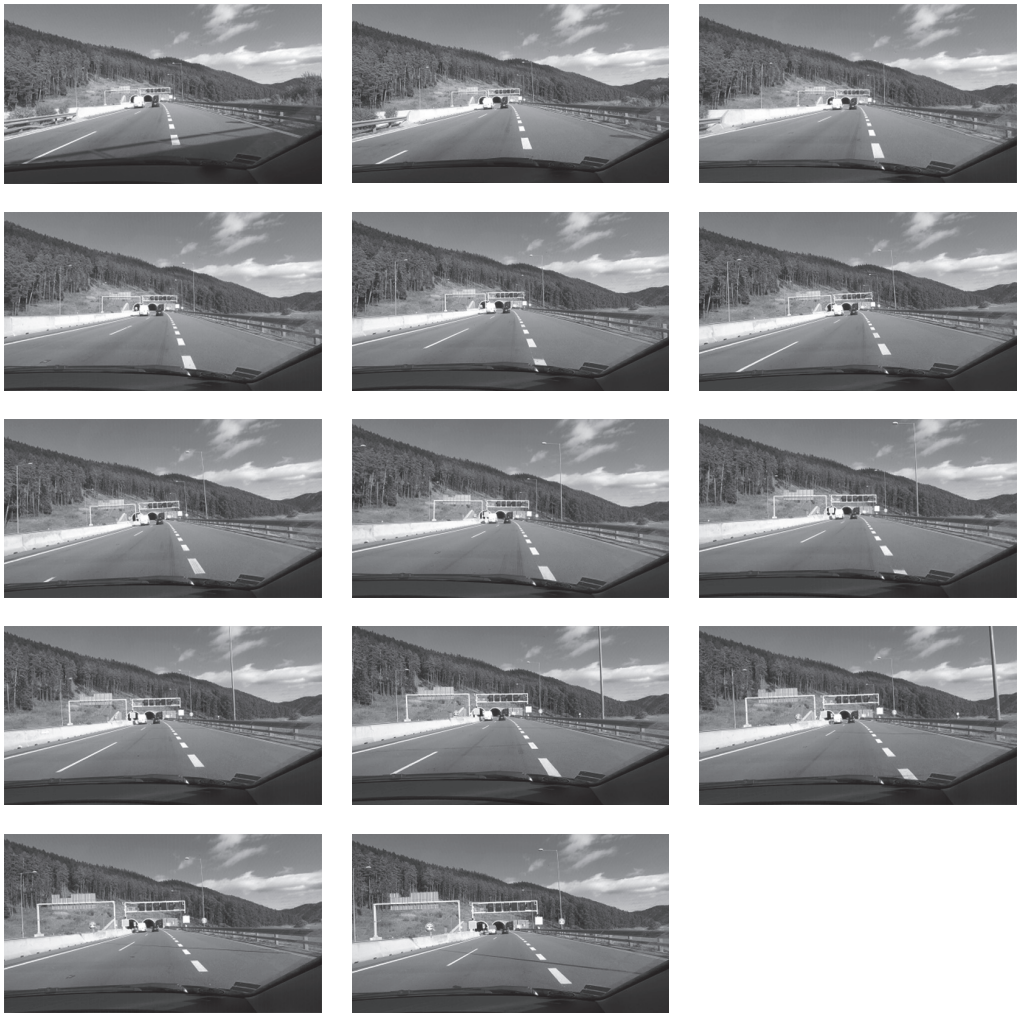
II. Fáza rekonštrukcie polohy, uhlov natočenia a ohniskovej vzdialenosti monokamery, ktorá zachytila dopravnú situáciu (ktorá je predmetom analytického skúmania) tak, aby sa parametre modelu kamery vo virtuálnom prostredí simulačného programu čo najviac blížili parametrom skutočnej kamery. Výsledkom je pohľad na simulovanú dopravnú situáciu vo virtuálnom prostredí simulačného programu v analogickom priestorovom perspektívnom zobrazení, aké je zachytené reálnou monokamerou.

III. Fáza rekonštrukcie trajektórie a pohybového stavu reálnych objektov záujmu (ROZ) v časových bodoch t_1 až t_n. V rámci tejto fázy sa z videozáznamu dopravnej situácie zachytenom monokamerou identifikujú kvázi-statické polohy reálnych objektov záujmu v 3D perspektívnom zobrazení videozáznamu na snímkach 1 až n v časových bodoch t_1 až t_n, ktoré sú od seba vzdialené o časový interval Δt. Tieto polohy sa následne identifikujú v 3D prostredí simulačného programu polohovaním virtuálneho modelu simulovaného objektu záujmu (SOZ) do získania vizuálneho prekrytia tohto modelu s polohou ROZ na danej snímke. Takto identifikované kvázi-statické polohy v 3D prostredí simulačného programu sa prenesú do pôdorysného zobrazenia v simulačnom programe. Z polôh zaznačených v pôdorysnom zobrazení sa určí trajektória pohybu ROZ a vykoná sa prvotné určenie pohybového stavu ROZ na základe vzájomných dráhových vzdialeností medzi následnými polohami objektov záujmu v časových bodoch t_1 až t_n a na základe veľkosti časového intervalu Δt.

A. Kroky vykonávané **v simulačnom programe** na analýzu dopravných nehôd, resp. jazdnej dynamiky, napr. program PC-Crash [11].

B. kroky vykonávané v programe **pre editáciu videozáznamu,** napr. HitFilm Express [12] a ProDad Defishr [13].

Príklad aplikácie vyššie uvedenej metódy v praxi na modelovom prípade je uvedený na nasledovných obrázkoch. Modelový prípad prestavuje určenie rýchlosti vozidla pohybujúceho sa po diaľnici, ktorého pohyb bol zachytený vozidlovou kamerou umiestnenou v inom pohybujúcom sa vozidle. Videozáznam bol vyhotovený vo rozlíšení 1920×1080 px a so snímacou frekvenciou 60 Hz. Pre analýzu bol použitý každý desiaty snímok záznamu a teda časový krok medzi dvomi po sebe vyhodnocovanými snímkami bol 0,1667 s ($10/60\ s^{-1} \approx 0{,}1667$ s). Sekvenčný export kľúčových snímkov záznamu je uvedený na obr. 4. Postupnosť snímkov je zľava doprava a zhora nadol.

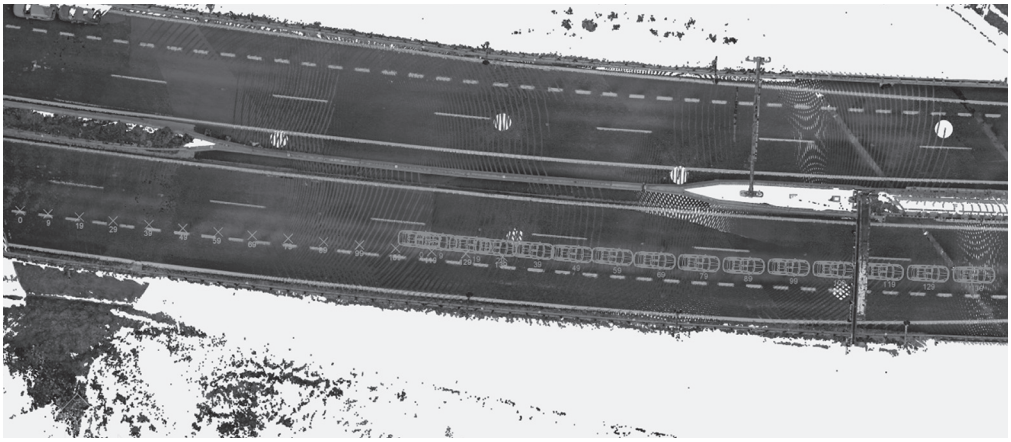


Obr. 4: Kľúčové snímky modelového videozáznamu

Model polohopisu dopravnej situácie bol vytvorený metódou 3D laserového skenovania prístrojom Faro Focus^{S} 350. Tento prístroj umožňuje veľmi presné zameranie priestorových súradníc s presnosťou ± 1 mm [14]. Výsledkom laserového skenovania bolo tzv. mračno bodov (priestorových súradníc bodov jednotlivých skenovaných objektov). V rámci celkového mračna bodov bola vykonaná triangulácia a vytvorenie aktívnej plochy (polygónu sklonov) toho úseku dopravnej infraštruktúry, po ktorej sa pohybovalo predmetné vozidlo. Výsledkom je verná reprodukcia pozdĺžnych a priečnych sklonov v predmetnom úseku. Takto vytvorený model polohopisu predmetnej dopravnej situácie slúžil ako podklad k spracovaniu výpočtu v programe PC-Crash 12.0. Priestorový pohľad na model polohopisu miesta dopravnej situácie je uvedený na obr. 5.

Obr. 5: 3D model polohopisu dopravnej situácie v perspektívnom zobrazení

Aplikáciou krokov metódy uvedených v schéme na obr. 3 boli získané polohy kamery ktorá vyhotovila záznam (a teda aj polohy vozidla v ktorej bola kamera umiestnená) a polohy vozidla ktoré bolo objektom záujmu (OA Škoda Octavia) v kľúčových snímkoch. Zrekonštruované polohy sú viditeľné v pôdorysnom zobrazení na obr. 6, pričom pri každej polohe je uvedené identifikačné číslo snímku videozáznamu ku ktorému sa daná poloha vzťahuje. Z priebehu jednotlivých polôh je ďalej možné ustáliť aj trajektóriu oboch vozidiel a nakoniec a identifikovať pohybový stav vozidiel, t. j. akou rýchlosťou sa dané vozidlo pohybovalo a či jeho pohyb bol nerovnomerný (t. j. či sa jeho rýchlosť menila v čase a teda či zrýchľovalo alebo spomaľovalo).



Obr. 6: Zrekonštruované polohy vozidiel v kľúčových snímkoch záznamu v pôdorysnom zobrazení

Vyššie uvedený výsledok rekonštrukcie je kinematického charakteru a poskytuje obmedzený súbor využiteľných údajov. Tento výsledok je však ďalej možné použiť ako vstup do simulačného výpočtu využitím modulu kinetiky simulačného programu a na základe tohto kinetického simulačného výpočtu získať aj dodatočné údaje o pohybe vozidla, napr. údaj o priečnom zrýchle-

ní vozidla, uhle natočenia riadiacich kolies, uhlovej rýchlosti vozidla. Na základe týchto údajov je potom možné identifikovať rôzne správanie a reakcie vodiča daného vozidla.

Úplne na záver si dovolíme prezentovať nádej a zároveň presvedčenie, že problematika monitorovania kamerovým systémom, osobitne vo vozidlách sa dočká komplexnej legislatívnej púpravy nielen na Slovensku, ale i na úrovni Európskej únie vzhľadom na nejednotnosť úpravy a prístupu využívania autokamier v rôznych krajinách EÚ.

Literatúra

Monografie

KLIMEK, Libor, ZÁHORA Jozef, HOLCR Květoň. *Počítačová kriminalita v európskych súvislostiach*. Bratislava, Wolters Kluwer, 2016, s. 445, ISBN 978-80-8168-538-5

NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň, Aleš Čeněk, 2018, s. 339, ISBN 978-80-7380-689-7

POLÁK, Peter. *Svedok v trestnom konaní*. Bratislava, Eurokódex 2011, s. 296, ISBN 978-80-89447-47-3

ZÁHORA, J. a kol.: *Dokazovanie v trestnom konaní*. 1. vydanie. Praha: Leges 2013

Učebnice a komentáre

IVOR Jaroslav, POLÁK Peter, ZÁHORA Jozef. *Trestné právo procesné 1*. Wolters Kluwer 2017, 528 s., ISBN 978-80-8168-593-4

IVOR Jaroslav, ZÁHORA Jozef. *Repetitórium trestného práva*. Bratislava, Wolters Kluwer, 2018, s. 220, ISBN 978_80-8168-769-9

KURUCOVÁ Zuzana, DEMOVIČOVÁ Andrea. *Introduction to the U. S. Law*. Wolters Kluwer Bratislava 154 s., ISBN 978-80-8168-725-9

Príspevky v zborníkoch

IVOR, Jaroslav. Monitorovanie kamerovým systémom ako dôkazný prostriedok v trestnom konaní. *Zborník príspevkov vedeckej konferencie „Prieniky trestného práva k iným právnym odvetviam a vedeckým disciplínam“*. Košice 2017, s. 9 – 20, ISBN 978-80-8152-493-6

IVOR, Jaroslav. 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

Články

IVOR, Jaroslav. Niektoré aktuálne trestnoprocesné problémy boja s organizovanou kriminalitou. *Justičná revue* č. 5–6/1998

Ostatné pramene

Rozhodnutie ESĽP 2/439/93 (Botta proti Taliansku),

Rozsudok Najvyššieho správneho súdu ČR 2AS45/2010-68,

Nález Ústavného súdu ČR I. ÚS 191/05,

Metodické usmernenia Úradu na ochranu osobných údajov SR č. 3/2013, 1/2014, 5/2016,

Stratégia prevencie kriminality a inej protispoločenskej činnosti na roky 2016 – 2020, schválená vládou SR v roku 2016.

Zoznam citovaných zdrojov:

1. Edelman, G., Bijhold, J.: *Tracking people and cars using 3D modeling and CCTV,* Forensic Science International, vol. 202, 26–35, 2010
2. Wong, T., W., at al.: *Application of cross-ratio in traffic accident reconstruction,* Forensic Science International, vol. 235, 19–23, 2014

3. Del Cesta. F., Del Cesta, A.: *Using CCTV data in the analysis of real vehicle accidents: a laser scanner approach,* 26th Annual Congress of the EVU: proceedings, 19.–21. 10. 2017, Haarlem, Netherlands, 2017, ISBN 978-90-903-0511-0
4. Ondruš, J., Hockicko, P.: *Braking deceleration measurement using the video analysis of motions by Sw tracker*, Transport and telecommunication, vol. 16, no. 2 (2015), s. 127–137, ISSN 1407-6160
5. www.ifixit.com
6. Crouch, M., Cash, S.: *Video Analysis in Collision Reconstruction*, 1st ed., ISBN-13 978-1788089302, 2017
7. Fenton, S., Neale, W., Rose, N., Hughes, C.: *Determining Crash Data Using Camera Matching Photogrammetric Technique*, SAE Technical Paper No. 2001-01-3313, Society of Automotive Engineers, Warrendale, PA, USA, 200, DOI: https://doi.org/10.4271/2001-01-3313
8. Neale, W., T., C., Fenton, S., McFadden, S., Rose, N., A.: *A Video Tracking Photogrammetry Technique to Survey Roadways for Accident Reconstruction*, SAE Technical Paper No. 2004-01-1221, Society of Automotive Engineers, Warrendale, PA, USA, 2004. DOI: https://doi.org/10.4271/2004-01-1221
9. Neale, W., T., C., Hessel, D., Terpstra, T.: *Photogrammetric Measurement Error Associated with Lens Distortion*, SAE Technical Paper No. 2011-01-0286, Society of Automotive Engineers, Warrendale, PA, USA, 2011, DOI: https://doi.org/10.4271/2011-01-0286
10. www.dod-tec.com
11. www.dsd.at
12. www.fxhome.com
13. www.prodad.com
14. www.faro.com

Táto práca bola zrealizovaná v rámci projektu ENABLE-S3, ktorý získal grantové financovanie zo Spoločného podniku ECSEL pod grantovou zmluvou č. 692455. Tento Spoločný podnik získava podporu z výskumného a inovačného programu Európskej únie HORIZON 2020 a z Rakúska, Dánska, Nemecka, Fínska, Českej republiky, Talianska, Španielska, Portugalska, Poľska, Írska, Belgicka, Francúzska, Holandska, Veľkej Británie, Slovenska a Nórska. Táto práca bola čiastočne podporená aj Ministerstvom školstva, vedy, výskumu a športu Slovenskej republiky.

This work has been conducted within the ENABLE-S3 project that has received funding from the ECSEL Joint Undertaking under Grant Agreement no. 692455. This Joint Undertaking receives support from the European Union's HORIZON 2020 research and innovation programme and Austria, Denmark, Germany, Finland, Czech Republic, Italy, Spain, Portugal, Poland, Ireland, Belgium, France, Netherlands, United Kingdom, Slovakia, Norway. This work was also partially supported by Ministry of Education, Science, Research and Sport of the Slovak Republic.

Obrazovo-zvukové záznamy vyhotovované súkromnými osobami a ich prípustnosť v trestnom konaní[1]

Video and Audio Records Made by Private Persons and their Admissibility in the Criminal Proceedings

Miloš Deset[2]

Abstrakt: *Tak ako pri vyhotovovaní obrazových, zvukových alebo obrazovo-zvukových záznamov príslušnými orgánmi štátu, aj pri obrazových a zvukových záznamoch vyhotovovaných súkromnými osobami vystupujú do popredia minimálne dva protichodné záujmy, ktorých posúdenie vôbec nie je jednoduché. Na jednej strane je to záujem na ochrane práva na súkromie obvineného, na druhej strane zasa záujem na objasnení trestného činu a zistení jeho páchateľa. Situácia je o to komplikovanejšia, že súkromná nahrávka nemá podľa odbornej verejnosti jasné právne základy, z ktorých by bolo evidentné, že takáto nahrávka by mohla byť považovaná za zákonný dôkaz, vďaka čomu by mohla byť aj prípustným dôkazom v trestnom konaní.*

Abstract: *Considering the making of video, audio or video-audio records by appropriate state authorities, the making such records by the private persons also evokes two opposite interests, which qualification is not easy, at all. On the one hand is the interest to protect the right to privacy of alleged person, on the other hand is the interest to investigate the crime and identification of its perpetrator. The situation is more complicated, because according to the expert community, the private record does not have the legal basis, which can give the conclusion, that such records could be considered as the legal and admissible evidence in the criminal proceedings.*

Kľúčové slová: *právo na súkromie, obrazové a zvukové záznamy, zákonnosť dôkazu, prípustnosť dôkazu, zásada legality, zásada legitimity, zásada proporcionality.*

Keywords: *the right to privacy, video and audio records, the legality of evidence, the admissibility of evidence, the standard of legality, the standard of legitimacy, the standard of proportionality.*

Úvod

Oblasť informačných technológií zaznamenala v posledných niekoľkých dekádach obrovský rozmach. Nové technológie zasiahli prakticky do všetkých spoločenských oblastí, právo nevynímajúc. V oblasti trestného práva sa tieto nové trendy prejavili napríklad v podobe formulovania nových skutkových podstát, v oblasti trestného práva procesného sa zasa zaviedli viaceré prostriedky zabezpečovania informácií dôležitých pre trestné konanie.

No predsa len by sme mohli povedať, že aj napriek badateľnému pokroku a vývoju v oblasti trestno-procesnej úpravy informačno-technických prostriedkov, prostriedkov operatívno-pátracej činnosti a dokazovania naše trestné právo, obzvlášť trestné právo procesné, akoby zaostávalo za najnovšími vývojovými tendenciami v oblasti informačných technológií.

Trestné právo procesné síce upravuje viaceré informačno-technické prostriedky a prostriedky operatívno-pátracej činnosti, ako napríklad odpočúvanie a záznam telekomunikačnej pre-

[1] Táto práca bola vypracovaná v rámci riešenia vedecko-výskumného projektu VEGA Ministerstva školstva, vedy, výskumu a športu Slovenskej republiky č. 1/0764/17 s názvom „Informačno-technické prostriedky a prostriedky operatívno-pátracej činnosti získavania informácií dôležitých pre trestné konanie“.

[2] Doc. JUDr. Miloš Deset, PhD., Trnavská univerzita v Trnave, Právnická fakulta, Univerzita Mateja Bela v Banskej Bystrici, Právnická fakulta, e-mail: deset.milos@gmail.com.

vádzky, vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov, agenta alebo sledovanie osôb a vecí, no neupravuje viacero ďalších spôsobov zabezpečovania informácií, ktoré si v rámci komunikácií medzi sebou vymieňajú napríklad užívatelia rozličných programov či mobilných aplikácií. Prostriedok odpočúvania a záznamu telekomunikačnej prevádzky napríklad umožňuje orgánom činným v trestnom konaní zistiť dôležité informácie pre trestné konanie, ktoré si dotknuté osoby medzi sebou vymieňajú prostredníctvom telefónu, no už im neumožňuje zabezpečovať informácie, ktoré by si takéto osoby medzi sebou vymieňali napríklad prostredníctvom aplikácií, ako napríklad Hangouts, Messenger či Skype. Pritom páchatelia trestnej činnosti si túto činnosť nemusia plánovať iba prostredníctvom telefónov, ale napríklad aj takýmto spôsobom. Komunikáciu v rámci páchania trestnej činnosti, resp. jej koordinácie alebo utajovania po jej spáchaní takisto nemusia uskutočňovať iba prostredníctvom telefónu.

Toto je však iba jedna z problematických oblastí, pri ktorej akoby naše trestné právo procesné takpovediac ťahalo za kratší oproti informačným technológiám. Ďalšími aktuálnymi otázkami by mohlo byť napríklad sledovanie podozrivých či obvinených osôb prostredníctvom GPS či lokalizačných služieb mobilných operátorov, vyhľadávačov, ako napríklad Google, alebo využívanie dronov napríklad pri sledovaní osôb a vecí či vykonávaní niektorých kriminalisticko-taktických metód (obhliadkach či prehliadkach).

Domnievam sa, že jednou z takýchto aktuálnych otázok je aj otázka využívania obrazových, zvukových alebo obrazovo-zvukových záznamov, ktoré vyhotovili súkromné osoby. Táto otázka sa stala aktuálnou vďaka masovej dostupnosti mobilných telefónov či tabletov), ktoré užívateľom umožňujú vyhotovovať si takéto záznamy pre svoje vlastné potreby.

Pre oblasť trestného práva, obzvlášť trestného práva procesného, by mohlo byť relevantné, ak by tieto záznamy obsahovali informácie dôležité pre trestné konanie. Ak by napríklad poškodený zaznamenal konanie páchateľa alebo aspoň časť páchaného skutkového deja, ktorým by páchateľ zasahoval do jeho základných práv a slobôd a zároveň aj napĺňal niektorú zo skutkových podstát trestného činu (napríklad trestného činu nebezpečného vyhrážania, nebezpečného prenasledovania, vydierania, atď.), kedy by sa orgány činné v trestnom konaní mohli ocitať v situáciách dôkaznej núdze, a práve takéto záznamy by im mohli výrazným spôsobom uľahčiť objasňovanie takýchto trestných činov a zisťovanie ich páchateľov.

1. Právna úprava práva na súkromie

V takýchto situáciách však vystupujú do popredia minimálne dva protichodné záujmy, ktorých posúdenie však vonkoncom nie je také jednoduché ako by sa na prvý pohľad mohlo zdať. Po prvé ide o verejný záujem na ochrane základných práv a slobôd a záujmov chránených Trestným zákonom č. 300/2005 Z. z. (ďalej len „Trestný zákon“), s ktorým ide ruka v ruke verejný záujem na objasnení trestného činu a zistení jeho páchateľa, aby mu bol uložený spravodlivý trest na strane jednej, a verejný záujem na ochrane práva na súkromie ako jedného zo základných práv páchateľa, resp. v závislosti od procesného postavenia podozrivého alebo obvineného, na strane druhej. Obrazovým, zvukovým alebo obrazovo-zvukovým záznamom vyhotovených súkromnou osobou (poškodeným, príp. inou osobou) sa nevyhnutne zasahuje do práva na súkromie tejto osoby, ktoré je zakotvené napríklad v čl. 8 Dohovoru o ochrane ľudských práv a základných slobôd (ďalej len „Európsky dohovor“) alebo v čl. 16 Ústavy Slovenskej republiky č. 460/1992 Zb. (ďalej len „Ústava“). Podľa čl. 8 ods. 1 Európskeho dohovoru každý má právo na rešpektovanie svojho súkromného a rodinného života, obydlia a korešpondencie; podľa čl. 16 ods. 1 Ústavy nedotknuteľnosť osoby a jej súkromia je zaručená.

Na túto európsku, resp. ústavnoprávnu ochranu nadväzuje aj občianskoprávna úprava, konkrétne § 11 ods. 1 Občianskeho zákonníka č. 40/1964 Zb. (ďalej len „Občiansky zákonník), podľa ktorého fyzická osoba má právo na ochranu svojej osobnosti, najmä života a zdravia, občianskej cti a ľudskej dôstojnosti, ako aj súkromia, svojho mena a prejavov osobnej povahy.

Do týchto práv, samozrejme, možno zasahovať z rôznych dôvodov, avšak za podmienky, že akékoľvek zásahy do ústavného, občianskeho práva na súkromie sa realizujú podľa zákona. Zákonný postup si vyžaduje aj vyhľadávanie a vykonávanie dôkazov v trestnom konaní, čo vyplýva z § 119 ods. 2 Trestného poriadku, podľa ktorého za dôkaz môže slúžiť všetko, čo môže prispieť na náležité objasnenie veci a čo sa získalo z dôkazných prostriedkov podľa tohto alebo podľa osobitného zákona.

2. Zákonnosť a prípustnosť súkromnej nahrávky ako dôkazu v trestnom konaní

V trestnom práve procesnom v zásade platí, že dôkaz je zákonný, ak bol nielen vykonaný zákonným spôsobom, ale aj získaný zo zákonného dôkazného prostriedku. V prípade vyhotovovania obrazových, zvukových alebo obrazovo-zvukových záznamov súkromnou osobou však problémom je, že takéto záznamy nie sú uznané ako dôkazné prostriedky podľa Trestného poriadku ani podľa iného zákona, to znamená, že ani nemôžu byť považované za zákonné dôkazy. A vzhľadom na znenie § 119 ods. 4 Trestného poriadku, podľa ktorého môže byť v trestnom konaní prípustný iba taký nezákonný dôkaz, ktorý bol získaný nezákonným donútením alebo hrozbou takého donútenia, okrem prípadu, ak sa použije proti osobe, ktoré také nezákonné donútenie alebo jeho hrozbu použila (pozri § 119 ods. 4), nemôže byť takýto záznam ani prípustný v trestnom konaní ako nezákonný dôkaz.

Práve na tieto ustanovenia Trestného poriadku poukazuje aj judikatúra. Podľa Rozsudku Najvyššieho súdu Slovenskej republiky, sp. zn. 4 TZ 9/2006, dôkaz získaný v rozpore so zákonom prenáša svoju nezákonnosť a procesnú nepoužiteľnosť aj na ďalší dôkaz, ktorý vychádza z obsahu nezákonne získaného dôkazu.[3] Takýto záver sa, samozrejme, vzťahuje nielen na orgány činné v trestnom konaní, ale aj na súkromné osoby.

Podľa iného názoru záznam vyhotovený súkromnou osobou a predložený v trestnom konaní ako dôkaz *a priori* nemôže byť neprípustný len z dôvodu nezákonnosti. Posúdenie, či určitý konkrétny obrazový a zvukový záznam bude prípustný v trestnom konaní, je vecou konkrétneho trestného konania a situácie, za ktorej majú byť takto získané informácie použité. Máme za to, že takýto záznam vyhotovený súkromnou osobou môže byť prípustný za podmienky, že zásah do súkromia je odôvodniteľný prevažujúcim záujmom na strane toho, kto takýto záznam zabezpečil a v trestnom konaní ako dôkaz predložil.[4]

Ak by sme totiž trvali na striktnom odmietnutí akýchkoľvek záznamov vyhotovených súkromnými osobami z dôvodu ich nezákonnosti, mohlo by to viesť k absurdným situáciám, v ktorých by sme mali vedomosť o páchateľovi trestnej činnosti, no kvôli neprípustnosti takýchto záznamov ako dôkazov z dôvodu ich nezákonnosti (v situácií dôkaznej núdze) by sme mu ju nevedeli dokázať. Mohlo by ísť napríklad o trestný čin ochrany súkromia v obydlí podľa § 194a Trestného zákona, trestný čin výroby detskej pornografie podľa § 368 Trestného zákona, trest-

[3] Rozsudok Najvyššieho súdu Slovenskej republiky, sp. zn. 4TZ 9/2006.

[4] Záhora, J. et al. Obrazové a zvukové záznamy v trestnom konaní. Bratislava: Wolters, Kluwer, 2018, s. 244, a Gajdičiar, V. – Strigáčová, D. Prípustnosť súkromnej nahrávky pri trestno-procesnom dokazovaní v slovenskej právnej úprave. In Justičná revue, 2004, č. 6–7, s. 827.

ný čin porušenia dôvernosti ústneho prejavu a iného prejavu osobnej povahy podľa § 377 alebo iné trestné činy.[5]

Za súčasnej právnej úpravy možno použiť ako dôkazy záznamy vyhotovené súkromnými osobami pri trestný činoch verejných činiteľov, pretože výkon právomoci verejných činiteľov nemožno považovať za prejav osobnej povahy. Nespadá totiž do práva na súkromie a nevzťahuje sa naň ochrana podľa § 11 Občianskeho zákonníka.[6] Zatiaľ čo do súkromia osôb, a teda aj do predmetu ochrany osobnosti patria zásadné otázky týkajúc sa ich intímnej sféry (písomnosti osobnej povahy, zvukové záznamy prejavov osobnej povahy), v prípade výkonu ústavnej alebo zákonnej právomoci verejných činiteľov na verejnosti ide o diametrálne odlišné otázky verejnej a nie súkromnej sféry, ktoré nemožno v žiadnom prípade považovať za súčasť ich základného práva na súkromie. Otázkou verejného záujmu je preto slobodné získavanie informácií o spôsoboch, akými verejní činitelia vykonávajú na verejnosti svoje ústavné alebo zákonné právomoci. Verejní činitelia si musia byť vedomí toho, že budú vystavení pozornosti verejnosti a budú musieť akceptovať výkon práva na informácie zo strany verejnosti minimálne v tom rozsahu, v akom svoje ústavné alebo zákonné právomoci vykonávajú na verejnosti.[7]

Ako dôkazy by mohli byť prípustné aj také súkromné nahrávky, na ktorých nie sú zaznamenané prejavy osobnej povahy fyzických osôb, ale napríklad budovy, motorové vozidlá, udalosti, živelné pohromy, zvieratá a pod.[8]

Oba právne názory, ktoré zohľadňujú takpovediac výnimky z neprípustnosti súkromných nahrávok ako dôkazov v trestnom konaní, sú, samozrejme, relevantné, o. i. aj preto, že zjemňujú prílišný formalizmus vyjadrený v Rozsudku Najvyššieho súdu Slovenskej republiky, sp. zn. 4 TZ 9/2006, a z neho prameniacu tvrdosť realizácie práva, ktorá sa bezprostredne dotýka dosiahnutia účelu trestného konania a práv poškodeného.

Okrem nich – vyhotovovanie súkromných nahrávok v prípade trestných činov verejných činiteľov a v prípade zachytávania budov, motorových vozidiel, udalostí, atď. – možno ešte spomenúť napríklad svojpomoc podľa § 6 Občianskeho zákonníka, podľa ktorého Ak hrozí neoprávnený zásah do práva bezprostredne, môže ten, kto je takto ohrozený, primeraným spôsobom zásah sám odvrátiť.

No podobne ako pri predchádzajúcich právnych názoroch, ani pri svojpomoci by sme nedospeli k uspokojivému riešeniu. Pri vyhotovovaní súkromných nahrávok verejných činiteľov alebo pri vyhotovovaní súkromných nahrávok zachytávajúcich budovy, motorové vozidlá či udalosti problém spočíva v tom, že takéto prípady sú pomerne špecifické. Nejde o dostatočne systematické, komplexné a všeobecné riešenie, ktoré by vyhovovalo potrebám vyšetrovateľskej a justičnej praxe. Pri svojpomoci zasa problém spočíva v tom, že svojpomoc môže realizovať iba poškodený, resp. osoba, ktorá je bezprostredne ohrozená, a že tak môže urobiť iba pred tým, ako dôjde k porušeniu jeho práva (v čase, kedy ešte stále bezprostredne hrozí neoprávnený zásah do práva). To znamená, že o svojpomoc by sa nedala oprieť súkromná nahrávka, ktorú by vyhotovil napríklad svedok, alebo nahrávka, ktorú by síce vyhotovil poškodený, ale až potom, čo došlo k porušeniu jeho práva.

[5] Nález Ústavného súdu Českej republiky, sp. zn. II. ÚS 143/06.

[6] Záhora, J. et al. Obrazové a zvukové záznamy v trestnom konaní. Bratislava: Wolters, Kluwer, 2018, s. 246.

[7] Nález Ústavného súdu Slovenskej republiky, sp. zn. II. ÚS 44/00-133.

[8] Šamko, P. Zákonnosť a použiteľnosť dôkazov trestnom konaní získaných utajovanou činnosťou detektívnej služby. In Zo súdnej praxe, 2017, č. 3, s. 110, a Záhora, J. et al. Obrazové a zvukové záznamy v trestnom konaní. Bratislava: Wolters Kluwer, 2018, s. 246.

Záver

Svojpomoc síce vykazuje vyššiu mieru všeobecnosti a komplexnosti riešenia otázky prípustnosti súkromnej nahrávky ako dôkazu v trestnom konaní, pretože sa netýka iba verejných činiteľov, ale prakticky všetkých občanov, no aj napriek tomu nemusí ísť o riešenie, ktoré by bolo vyhovujúce potrebám vyšetrovateľskej a justičnej praxe. Ak sa totiž pozrieme na európske štandardy či ústavné zásady sformulované Ústavným súdom Slovenskej republiky, tak je zrejmé, že zásahy do práva na súkromie musia spĺňať podmienky plynúce zo zásad legitimity, legality a proporcionality. Je nepochybné, že aj súkromná nahrávka by mohla vyhovovať zásade legitimity, ktorá o. i. zahŕňa verejný záujem na objasnení trestného činu a zistení jeho páchateľa tak, ako to vyplýva z čl. 8 ods. 2 Európskeho dohovoru. Pri zásade proporcionality by zasa bolo relevantné posúdenie či by použiteľnosť takejto nahrávky vychádzala z potrebnosti takéhoto dôkazu v trestnom konaní a či by verejný záujem na objasnení trestného činu prevládal nad verejným záujmom na ochrane práva na súkromie obvineného. Ak by takáto nahrávka nemusela byť potrebná, pretože by sa k rovnakému sledovanému legitímnemu cieľu mohli orgány činné v trestnom konaní dopracovať aj prostredníctvom iných, k základnému právu šetrnejším dôkazom, nemalo by zmysel polemizovať nad tým, či ju použiť alebo nie. Pokiaľ ide posúdenie kolízie spomenutých dvoch verejných záujmov, treba povedať, že tieto nie sú imaginárne či abstraktné. Samozrejme, ich posúdenie závisí od konkrétneho orgánu, napríklad sudcu, no treba mať na pamäti, že ani základné práva a slobody nemožno vykladať absolútne či bezbreho. Z toho vyplýva otázka, do akej miery sa obvinený môže pri svojej obhajobe odvolávať na svoje základné právo (právo na súkromie), ak svojim konaním, ktorým naplnil znaky skutkovej podstaty niektorého z trestných činov a zároveň zasiahol do základného práva iného (napríklad pri trestnom čine nebezpečného vyhrážania či vydierania by išlo o to isté základné právo – právo na súkromie). Nastala by maximálne absurdná situácia, ak by sme v takomto prípade uprednostnili právo na súkromie obvineného, pred ochranou práva na súkromie, príp. iných práv, a verejným záujmom na objasnení trestného činu a spravodlivom potrestaní jeho páchateľa.

Samozrejme, že ak by mala byť súkromná nahrávka prípustná ako dôkaz v trestnom konaní, muselo by sa skúmať, či je autentická, t. j. či nebola zámerne a účelovo pozmenená, a či nebola vyhotovená iba so zámerom špicľovania iného. No ak by sa nepotvrdilo ani jedno, ani druhé a ak by súkromná nahrávka bola vyhotovená napríklad poškodeným výlučne na obranu jeho práv, situácia by bola úplne iná.

Súkromná nahrávka by tak – podobne ako pri zásade legitimity – mohla vyhovovať aj kritériám plynúcim zo zásady proporcionality. Otáznik však visí nad zásadou legality. Svojpomoc podľa občianskeho práva je zrejme najpevnejším právnym základom pre posúdenie súkromnej nahrávky ako zákonného a prípustného dôkazu v trestnom konaní, no je otázne, či by takéto riešenie vyhovovalo kritériám plynúcim zo zásady legality, pretože, vychádzajúc z aktuálnej judikatúry, právna úprava upravujúca zásahy do práva na súkromie by mala byť dostatočne presná, zrozumiteľná a predvídateľná, aby potenciálne dotknutým osobám poskytovala dostatočne presnú informáciu o podmienkach, za ktorých môže dôjsť k zásahu do ich základného práva.[9]

Ak by týmto kritériám svojpomoc nevyhovovala, prakticky by to znamenalo, že vzhľadom na absenciu inej právnej úpravy, ktorá by umožňovala použiteľnosť súkromných nahrávok ako dôkazov v trestnom konaní, a vzhľadom na rozšírenosť zariadení, ktoré užívateľom umožňujú vyhotovovať si takéto nahrávky, by bolo nevyhnutné novelizovať § 119 Trestného poriadku, a to

[9] Pozri napríklad nález Ústavného súdu Českej republiky, sp. zn. Pl. ÚS 24/11, alebo nález Ústavného súdu Slovenskej republiky, sp. zn. I. ÚS 274/05.

takým spôsobom, že by sa buď inak definoval dôkaz, príp. dôkazný prostriedok v odseku 2, aby zahŕňal aj takéto nahrávky ako zákonné a prípustné dôkazy, alebo by sa inak sformulovali podmienky zákonnosti a prípustnosti dôkazu v odseku 4, pretože ak by mali byť takéto nahrávky považované za nezákonné dôkazy, práve v odseku 4 by sa takouto novelizáciou mohlo umožniť, aby boli prípustné v trestnom konaní.

Literatúra

Gajdičiar, V. – Strigáčová, D. Prípustnosť súkromnej nahrávky pri trestno-procesnom dokazovaní v slovenskej právnej úprave. In Justičná revue, 2004, č. 6–7.

Šamko, P. Zákonnosť a použiteľnosť dôkazov trestnom konaní získaných utajovanou činnosťou detektívnej služby. In Zo súdnej praxe, 2017, č. 3.

Záhora, J. et al. Obrazové a zvukové záznamy v trestnom konaní. Bratislava: Wolters Kluwer, 2018.

Nález Ústavného súdu Českej republiky, sp. zn. II. ÚS 143/06.

Nález Ústavného súdu Slovenskej republiky, sp. zn. II. ÚS 44/00-133.

Nález Ústavného súdu Českej republiky, sp. zn. Pl. ÚS 24/11.

Nález Ústavného súdu Slovenskej republiy, sp. zn. I. ÚS 274/05.

Rozsudok Najvyššieho súdu Slovenskej republiky, sp. zn. 4TZ 9/2006.

Skutočne možno použiť v trestnom konaní nezákonné dôkazy získané súkromnými osobami?[1]

Is it Possible to use Unlawful Evidence Obtained by Private Individuals in Criminal Proceedings?

Peter Šamko[2]

Abstrakt: *Článok sa zaoberá spornou problematikou posudzovania zákonnosti, či nezákonnosti vyhotovenia obrazovo zvukových záznamov, ktoré boli vyhotovené súkromnou osobou bez súhlasu nahrávanej osoby a ich následnej dôkaznej použiteľnosti, či nepoužiteľnosti v trestnom konaní, pričom uvádza argumenty proti aplikačnej praxi, ktorá je náchylná k využívaniu nezákonne získaných dôkazov zo strany súkromných osôb.*

Abstract: *The article deals with the disputed issue of assessing the legality or illegality of the production video-audio records which have been made by a private individual without the consent of the recorded person and their subsequent probative applicability or inapplicability in Criminal proceedings, stating arguments against application practice, which is prone to the use of illegally obtained evidence by private individuals.*

Kľúčové slová*: obrazovo zvukový záznam, súkromná osoba, dokazovanie, ochrana súkromia.*

Keywords*: video-audio records, private person, proving, protection of privacy.*

Cieľom tohto príspevku je pokračovať v odbornej diskusii[3] o spornej problematike zákonnosti, či nezákonnosti vyhotovenia obrazovo-zvukových záznamov, ktoré boli vyhotovené súkromnou osobou (t. j. osobou odlišnou od orgánu činného v trestnom konaní) bez súhlasu nahrávanej osoby a ich následnej dôkaznej použiteľnosti, či nepoužiteľnosti v konaní pred súdom. Riešenie naznačenej otázky je vyslovene sporné aj v rozhodovacej činnosti orgánov aplikácie práva,[4] pričom rozoberaná problematika nebola doposiaľ riešená (oficiálnou) judikatúrou, či zjednocujúcim stanoviskom Najvyššieho súdu SR.[5]

---

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

[2] JUDr. Peter Šamko, sudca Krajského súdu v Bratislave, e-mail: peter.samko@justice.sk

[3] Pozri napríklad
Gajdičiar, V., Strigáčová, D.: Prípustnosť súkromnej nahrávky pri trestno-procesnom dokazovaní v slovenskej právnej úprave, Justičná revue. 2014, roč. 66, č. 6–7, s. 831 a nasl.,
Čentéš, J.: Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. Bratislava: C. H. Beck, 2013
Šamko, P.: K zákonnosti získavania dôkazov (nad jedným rozhodnutím Ústavného súdu SR, Zo súdnej praxe. 2015, č. 4
Kyjac, Z.: Použitie informačno – technických prostriedkov v trestnom konaní. Odpočúvanie a záznam telekomunikačnej prevádzky, Wolters Kluwer, 2015, s. 265 a nasl.,
Šamko, P.: Zákonnosť a použiteľnosť dôkazov v trestnom konaní získaných utajovanou činnosťou detektívnej služby, Zo súdnej praxe č. 3/2017
Ivor, J.: Monitorovanie kamerovým systémom ako efektívny dôkazný prostriedok, publikované v Dokazování v trestním řízení v kontextu práva na spravedlivý proces. Praha: Leges, 2018, s. 283 a nasl.,
Záhora, J. et al.: Obrazové a zvukové záznamy v trestnom konaní, Bratislava: Wolters Kluwer, 2018.

[4] Napríklad uznesenie Krajského súdu v Žiline sp. zn. 1To/42/2010 zo dňa 22. 4. 2010 a kritiku tohto rozhodnutia v rozsudku Okresného súdu v Pezinku http://www.pravnelisty.sk/rozhodnutia/a189-sukromna-diktafonova-nahravka-a-nezakonnost-dokazu, uznesenie Najvyššieho súdu SR sp. zn. 2 Tost 4/2014 zo dňa 2. 4. 2014 a kritiku tohto rozhodnutia v článku Šamko, P.: Zákonnosť a použiteľnosť dôkazov v trestnom konaní získaných utajovanou činnosťou detektívnej služby, Zo súdnej praxe č. 3/2017.

[5] Naznačená problematika zahŕňa rôzne spektrum činnosti súkromnej osoby pri vyhotovovaní obrzovozvukových záznamov fyzickej osoby (napríklad vyhotovanie zjavným alebo utajovaným spôsobom na verejnosti, v súkromí,

Pod pojmom „súkromná nahrávka" je v aplikačnej praxi nutné rozumieť najmä prípady vyhotovovania obrazovných, zvukových, či obrazovozvukových nahrávok zo strany fyzických, či právnických osôb (napríklad detektívnej služby), ktoré zobrazujú podobu, prejav, respektíve oboje konkrétnej fyzickej osoby a to bez súhlasu tejto zobrazovanej (či nahrávanej) fyzicky osoby, pričom ide buď o nahrávky vyhotovené utajeným spôsobom (nahrávaná osoba nevie, že je nahrávaná), respektíve neutajovaným spôsobom, avšak proti vôli nahrávanej osoby (napríklad fyzická osoba na verejnosti vidí, že je nahrávaná inou osobou a vysloví svoj nesúhlas s takýmto postupom). Pokiaľ ide o zariadenia, ktoré sa spravidla využívajú na vyhotovovanie takýchto záznamov tak ide hlavne o fotenie, či vyhotovovanie videonahrávok inej osoby, či jej prejavov prostredníctvom mobilného telefónu, fotoaparátu, diktafónu, či kamerového systému.

A práve posudzovanie (ne)zákonnosti vyhotovovania takýchto záznamov a od nej sa odvíjajúcej procesnej (ne)použiteľnosti takýchto záznamov vyhotovených súkromnou osobou v trestnom konaní je v praxi pomerne sporné, nakoľko naráža na ustanovenie § 119 ods. 2 Tr. por. ako aj na ustanovenie § 12 Občianskeho zákonníka. V tomto smere treba zdôrazniť, že cielené (úmyselné) nahrávanie inej osoby bez jej súhlasu sa vždy dostáva do konfliktu s ustanovením § 12 Občianskeho zákonníka, pričom zobrazenie inej fyzickej osoby napríklad prostredníctvom vyhotovenia obrazovej snímky, či obrazového záznamu bez jej súhlasu je vždy zásahom do práva na ochranu osobnosti osoby, ktorej snímka, či záznam sa vyhotovuje. Typickým príkladom zásahu do tohto práva je napríklad (cielené, systematické) fotografovanie inej osoby na ulici bez súhlasu fotografovaného.[6]

Takáto právna úprava (§ 12 Občianskeho zákonníka) je logická, nakoľko štát nemá záujem na tom, aby medzi jednotlivými súkromnými osobami dochádzalo k špehovaniu, či sledovaniu, respektíve k nahrádzaniu činnosti orgánov činných v trestnom konaní a aby si iné osoby bez súhlasu konkrétnej fyzickej osoby mohli úmyselne vyhotovovať jej podobizne (snímky, videá) a využívať ich na rôzne účely.[7]

Časť odbornej literatúry ako aj časť orgánov aplikácie práva sa už dlhodobo snaží „prekonať" ustanovenie § 12 Občianskeho zákonníka ako aj ustanovenie § 119 ods. 2 Tr. por. rôznymi výkladmi smerujúcimi k tomu, aby sa mohli súkromné nahrávky využívať na ustaľovanie skutkového stavu veci v trestnom konaní a to aj napriek tomu, že boli vyhotovené (získané) v rozpore so zákonom (ustanovením § 12 Občianskeho zákonníka) a preto by správne mali byť v trestnom konaní odmietnuté (§ 119 ods. 2 Tr. por.).

Je pozoruhodné ako sa napriek pomerne jednoznačnému zneniu ustanovenia § 119 ods. 2 Tr. por. stále vyskytuje snaha kontaminovať trestné konanie nezákonnými dôkazmi a tento postup ospravedlniť rôznymi, skôr subjektívnymi hodnotovými postojmi, než objektívnym výkladom práva.

v obchodných priestoroch, prostredníctvom iných osôb, napríklad detektívnej služby a podobne).

[6] K uvedenému pozri bližšie napríklad Fekete, I.: Občiansky zákonník 1. Veľký komentár, Bratislava: Eurokódex 2011, s. 120 a nasl.

[7] Od takejto situácie je nutné odlíšiť prípady, v ktorých dochádza na verejnom priestranstve k náhodnému zachyteniu konkrétnej fyzickej osoby napríklad prostredníctvom fotoaparátu, či kamery. Typicky, napríklad turista pri fotografovaní kultúrnej pamiatky náhodou zachytí inú fyzickú osobu ako pácha trestný čin; v takomto prípade ide o vedľajší, nechcený výsledok činnosti fyzickej osoby, pričom použitie takéhoto náhodnou činnosťou súkromnej osoby získaného dôkazu v trestnom konaní spravidla nevzbudzuje žiadne podstatné pochybnosti o svojej zákonnosti. Ak by sa turista rozhodol využiť vyhotovené snímky inej fyzickej osoby aj na iný účel, než je ich odovzdanie polícii (napríklad by ich umiestnil na web, či vyhotovený video záznam by „zavesil" na youtube) išlo by už o konanie nelegálne.

Vzhľadom k uvedenému je nutné venovať pozornosť jednotlivým argumentom, ktoré sa uvádzajú ako odôvodnenie možného kontaminovania trestného konania nezákonne vyhotovenými súkromnými nahrávkami.

1/ využitie českej judikatúry vrcholových súdov, ktorá za určitých okolností pripúšťa použitie aj nezákonne vyhotovenej súkromnej nahrávky ako dôkaz v trestnom konaní

Spravidla prvým a často aj nosným argumentom za využívanie aj nezákonne vyhotovených súkromných nahrávok v trestnom konaní v SR býva odkaz na pomerne bohatú judikatúru Najvyššieho súdu ČR, či Ústavného súdu ČR,[8] z ktorej vyplýva, že s ohľadom na ustanovenie § 89 ods. 2 Trestného poriadku účinného v ČR zásadne nemožno vylúčiť možnosť, aby bol ako dôkaz použitý aj (obrazový, či zvukový) záznam, ktorý bol vyhotovený súkromnou osobou bez súhlasu osôb, ktorých obraz, či hlas bol takto zaznamenaný. Vychádza sa tu z toho, že ani dôkaz získaný za porušenia ustanovenia § 12 Občianskeho zákonníka nemôže byť a priori vylúčený ako dôkaz v trestnom konaní, pričom využiteľným dôkazom môže byť za podmienky, že zásah do súkromia je odvoditeľný záujmom na strane toho, kto záznam zadovážil a následne použil.

Využitie judikatúry českých vrcholových súdov aj v právnych podmienkach SR teda vychádza z komparatívneho výkladu práva. Tu však treba zdôrazniť, že komparatívna (porovnávacia) metóda výkladu práva prichádza do úvahy iba v prípadoch, ak je právna úprava v cudzine (v danom prípade v ČR) zhodná alebo aspoň výrazne podobná s právnou úpravou v SR. Pokiaľ tak nie, a právna úprava v ČR je dokonca výrazne obsahovo odlišná ako v SR, potom je nutné takúto metódu výkladu práva odmietnuť, nakoľko judikatúra českých vrcholových súdov vykladá obsahovo odlišnú právnu úpravu.

Tak je tomu aj v posudzovanom prípade, nakoľko ustanovenie § 89 ods. 2 českého Trestného poriadku znie tak, že za „dôkaz môže slúžiť všetko, čo môže prispieť k objasneniu veci...".[9] Z obsahového znenia tohto ustanovenia je zrejmé, že pojem „všetko" nespája iba a len s pojmom „zákonné všetko" a preto možno dospieť k záveru, že za určitých okolností je možné využiť na objasnenie veci aj nezákonne získaný dôkaz. A práve vrcholové české súdy hľadajú a vymedzujú vo svojej judikatúre hranice (priestor), v ktorých je možné použiť v trestnom konaní aj nezákonne získaný dôkaz.

Na území SR však platí obsahovo (z hľadiska zákonnosti) diametrálne odlišná práva úprava.

Podľa § 119 ods. 2 Tr. por. „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 predpisu". Z obsahového vymedzenia predmetného ustanovenia je zrjemé, že pojem „všetko" viaže výhradne na „zákonné všetko", t. j. pojem „všetko" sa spája len s takým dôkazným prostriedkom, ktorý bol získaný podľa Trestného poriadku, respektíve podľa iného zákona. Musí ísť teda o dôkaz zákonný, nakoľko iba vtedy možno povedať, že bol získaný postupom predpokladaným Trestným poriadkom, či iným osobitným predpisom. Alebo povedané inak, „všetko" čo síce môže prispieť na náležité objasnenie veci a čo sa nezískalo z dôkazných prostriedkov podľa Trestného poriadku alebo podľa osobitného predpisu nie je možné považovať v trestnom konaní za dôkaz (§ 119 ods. 2 Tr. por. argumentum a contrario).

---

[8] Napríklad uznesenie Najvyššieho súdu ČR sp. zn. 5Tdo/459/2007 zo dňa 3. 5. 2007, uznesenie Ústavného súdu ČR sp. zn. I. ÚS 604/2010 a podobne.

[9] Obsahovo zhodné ustanovenie obsahoval aj Trestný poriadok účinný na území SR do 31. 12. 2005.

Na rozdiel od právnej úpravy v ČR, v právnych podmienkach SR už zákonodarca sám vymedzil priestor, v ktorom sa musia pohybovať získané dôkazy a týmto priestorom je len a výhradne priestor zákonný. Všetko, čo je mimo hraníc priestoru zákonnosti, zákonodarca vyňal z pojmu „všetko" a tým pádom aj využiteľnosti ako dôkazu v trestnom konaní. Na tieto významné rozdiely medzi českou a slovenskou právnou úpravou napokon upozorňuje aj samotná česká odborná literatúra.[10]

Skutočnosť, že v právnych podmienkach SR kladie zákonodarca zrejmý dôraz na zákonnosť získaných dôkazoch možno nepochybne vyvodiť aj zo základnej zásady trestného konania vymedzenej v ustanovení § 2 ods. 12 Tr. por. podľa ktorej „orgány činné v trestnom konaní a súd hodnotia dôkazy získané **zákonným** spôsobom...". Z uvedenej základnej zásady trestného konania teda vyplýva, že orgány činné v trestnom konaní a ani súd nemôžu vôbec pojať do hodnotenia dôkazov také dôkazy, ktoré boli získané nezákonne. A práve na túto základnú zásadu trestného konania následne nadväzuje ustanovenie § 119 ods. 2 Tr. por.

Možno preto uzatvoriť, že pripustiť nezákonne získanú súkromnú nahrávku ako dôkaz v trestnom konaní v právnych podmienkach SR nie je možné len s odkazom na právnu argumentáciu uvedenú v rozhodnutiach vrcholových súdov ČR, pretože sa vzťahuje na výklad obsahovo odlišného ustanovenia než je ustanovenie § 119 ods. 2 Tr. por. Ustanovenie § 2 ods. 12 Tr. por., či ustanovenie § 119 ods. 2 Tr. por. nie je možné opomenúť (ignorovať) iba s poukazom na judikatúru súdov cudzieho štátu, ktorý nemá rovnakú právnu úpravu ako SR.

2/ využitie judikatúry Európskeho súdu pre ľudské práva (ESĽP), ktorá za určitých okolností pripúšťa použitie aj nezákonne vyhotovenej súkromnej nahrávky ako dôkaz v trestnom konaní

Ďalším argumentom zástancov využitia aj nezákonne získaných súkromných nahrávok v trestnom konaní je odkaz a využitie judikatúry ESĽP. V tomto smere sa odkazuje spravidla na rozhodnutie ESLP vo veci Schenk proti Švajčiarsku,[11] z ktorého vyplýva, že pokiaľ bol dôkaz získaný v rozpore s vnútroštátnym právom, táto skutočnosť sama osebe nemusí byť porušením práva na spravodlivý proces v zmysle článku 6 Dohovoru o ochrane ľudských práva a základných slobôd. ESĽP spravidla označí vedené trestné konanie ako spravodlivé vo svojom celku, ak síce bola pripustená nezákonne získaná nahrávka v trestnom konaní ako dôkaz, ale nešlo o jediný usvedčujúci dôkaz a ak boli dodržané práva obhajoby spočívajúce v možnosti spochybniť takýto dôkaz.

Aj v prípade bezbrehého preberania (opisovania) judikatúry ESĽP do právnej argumentácie vnútroštátneho súdu pritom možno mať relevantné pochybnosti o tom, či možno vnútroštátne právo ignorovať len s poukazom na judikatúru ESĽP a fakticky nahrádzať ustanovenia vnútroštátneho práva judikatúrou ESĽP. Aby bolo trestné konanie spravodlivé, malo by byť postavené na dôkazoch, ktoré boli získané a vykonané v súlade s vnútroštátnym právom. Nie je možné, aby vnútroštátny súd rezignoval na vnútroštátnu právnu úpravu dokazovania, ktorá je pre neho záväzná a svoj nezákonný procesný postup v zmysle vnútroštátneho práva preklenul odkazom na „celkovú spravodlivosť konania" v zmysle judikatúry ESĽP.

V tomto smere možno poukázať na uznesenie Krajského súdu v Bratislave sp. zn. 4To/61/2018 zo dňa 8. 11. 2018, ktorý k riešenej problematike uviedol, že „relevantné ustanovenia Trestného poriadku (§ 2 ods. 12 a § 119 ods. 2 Tr. por.) nemožno obísť len všeobecným poukazom na judikatúru Dohovoru o ochrane ľudských práv a základných slobôd, ktorý navyše ani žiadne pra-

[10] Zaoralová, P.: Procesní použitelnost dukazu v trestním řízení a její meze. Praha: Leges, 2018, s. 59 a nasl. a s. 73.
[11] Rozhodnutie ESĽP zo dňa 12. 7. 1988, č. 10862/84.

vidlá o prípustnosti dôkazov nestanovuje. Z ustanovenia § 119 ods. 2 Tr. por. jednoznačne vyplýva, že za dôkaz môže slúžiť len to, čo bolo získané podľa zákona (t. j. v súlade so zákonom), pričom orgány činné v trestnom konaní ako aj súdy môžu hodnotiť iba dôkazy získané zákonným spôsobom (§ 2 ods. 12 Tr. por.). Zo základnej zásady trestného konania bližšie špecifikovanej v ustanovení § 119 ods. 2 Tr. por. teda evidentne vyplýva (za použitia argumentu a contrario) zákaz použitia nezákonne získaných dôkazov pri ustaľovaní skutkového stavu veci (so špecifickými výnimkami ako napríklad výnimkou uvedenou v ustanovení § 119 ods. 4 Tr. por.). Ignorovanie predmetných vnútroštátnych ustanovení Trestného poriadku iba s lakonickým poukazom na Dohovor (ktorého základom je, aby vnútroštátny orgán postupoval v prvom rade v súlade s vlastným právom) nemôže odôvodniť použitie nezákonného dôkazu v trestnom konaní".

Tieto závery napokon vyplývajú aj z rozhodovacej činnosti ESĽP, ktorý opakovane judikuje, že Dohovor nereguluje prípustnosť dôkazov v trestnom konaní, nakoľko táto oblasť je v prvom rade vecou vnútroštátneho práva a ESĽP neprináleží vyslovovať in abstracto zákaz použitia nejakého nezákonne získaného dôkazu. Jediné, čo môže vykonať, je posúdiť spravodlivosť trestného konaní ako celku.[12]

Pokiaľ sa často pri pripustení nezákonne získanej súkromnej nahrávky ako dôkazu v trestnom konaní argumentuje vyššie uvedenými závermi judikatúry ESĽP vychádzajúcej z toho, že je nutné skúmať, či nezákonne získaný dôkaz bol jediným, či iba jedným z viacerých usvedčujúcich dôkazov a či ho mal možnosť obžalovaný v trestnom konaní spochybniť, tak je potrebné dodať, že Trestný poriadok neumožňuje obísť ustanovenia § 2 ods. 12 a § 119 ods. 2 Tr. por. ani z dôvodu, že nezákonne získaná súkromná nahrávka je len jedným z usvečujúcich dôkazov proti obžalovanému, respektíve, že obvinený, či jeho obhajca mali možnosť sa k tomuto dôkazu vyjadriť a spochybniť ho. Tu treba opätovne zdôrazniť, že nezákonnosť získania dôkazu vylučuje takýto dôkaz z ustaľovania skutkového stavu veci ako aj z hodnotenia orgánmi činnými v trestnom konaní, či súdmi.

Navyše, ak je takýto nezákonne získaný dôkaz len jedným z usvedčujúcich dôkazov, tak nie je vôbec nutné na ňom alebo aj na ňom založiť odsúdenie obžalovaného, pričom možnosť obhajoby vyjadriť sa k takémuto dôkazu je len iluzórna, nakoľko obhajoba namieta spravidla nezákonnosť takéhoto dôkazu a súd, ak použije vyššie uvedený argument judikatúrou ESĽP, túto námietku „odbije" tým, že ide len o jeden z viacerých usvedčujúcich dôkazov proti obžalovanému a preto trestné konanie ako celok bolo spravodlivé.

Nahrádzanie porušenia vnútroštátnej úpravy odkazom na konkrétne rozhodnutie ESĽP, ktoré zo subjektívneho hľadiska v konkrétnej trestnej veci vyhovuje orgánom aplikácie práva, nie je možné akceptovať. Napokon, ani týmto súdom vytvorené možnosti pripustenia nezákonne získanej nahrávky v prípadoch ak nejde o jediný usvedčujúci dôkaz a bolo dodržané právo obvineného na obhajobu nevyznievajú veľmi presvedčivo.

Nie je možné akceptovať, aby prípustnosť či neprípustnosť konkrétneho dôkazu v trestnom konaní závisela od toho, či v trestnej veci existujú aj iné usvedčujúce dôkazy (a vtedy je možné pripustiť aj nezákonne získaný dôkaz), respektíve neexistujú (a vtedy už pripustenie nezákonného dôkazu neprichádza do úvahy). Procesná využiteľnosť konkrétneho dôkazu nemôže závisieť od náhody spočívajúcej v tom, či sa orgánom činným v trestnom konaní podarí alebo nepodarí zhromaždiť aj iné usvedčujúce dôkazy o prípadnej vine obvineného.

V tomto smere je nutné uviesť, že závery rozhodnutia ESĽP vo veci Schenk, či na neho nadväzujúcich rozhodnutí nie sú odbornou verejnosťou prijímané bezvýhradne a boli kritizované už v čase jeho vydania. Stojí za pozornosť napríklad spoločný disent štyroch sudcov, ktorí namieta-

[12] Rozhodnutie ESĽP zo dňa 12. 7. 1988, č. 10862/84.

li, že zákonnosť dôkazov v trestnom konaní má pre posúdenie spravodlivosti trestného konania zásadný význam. Zdôraznili, že **žiadny súd nesmie, bez toho, aby sa sprotivil dobrej správe spravodlivosti, brať do úvahy dôkaz, ktorý bol získaný nezákonne**. Pokiaľ tak urobí, konanie nemôže byť spravodlivé v zmysle Dohovoru. Skutočnosť, že vnútroštátne súdy založili, hoci aj len čiastočne, uznanie viny na nezákonnom dôkaze, viedla týchto štyroch disentujúcich sudcov k záveru, že konanie nemohlo byť spravodlivé.[13]

S týmto záverom je nutné sa stotožniť, nakoľko právo na spravodlivý proces nemôže byť zaručené ak odsúdenie obžalovaného je založené na dôkazoch, ktoré boli získané za porušenia práva na súkromie v zmysle článku 8 Dohovoru.[14] Samozrejme, podstatným tu musí byť posúdenie o akú nezákonnosť ide, nakoľko drobné, či formálne nezákonnosti pri získavaní dôkazu ešte nemusia byť takého podstatného (závažného) charakteru, že budú znamenať zásah do práva na súkromie, či do práva na spravodlivý proces.[15]

3/ argument spočívajúci v tom, že ak by sa neumožnilo v odôvodnených prípadoch použitie nezákonne získanej súkromnej nahrávky v trestnom konaní nebolo by možné v trestnom konaní použiť akýkoľvek záznam zachytávajúci prejavy páchateľov[16]

Ďalší z argumentov slúžiacich na „vtiahnutie" nezákonne získanej súkromnej nahrávky do dokazovania spočíva v tom, že ak by sa neumožnilo v odôvodnených prípadoch použitie nezákonne získanej súkromnej nahrávky v trestnom konaní nebolo by možné v trestnom konaní použiť

[13] Pozri bližšie Nejedlý, J.: Zákonnost dukazu v trestním řízení ve světle Evropské úmluvy o ochraně lidských práv a základných svobod, Univerzita Karlova v Praze, Právnická fakulta, Praha, 2013, s. 96 a nasl.

[14] Napokon, právo na súkromie v zmysle článku 8 Dohovoru zakotvuje ako prvú podmienku jeho možného obmedzenia práve požiadavku legality. Je možné skutočne tvrdiť, že obmedzenia uvedené v článku 8 Dohovoru platia iba pre štátne orgány a preto súkromné osoby môžu získavať dôkazy za porušenia vnútroštátneho práva, pretože sa ich netýkajú ustanovenia Dohovoru? Takýto zjednodušený výklad vzájomného vzťahu vnútroštátnej právnej úpravy a Dohovoru nie je možné pripustiť.

[15] Je nutné sa pripojiť k odbornej kritike rozhodovacej činnosti ESĽP, ktorá, a celkom oprávnene, kritizuje súčasný prístup ESĽP z niekoľkých zásadných dôvodov. Hlavným dôvodom je skutočnosť, že judikatúra ESĽP vedie k paradoxnému a celkom nevhodnému záveru, že nezákonný dôkaz získaný za porušenia článku 8 Dohovoru možno použiť v rámci trestného konania. ESĽP týmto svojim judikatórnym prístupom celkom nepochopiteľne posvecuje užívanie dôkazov získaných za porušenia článku 8 Dohovoru v trestnom konaní a tým pádom aj samotné porušovanie tohto ustanovenia za účelom získania potrebných dôkazov vyšetrujúcimi orgánmi. Vyšetrovacie orgány členských štátov sa totiž môžu podľa svojho voľného uváženia rozhodnúť, kedy sa im oplatí porušovať právo na súkromie osôb spadajúcich pod ich jurisdikciu (tento záver možno primerane použiť aj na konanie súkromných osôb napríklad pri získavaní obrazovozvukových dôkazov utajovaným spôsobom) a kedy už nie. Takýto prístup zásadným spôsobom oslabuje význam zákazu získavať dôkazy za porušenia článku 8 Dohovoru, pretože právo zaručené v článku 8 Dohovoru sa tak stáva iba právom teoretickým (iluzórnym). Je evidentné, že článok 3 Dohovoru (zákaz mučenia a iného neľudského a ponižujúceho zaobchádzania alebo trestu) obsahuje absolútny zákaz, zatiaľ čo zákaz zásahov do súkromia v zmysle článku 8 Dohovoru je len relatívny. Možno pochopiť názor, že napríklad mučenie predstavuje vyššiu mieru závažnosti než nezákonný odposluch. Možno však skutočne presvedčivo tvrdiť, že nezákonné odpočúvanie telefónu (ale napríklad aj dlhodobé monitorovanie inej osoby vykonávané utajovaným spôsobom za použitia vyhotovovania obrazovozvukových záznamov) je menej závažné, ako nerealizovaná vyhrážka mučením, ktorá trvá niekoľko minút? Judikatúra ESĽP je tak charakteristická minimalistickou koncepciou nielen práva na spravodlivý proces, ale aj práva na ochranu súkromia. Je pritom celkom zrejmé, že v dnešnej dobe moderných technológií, kedy sa zásahy do súkromia stávajú stále jednoduchšími a častejšími, je efektívna ochrana súkromia potrebnejšia než kedykoľvek predtým. K uvedenému pozri bližšie Nejedlý, J.: Zákonnost dukazu v trestním řízení ve světle Evropské úmluvy o ochraně lidských práv a základných svobod, Univerzita Karlova v Praze, Právnická fakulta, Praha, 2013, s. 100 a 101.

[16] Záhora, J. et al.: Obrazové a zvukové záznamy v trestnom konaní, Bratislava: Wolters Kluwer, 2018, s. 244.

akýkoľvek záznam zachytávajúci prejavy páchateľov trestných činov, napríklad trestného činu výroby detskej pornografie podľa § 368 Tr. zák.

Tento argument je vyslovene nesprávny a vôbec sa netýka posudzovanej problematiky.

V prvom rade je nutné uviesť, že napríklad pri trestnom čine výroby detského pornografického diela podľa § 368 ods. 1 Tr. zák. je vyhotovovanie detskej pornografie znakom základnej skutkovej podstaty tohto trestného činu. Trestný zákon teda zakazuje vyhotovovanie takéhoto materiálu. V tomto smere je preto bez významu, či dieťa ktoré je zobrazované na pornografické účely dalo alebo nedalo súhlas páchateľovi na vyhotovenie takéhoto záznamu, nakoľko sa postihuje aj v prípade súhlasu dieťaťa. Výroba detského pornografického diela je zakázaná za každých okolností a nie je tu možnosť inej voľby. Ustanovenie § 12 Občianskeho zákonníka (a prípadný súhlas, či nesúhlas zobrazovanej osoby) tu preto nehrá žiadnu úlohu, pretože vyhotovenie súkromnej nahrávky je tu zakázané priamo Trestným zákonom a už samo osebe je trestným činom. Trestný zákon má v tomto smere prednosť pred ustanovením § 12 Občianskeho zákonníka. Nahrávka dieťaťa, ktorú vyhotovil páchateľ teda môže byť použitá ako dôkaz v trestnom konaní, nakoľko preukazuje práve jeden zo znakov základnej skutkovej podstaty trestného činu výroby detského pornografického diela. Obdobne je to aj v prípadoch trestného činu ochrany súkromia v obydlí podľa § 194a Tr. zák. (narušenie práva na súkromie za použitia ITP), či trestného činu porušenia dôvernosti ústneho prejavu a iného prejavu osobnej povahy podľa § 377 Tr. zák. (narušenie práva na súkromie v neverejných priestoroch).

Naproti tomu, v tomto príspevku vymedzená problematika sa týka spravidla vyhotovovania nahrávok súkromnými osobami na verejnom priestranstve, či v miestach verejnosti prístupných (ulica, kaviareň, obchodný dom, verejné garáže, vozidlá MHD, školy, nemocnice, kiná). Takéto vyhotovovanie záznamov súkromnými osobami nie je postihované Trestným zákonom (ako trestný čin, t. j. tak ako je to napríklad pri trestnom čine výroby detskej pornografie), ale môže byť v kolízii práve s ustanovením § 12 Občianskeho zákonníka, pričom spravidla zachytáva niečo, čo by mohlo byť významné pre objasňovanie trestného činu (a preto by taká nahrávka mohla byť významná ako dôkaz v trestnom konaní).[17]

4/ argumnet, že ustanovenia Trestného poriadku o zadovažovaní dôkazov sa týkajú iba orgánov činných v trestnom konaní, či súdu a nie súkromných osôb a že žiadne ustanovenie Trestného poriadku neustanovuje pravidlá pre zabezpečovanie súkromnej nahrávky

Aj tento argument je nutné označiť za mylný. Ustanovenie § 119 ods. 2 Tr. por. sa týka toho čo a za akých podmienok môže byť dôkazom v trestnom konaní a nie toho kto dôkaz zabezpečuje. Predmetné ustanovenie sa preto vzťahuje na získavanie dôkazov nielen zo strany orgánov činných v trestnom konaní, ale aj súkromných osôb.

To napokon vyplýva z celého kontextu ustanovenia § 119 ods. 2 Tr. por. v zmysle ktorého môže byť v trestnom konaní využitý (vykonaný) aj dôkaz, ktorý bol získaný podľa osobitného zákona. Dôkaz použiteľný v trestnom konaní teda nemusí byť vždy získaný len postupom pod-

[17] Je rozdiel v tom, keď napríklad osoba znásilní ženu (to Trestný zákon zakazuje) od situácie, keď si iná osoba nahráva znásilnenie (nahrávanie znásilnenia Trestný zákon, na rozdiel od znásilnenia samotného, nezakazuje). Z hľadiska posudzovanej problematiky je preto nutné odlíšiť prípady pri ktorých už samotné vyhotovovanie obrazových záznamov je trestným činom (napríklad výroba detského pornografického diela, kde podstatou tohto trestného činu je zákaz vyhotovovania obrazových záznamov, ktoré vykazujú znaky detského pornografického diela) od prípadov, pri ktorých vyhotovovanie obrazových záznamov trestné nie je, ale len zachytáva niečo (spravidla priebeh skutku), ktorý už trestným môže byť.

ľa Trestného poriadku a nemusí byť vždy získaný (vypátraný) len zo strany orgánov činných v trestnom konaní. Navyše, ustanovenie § 119 ods. 3 Tr. por. vyslovene stanovuje, že dôkazy môžu obstarávať aj strany na vlastné náklady. Uvedené ustanovenie teda jednoznačne predpokladá a umožňuje aktivitu procesných strán pri obstarávaní dôkazov využiteľných v trestnom konaní.

Základnou podmienkou na pripustenie dôkazu v trestnom konaní tak pre orgány činné v trestnom konaní ako aj pre súkromné osoby je to, aby bol dôkaz obstaraný zákonne, t. j. v súlade s Trestným poriadkom, či osobitným zákonom.

Ak sa teda niekedy namieta, že žiadne ustanovenie Trestného poriadku nestanovuje pre súkromné osoby pravidlá pre zabezpečenie záznamu vyhotoveného súkromnou osobou, tak ide o námietku nesprávnu, nakoľko takouto normou je práve ustanovenie § 119 ods. 2 Tr. por., ktoré stanovuje podmienku prípustnosti dôkazu do trestného konania a tou je podmienka zákonnosti, teda podmienka stanovujúca, že dôkaz musí byť získaný postupom podľa Trestného poriadku alebo podľa osobitného predpisu. Takýmto osobitným predpisom je aj Občiansky zákonník s tým, že pri vyhotovovaní súkromných nahrávok iných osôb musí byť rešpektované ustanovenie § 12 Občianskeho zákonníka.

Pomerne prekvapivou v tomto smere je trestná rozhodovacia činnosť Najvyššieho súdu SR,[18] ktorý v trestnej veci skonštatoval, že vyhotovovanie obrazovozvukových záznamov utajovaným spôsobom môže kolidovať s ustanovením § 12 Občianskeho zákonníka. Na rozdiel od verejnoprávnych úprav (trestnoprávnej a administratívnej) však súkromnoprávna úprava dôkaznú použiteľnosť záznamu v trestnom konaní neobmedzuje (obsahuje len sankcie uvedené v § 13 a 16 Občianskeho zákonníka), nevyníma teda taký záznam z definície „všetkého" čo môže byť použité ako dôkaz v zmysle § 119 ods. 2 Tr. por. Záznam ako dôkazný prostriedok však musí byť orgánmi činnými v trestnom konaní alebo súdom zabezpečený na účely trestného konania v súlade s Trestným poriadkom.

S týmto názorom sa nemožno stotožniť. Občiansky zákonník nemá ambície (dôvod) stanovovať sankcie nepoužiteľnosti konkrétneho dôkazu v trestnom konaní. Občiansky zákonník tu upravuje problematiku ochrany osobnosti a stanovuje neprípustnosť zásahov do súkromia fyzickej osoby bez jej súhlasu. Túto právnu úpravu pritom musia rešpektovať nielen súkromné fyzické osoby, ale aj štátne orgány, a to aj orgány činné v trestnom konaní pri dokazovaní trestnej činnosti. Nie je preto možné pripustiť dôkazy získané porušením Občianskeho zákonníka len lakonickým odkazom na to, že ide o súkromnoprávny predpis. Aj tu ide o zákon, pričom Trestný zákon, či Trestný poriadok nie je nadradený Občianskemu zákonníku.

Sankciu nepoužiteľnosti nezákonného dôkazu stanovuje pritom priamo ustanovenie § 119 ods. 2 Tr. por., ktoré pre použiteľnosť dôkazu vyžaduje, aby bol dôkaz získaný v súlade s Trestným poriadkom alebo osobitným zákonom. Takýto osobitným zákonom (ktorým spravidla je súkromnoprávny predpis) môže byť aj Občiansky zákonník a ak je dôkaz získaný v rozpore s ním je nezákonný a tým pádom aj vylúčený zo všetkého v zmysle § 119 ods. 2 Tr. por. (argumentum a contrario). Požiadavka zákonnosti získaného dôkazu je vyslovene vyjadrená aj v základnej zásade trestného konania uvedenej v ustanovení § 2 ods. 12 Tr. por. podľa ktorej orgány činné v trestnom konaní a súdy hodnotia len dôkazy získané zákonným spôsobom (t. j. dôkazy získané v rozpore s Trestným poriadkom alebo iným právnym predpisom nie sú spôsobilé na ustálenie skutkového stavu veci a nemôžu byť ani hodnotené v trestnom konaní). Nie je možné pripustiť, aby podkladom pri zisťovaní skutkového stavu veci v trestnom konaní boli nezákon-

[18] Uznesenie Najvyššieho súdu SR sp. zn. 2 Tost 4/2014 zo dňa 2. 4. 2014.

né dôkazy, ktoré by sa pripustili len z toho dôvodu, že boli získané iba v rozpore so súkromnoprávnymi normami.[19]

Nie je možné akceptovať taký záver, že pri zabezpečeovaní dôkazov existujú dve kategórie (druhy) nezákonnosti a to nezákonnosť spôsobená orgánmi činnými v trestnom konaní, respektíve súdom, ktorá má za následok nepoužiteľnosť takéhoto dôkazu v trestnom konaní a nezákonnosť spôsobená súkromnými osobami, ktorá je tolerovateľná a podľa okolností prípadu možno ustaľovať skutkový stav veci aj na podklade takéhoto nezákonného dôkazu. Umožniť súkromným osobám získavať dôkazy nezákonne nie je možné ospravedlniť, pretože otvára dvere svojvôli, ktorá môže končiť až v situáciách, v ktorých sa budú získavať dôkazy aj prostredníctvom páchania majetkovej, či násilnej trestnej činnosti.

5/ argument aplikáciou testu proporcionality – porovnanie váhy verejného záujmu na postihu konkrétneho trestného činu a uloženie sankcie jeho páchateľovi so záujmom jednotlivca, aby dôkazy v jeho neprospech boli zadovážené zákonnou cestou

Tento argument pre využitie nezákonne získaných súkromných nahrávok v trestnom konaní vychádza z toho, že je nutné prihliadnuť na váhu verejného záujmu na postihu za konkrétny trestný čin a na uloženie jeho sankcie páchateľovi a túto porovnať so záujmom jednotlivca, aby dôkazy v jeho neprospech boli zadovážené zákonnou cestou. Takto získaná informácia môže byť dôkazom len za podmienky, že zásah do súkromia je odvoditeľný prevažujúcim záujmom na strane toho, kto informáciu takýmto spôsobom vyhotovil a následne použil. Koho záujem prevažuje by malo byť v každom jednotlivom prípade ponechané na zváženie súdu.[20]

Predmetný argument vzbudzuje pochybnosti o svojej správnosti už len z toho dôvodu, že plne závisí nie od objektívneho výkladu práva, ale od hodnotového (subjektívneho) nastavenia sudcu (prípadne policajta alebo prokurátora), ktorý vo veci rozhoduje. Neexistujú totiž žiadne objektívne kritériá pri aplikácii ktorých by sa dalo predvídať či u konkrétnej osoby, ktorá rozhoduje preváži verejný záujem na postihu za spáchaný trestný čin alebo preváži záujem jednotlivca, aby dôkazy v jeho neprospech boli zadovážené v súlade so zákonom.

Odborná literatúra[21] sa síce snaží tento subjektívny postup „vťahovania" nezákonného dôkazu do trestného konania objektivizovať za vytvárania viacerých špecifických kritérií (napríklad aká je povaha trestného činu, pre ktorý sa vedie trestné stíhanie, či vyhotovením záznamu bol sledovaný legitímny cieľ alebo nie, či ide o jediný usvedčujúci dôkaz a podobne), avšak aj tieto kritériá sú založené čisto na subjektívnom hodnotovom nazeraní na výklad práva, sú pomerne vágne a umožňujú „schovať" pod seba prakticky akýkoľvek (ľubovoľný) obsah.

Nie je pritom jasné prečo vôbec boli vytvorené, keď k otázke nezákonnosti dôkazov existuje ustanovenie § 119 ods. 2 Tr. por. ako aj ustanovenie § 2 ods. 12 Tr. por., ktoré neumožňujú ich prelomenie na podklade literatúrou uvádzaných špecifických subjektívnych kritérií.

Navyše, nie je možné ani paušálne tvrdiť, že záujem na tom, aby usvedčujúce dôkazy boli získané zákonnou cestou je len záujmom jednotlivca a teda že tu stojí na jednej strane verej-

[19] Napokon, porušenie ustanovenia § 12 Občianskeho zákonníka sankcionuje Trestný zákon aj hmotnoprávne a to napríklad skutkovou podstatou trestného činu porušenia dôvernosti ústneho prejavu a iného prejavu osobnej povahy podľa § 377 Tr. zák. K uvedenému pozri aj Šamko, P.: Zákonnosť a použiteľnosť dôkazov v trestnom konaní získaných utajovanou činnosťou detektívnej služby, Zo súdnej praxe č. 3/2017.

[20] Záhora, J. et al.: Obrazové a zvukové záznamy v trestnom konaní, Bratislava: Wolters Kluwer, 2018, s. 248, 249.

[21] Záhora, J. et al.: Obrazové a zvukové záznamy v trestnom konaní, Bratislava: Wolters Kluwer, 2018, s. 247 a nasl.

ný záujem (ako určitý vyšší princíp) a na strane druhej (len) záujem jednotlivca. Som názoru, že záujem na tom, aby páchateľom bola preukázaná ich trestná činnosť iba dôkazmi získanými v súlade so zákonom je taktiež záujmom verejným a nie iba záujmom jednotlivca. Celkom určite nie je vo verejnom záujme, aby sa trestná činnosť páchateľom preukazovala v rozpore so zákonom, respektíve, aby súkromné osoby zabezpečovali dôkazy za porušenia právneho poriadku, prípadne aby takouto činnosťou suplovali orgány činné v trestnom konaní.

Pri bezbrehom aplikovaní tohto spôsobu právnej argumentácie by potom bolo možné ospravedlniť akékoľvek porušenie zákona v dokazovaní verejným záujmom na objasňovaní trestnej činnosti a zisťovaní jej páchateľa. Ustanovenie § 119 ods. 2 Tr. por. nie je vyjadrením právneho formalizmu, ktoré musí, či má ustúpiť hodnotovému nazeraniu orgánu aplikácie práva, ktorý je názoru, že verejný záujem (nech už toto slovné spojenie znamená čokoľvek) môže „zlomiť" zákonnosť pri získavaní dôkazov ak je to nevyhnutné na podporenie konkrétnej dôkaznej situácie. Právne naopak, ustanovenie § 119 ods. 2 Tr. por. je právnou normou, ktorej obsah je zrejmý a je nutné ho rešpektovať.

Kedy je teda možné použiť (využiť) nahrávku inej osoby, ktorá bola vyhotovená súkromnou osobou ako dôkaz v trestnom konaní?

Z hľadiska možného využitia súkromných nahrávok inej osoby v trestnom konaní možno uzatvoriť, že ako všeobecné pravidlo musí platiť neprípustnosť získavania dôkazov zo strany súkromnej osoby za porušenia ustanovenia § 11 a § 12 Občianskeho zákonníka, t. j. vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov inej osoby bez jej súhlasu, napríklad utajovaným spôsobom (a je bez významu, či ide o fyzickú osobu alebo právnickú osoba). Je neprijateľné, aby súkromná osoba cielene (úmyselne) porušovala uvedené ustanovenia Občianskeho zákonníka s tým, že tak robí z dôvodu možného získania informácie, ktorá by mohla byť použiteľná niekedy v blízkej, či vzdialenej budúcnosti v trestnom, či inom konaní. Špehovanie iných a vyhotovovanie ich podobizní, či zachytávanie ich hlasov na záznamové zariadenie utajovaným spôsobom s úmyslom, že „možno poskytnú nejaký dôkaz proti sebe" celkom určite nie je možné označiť za konanie, ktoré by malo byť tolerované, či chránené štátom a ktoré by malo byť postavené na rovnakú úroveň ako je získavanie dôkazov zákonným spôsobom, t. j. bez porušovania právnych predpisov. Účel by tu celkom určite nemal prelomiť spôsobenú nezákonnosť pri získavaní dôkazu a z dôvodu tejto nezákonnosti by mal byť takýto dôkaz vylúčený podľa § 119 ods. 2 Tr. por. a ako taký by nemal byť vôbec hodnotený orgánmi činným v trestnom konaní, či súdmi (§ 2 ods. 12 Tr. por.). Tu treba pripomenúť, že žiadne ustanovenie Trestného poriadku, Občianskeho zákonníka, či iného právneho predpisu neumožňuje štátu, či súkromným osobám systematické zaznamenávanie hlasových prejavov, či obrazových podobizní inej osoby a to len z dôvodu možného získania dôkazu proti takejto osobe. Takéto privilégium majú len orgány činné v trestnom konaní, či súdy (respektíve aj iné subjekty podľa zákona č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov) a aj to len v špecifických prípadoch a spravidla len na podklade rozhodnutia, či súhlasu sudcu.[22]

V tomto smere nutné opätovne zvýrazniť, že je neprípustné, aby si súkromná osoba (teda osoba odlišná od orgánu činného v trestnom konaní, či súdu) nahrávala utajovaným spôsobom obrazový, či zvukový prejav iného cielene len za tým účelom, aby ho vzápätí použila ako dôkaz v trestnom, či inom konaní. Názor, podľa ktorého ustanovenie § 12 ods. 2 Občianskeho zákon-

[22] K uvedenému pozri Šamko, P.: Zákonnosť a použiteľnosť dôkazov v trestnom konaní získaných utajovanou činnosťou detektívnej služby, Zo súdnej praxe, č. 3/2017.

níka je potrebné vykladať tak, že vo všeobecnosti Trestný poriadok dovoľuje zaznamenávať hlasové prejavy iných osôb a používať ich k dôkazným účelom je nutné považovať za neprípustne extenzívny. Vzťah ustanovenia § 12 Občianskeho zákonníka k Trestnému poriadku je taký, že tu ide o dve zákonné normy v zásade na sebe nezávislé, stojace vedľa seba. Samotný záujem získať informácie použiteľné neskôr v trestnom, či inom konaní ako dôkaz (obvykle práve proti osobe, ktorej prejav je nahrávaný) nie je dostatočným záujmom odôvodňujúcim porušenie práva na súkromie. A pretože tu o porušenie práva na súkromie nesporne ide, znamenal by prístup orgánov verejnej moci, pokiaľ by bez ďalšieho hodnotenia odôvodnenosti prielomu do súkromia inej osoby preberali takto získané informácie do dôkazného základu prejednávanej veci fakticky akúsi konvalidáciu nezákonnosti uskutočnenej v súkromnej sfére vykonanou ich úradným postupom. Preto nestačí len formálne zhodnotenie prípustnosti takto získaných informácií z hľadiska ich dôležitosti pre posúdenie merita veci spolu s posúdením autenticity zaznamenaného hlasového prejavu určitej osoby.[23]

Na strane druhej však treba zdôrazniť aj to, že absolútny zákaz použitia súkromných nahrávok pre dôkazné účely neplatí. Aj tu platia výnimky, ktoré môžu takéto zásahy za určitých konkrétnych podmienok odôvodniť.

Môže sa tak však stať iba vtedy, ak z okolností vyhotovenia súkromnej nahrávky bez rozumných pochybností vyplýva (a tento záver musí byť predmetom dokazovania), že táto bola vyhotovená napríklad za takých okolností, pri ktorých išlo o realizáciu výkonu práva zo strany osoby, ktorá nahrávku vyhotovila. Oprávnený výkon práva potom spôsobuje taký stav, že vyhotovenie súkromnej nahrávky nie je porušením zákona, ale práve naopak, právom predpokladaným konaním. Keďže tu pôjde o postup v súlade so zákonom, nepôjde o dôkaz nezákonný a tým pádom ho bude možné vykonať v trestnom konaní a prípade aj na ňom založiť odsúdenie obžalovaného.

Do kategórie zásahov do práva na súkromie zo strany súkromných osôb, ktoré bude v súlade s právom možno zaradiť tieto prípady:

a) svojpomoc v zmysle § 6 Občianskeho zákonníka

Podľa § 6 Občianskeho zákonníka, ak hrozí neoprávnený zásah do práva bezprostredne, môže ten, kto je takto ohrozený primeraným spôsobom zásah odvrátiť.

Svojpomoc je možná vtedy, ak sa nedá dovolať pomoci zo strany verejnej moci. Ide tu o výnimku z pravidla, že ochrana subjektívnych práv patrí zásadne štátnym orgánom. Len celkom výnimočne a to vtedy, ak hrozí bezprostredné nebezpečenstvo, že by právna ochrana štátnym orgánom prišla neskoro, umožňuje Občiansky zákonník, aby fyzická osoba sama, aktívne a primeraným spôsobom odvrátila neoprávnený zásah. Dovolená obranná svojpomoc je okolnosťou vylučujúcou protiprávnosť a je možná iba celkom výnimočne.[24]

Súčasťou svojpomoci je nielen to, že sa bezprostredne napadnutý môže (má právo) brániť proti neoprávnenému zásahu, ale aj to, že si tento svoj postup môže dokumentovať (napríklad si vyhotovuje obrazový, zvukový alebo obrazovozvukový záznam o konaní útočníka). Musí ísť však o konanie útočníka, ktoré hrozí bezprostredne (t. j. má byť vykonané ihneď), respektíve ide o konanie útočníka, pri ktorom neoprávnený zásah už nastal a nebol ukončený. Skutočnosť, že

[23] Primerane Stanovisko Nejvyššího státního zastupitelství ČR ke sjednocení výkladu zákonů a jiných právních předpisů k použitelnosti magnetofonového záznamu rozhovoru jako důkazu v trestním řízení, Por. č. 2/2004, SL 750/2001.

[24] K uvedenému pozri bližšie napríklad Fekete, I.: Občiansky zákonník 1. Veľký komentár, Bratislava: Eurokódex 2011, s. 72 a nasl.

sa poškodený bráni proti neoprávnenému zásahu pritom neznamená, že sa voči nemu musí aj ubrániť. O svojpomoc teda nejde len vtedy, ak je úspešná.

V aplikačnej praxi bolo ako svojpomoc napríklad posúdené konanie poškodenej (manželky obžalovaného), ktorý ju fyzicky napadol, pričom poškodenej sa podarilo tesne pred fyzickým útokom zapnúť nahrávacie zariadenie na svojom mobilnom telefóne a takto (z časti aj obrazovo) zdokumentovať priebeh skutku (t. j. fyzický útok manžela, svoju obranu ako aj slovný prejav manžela, ktorý sa jej pri útoku aj vyhrážal). Táto nahrávka bola použitá v trestnom konaní ako zákonne získaný dôkaz, nakoľko bolo skonštatované, že pri konaní poškodenej boli splnené všetky zákonné podmienky svojpomoci v zmysle § 6 Občianskeho zákonníka, t. j. išlo o konanie zákonné a to vrátane obrazovozvukového dokumentovania priebehu skutku.

Obdobne to bolo aj v prípade vedenom pre trestný čin znásilnenia, pri ktorom poškodená dokázala zachytiť priebeh skutku na zvukový záznam, ktorý bol následne použitý ako zákonný dôkaz v trestnom konaní na podporu svedeckej výpovede poškodenej.

V tejto súvislosti je však nutné zdôrazniť, že celkom určite za konanie, ktoré sa blíži podmienkam dovolenej svojpomoci alebo krajnej núdzi nie je možné označiť prípad z praxe, v ktorom došlo jedným z manželov k namontovaniu sledovacieho zariadenia priamo do obývačky bytu s tým, že išlo o cielené celoročné nahrávanie tohto priestoru so zámerom, že druhý z manželov sa skôr, či neskôr dopustí protiprávneho konania a to domáceho násilia.

Za nezákonné a zjavne sa vymykajúce podmienkam svojpomoci je nutné označiť aj prípady, v ktorých išlo o monitorovanie (priestorové za využitia skrytých kamerových systémov) kancelárií, či motorových vozidiel obchodných partnerov, respektíve osôb, ktoré spolupôsobili v štatutárnych orgánoch obchodných spoločností (napríklad monitorovanie jedného konateľa zo strany druhého konateľa tej iste obchodnej spoločnosti, v ktorej pôsobili spoločne).

b) analogické použitie ustanovenia § 85 ods. 2 Tr. por.

V tomto smere je nutné pripomenúť, že podľa ustanovenia § 85 ods. 2 Tr. por. môže ktokoľvek obmedziť osobnú slobodu inej osoby, ktorá bola pristihnutá pri trestnom čine alebo bezprostredne po ňom, ak je to potrebné na zistenie jej totožnosti, zabránenie úteku, zabezpečenie dôkazov alebo zabráneniu ďalšiemu páchaniu trestnej činnosti.

Z dôvodu nutnosti zabezpečenia dôkazov o osobe možného páchateľa trestného činu a jeho totožnosti možno toto ustanovenie analogicky vtiahnuť aj na prípady, pri ktorých príde k spáchaniu trestného činu (napríklad krádeže, výtržníctva, vraždy, nebezpečného vyhrážania, nebezpečného prenasledovania a podobne), pričom podozrivá osoba bude napríklad utekať z miesta činu bezprostredne po jeho spáchaní a iná osoba si takúto utekajúcu osobu nahrá napríklad na mobilný telefón, respektíve vyhotoví jeho fotografiu. Môže ísť aj o prípady, pri ktorých fyzická osoba napríklad nahrá na mobilný telefón celý priebeh trestného činu (napríklad fyzický útok páchateľa na poškodeného).

V takýchto prípadoch ide síce o konanie, ktoré je formálne v rozpore s ustanovením § 12 Občianskeho zákonníka, avšak zároveň ide o konanie, ktoré sa materiálne blíži zadržaniu podozrivej osoby zo strany inej osoby, t. j. pôjde o konanie obdobné tomuto inštitútu a preto dôkazy takto získané budú v trestnom konaní prípustné, nakoľko tu pôjde o oprávnený výkon práva v zmysle § 85 ods. 2 Tr. por.

Pokiaľ totiž ustanovenie § 85 ods. 2 Tr. por. umožňuje obmedzenie osobnej slobody podozrivej osoby pristihnutej na mieste činu, či bezprostredne po ňom akejkoľvek osobe a fakticky akýmkoľvek primeraným spôsobom, ktorým sa dosiahne účel tohto ustanovenia, potom sa celkom určite zákonu neprieči ani také konanie, ktorým príde k „chyteniu“ podozrivej osoby, či k obrazovo zvukovému zdokumentovaniu priebehu trestného činu prostredníctvom záznamu

podozrivej osoby, čo je menej závažnejší zásah voči podozrivej osobe ako jej obmedzenie osobnej slobody a navyše, je aj menej nebezpečný pre osobu, ktorá záznam vyhotovuje. Od súkromnej osoby, ktorá napríklad nahrá na svoj mobilný telefón priebeh trestného činu vraždy, celkom určite nemožno vyžadovať, aby zároveň aj postupovala podľa § 85 ods. 2 Tr. por. a obmedzila páchateľa na osobnej slobode, ak vzhľadom na osobu páchateľa, či okolnosti prípadu by bolo takýmto konaním zjavne sama vystavená nebezpečenstvu. V takýchto prípadoch je preto možné postupovať aj analogicky v zmysle § 85 ods. 2 Tr. por. a podozrivú osoby, či osoby, respektíve priebeh skutku, ktorý by mohol vykazovať znaky skutkovej podstaty trestného činu zachytiť na nahrávacie zariadenie a o prípade aj utajovaným spôsobom.[25]

K uvedenému analogickému argumentu využitia § 85 ods. 2 Tr. por. je nutné uviesť, že analógia v trestnom práve procesnom je prípustná. Navyše, v danom prípade ani nejde o analógiu v neprospech podozrivého, ktorá by zasahovala do jeho práv viac (nadmieru) než je umožnený zásah do osobnej slobody podozrivej osoby v zmysle § 85 ods. 2 Tr. por. Je nutné vychádzať z toho, že sa tu síce postupuje obdobne ako je uvedené v ustanovení § 85 ods. 2 Tr. por. („chytenie podozrivého" prostredníctvom obrazového záznamu), avšak s tým, že zásah do práv podozrivej osoby je minimálny (len zachytenie priebehu skutku vrátane podozrivej osoby fotograficky, či prostredníctvom videa). Nahráva sa skôr samotný priebeh skutku (možné spáchanie trestného činu), ktorý vytvára podozrivá osoba svojím konaním. Fakticky je to analógia v prospech podozrivého, nakoľko ten, kto zachytáva priebeh skutku volí (často z dôvodu vlastnej bezpečnosti) namiesto intenzívneho zásahu do osobnej slobody podozrivého (obmedzenie osobnej slobody podozrivého v zmysle § 85 ods. 2 Tr. por.) zásah neporovnateľne miernejší, ktorý sa týka iba vyobrazenia podozrivého.

c) dodatočný súhlas nahrávanej osoby

V aplikačnej praxi sa môžu vyskytnúť prípady, v ktorých boli napríklad obrazové záznamy konkrétnej fyzickej osoby vyhotovené utajeným spôsobom (bez vedomia) tejto fyzickej osoby, respektíve napriek jej výslovnému nesúhlasu, t. j. v rozpore s ustanovením § 12 Občianskeho zákonníka, avšak následne táto fyzická osoba svoj súhlas udelí a chce, aby sa tieto obrazové záznamy využili ako dôkazy v trestnom konaní.

V tomto smere je nutné zdôrazniť, že ustanovenie § 12 Občianskeho zákonníka je založené na ochrane hodnôt ľudskej osobnosti, ktoré sa týkajú prejavov osobnej povahy fyzickej osoby. Do týchto hodnôt možno zasahovať len so súhlasom dotknutej fyzickej osoby. Ak s takýmto zásahom dotknutá osoba súhlasí, ide o zásah legálny, ktorý sa neprieči ustanoveniu § 12 Občianskeho zákonníka. Nie je žiadny dôvod na to, prečo by postup v rozpore s ustanovením § 12 Občianskeho zákonníka nemohol byť „napravený" dodatočným súhlasom dotknutej fyzickej osoby, nakoľko ochrana ustanovenia § 12 Občianskeho zákonníka sa týka iba a výslovne dotknutej fyzickej osoby, s možnosťou dobrovoľného pripustenia zásahov do vlastných osobnostných práv.

Takýto dodatočný súhlas dotknutej fyzickej osoby by však mal byť riadne a podrobne zadokumentovaný v príslušnej zápisnici o výsluchu tejto osoby. Ak sa tak stane, potom počiatočná relatívna nezákonnosť získaného dôkazu „odpadne" a dôkaz bude využiteľný v trestnom konaní.

d) páchateľ si nahráva svoju obeť

V neposlednom rade je nutné uviesť aj prípady, v ktorých si sám páchateľ (respektíve spolupáchateľ) zaznamenáva páchanie vlastnej trestnej činnosti, ktorej sa dopúšťa voči inej fyzickej osobe (napríklad páchateľ si nahráva ako znásilňuje ženu, respektíve ako mučí inú osobu, či drží inú osobu uväznenú v miestnosti a podobne).

[25] Táto koncepcia bola využitá aj v uznesení Krajského súdu v Bratislave sp. zn. 4To/61/2018 zo dňa 8. 11. 2018.

Výklad ustanovenia § 12 Občianskeho zákonníka je pritom založený na tom, že dotknutá fyzická osoba má slobodnú vôľu a slobodne sa môže rozhodnúť, či dá alebo nedá súhlas v zmysle § 12 ods. 1 Občianskeho zákonníka. Narušiteľ túto vôľu dotknutej fyzickej osoby buď nerešpektuje alebo ani nezisťuje (napríklad pri vyhotovovaní záznamov fyzickej osoby utajovaným spôsobom).

V prípadoch, pri ktorých bol spáchaný trestný čin alebo je ešte páchaný a páchateľ (alebo spolupáchateľ) si obeť, ktorá je pod vplyvom páchaného trestného činu, zaznamenáva, je nutné vychádzať z toho, že vôľa osoby proti ktorej je páchaný trestný čin nie je nikdy slobodná. Vzhľadom k uvedenému sa takáto osoba ani nemôže reálne (racionálne) rozhodovať v zmysle § 12 ods. 1 Občianskeho zákonníka a aplikácia tohto ustanovenia tu vôbec neprichádza do úvahy. Práve preto je nutné pripustiť, že takéto záznamy obetí vyhotovované páchateľmi nie sú nezákonné a preto ich možno použiť v trestnom konaní ako dôkazy. Skutočnosť, že páchateľ trestného činu sám vyhotovuje dôkazy o svojej trestnej činnosti (napríklad nahrávanie si znásilnenia) nie je totiž v rozpore so zákonom.

Záver

Nosným východiskovým bodom pri úvahách či umožniť, respektíve neumožniť prienik nezákonne získaných dôkazov do dokazovania v trestnom konaní by malo byť poznanie, že zisťovaniu skutkového stavu veci nie je možné účelovo obetovať zákonnosť ako nosný pilier spravodlivého trestného procesu. Ani pravda nemôže byť zisťovaná za každú cenu. Pokiaľ sa pripustí porušovanie zákona pri získavaní dôkazov zo strany súkromných osôb, potom je to cesta, ktorú možno označiť za koniec trestného procesu (akýchkoľvek pravidiel dokazovania), nakoľko otvára dvere akémukoľvek porušovaniu zákona. Nie je preto možné rezignovať na to, akým spôsobom bol dôkaz získaný, respektíve ignorovať nezákonnosť jeho získania a to len z dôvodu, že nám obsah tohto dôkazu vyhovuje pri ustaľovaní skutkového stavu veci nevyhnutného na rozhodnutie.

Výrazným legislatívnym nedostatkom súčasnej právnej úpravy je skutočnosť, že posudzovanie použiteľnosti, respektíve nepoužiteľnosti záznamov získaných súkromnými osobami v trestnom konaní nemá žiadnu výslovnú právnu úpravu, t. j. žiadne jasné, zrozumiteľné a predvídateľné pravidlá. Rozhodnutia orgánov aplikácie práva sú tak v podobných prípadoch často veľmi protichodné a nemožno tu hovoriť ani o ustálenej súdnej praxi, ktorá by aspoň nahrádzala absentujúcu právnu úpravu.

De lege ferenda by bolo vhodným prijať samostatný zákon, ktorý by sa týkal posudzovania použiteľnosti dôkazov vo všeobecnosti (pravidlá by platili bez ohľadu na to, či by išlo o dôkaz získaný súkromnými osobami alebo štátom), t. j. išlo by o právnu normu, ktorá by sa zaoberala nezákonnosťou dôkazov, neprípustnosťou dôkazov a stanovovala by aj následky s tým spojené (napríklad doktrínu ovocia z otráveného stromu), pričom by mala obsahovať aj prípady (uvedené aspoň demonštratívne), kedy pri vyhotovovaní záznamov fyzickej osoby vyhotovenej zo strany súkromnej osoby nehrá ustanovenie § 12 Občianskeho zákonníka žiadnu úlohu, t. j. prípady, za akých by sa v trestnom konaní mohol takýto dôkaz použiť.

Koncepcie a funkcie používania ITP v procesoch kriminálno-policajného poznania

Concepts and Functions Use ITP in Criminal-police Knowledge

Miroslav Lisoň[1]
Michal Marko[2]

***Abstrakt**: Autori v príspevku vymedzením koncepcií a funkcií používania ITP v procesoch kriminálno-policajného poznania zdôrazňujú prínos teórie, ktorú spolu so svojimi kolegami kreujú v systéme policajných vied. Osobitne zastávajú názor, že výstupy z použitia ITP sú akceptovateľným dôkazom.*

***Abstract:** In defining the concepts and functions of using ITP in criminal-police knowledge processes, the authors emphasize the added value of the theory that they and their colleagues create in the police science system. In particular, they consider that the outputs from the use of ITP are acceptable evidence.*

***Kľúčové slová:** kriminálno-policajné poznanie, teória kriminálno-policajného poznania, informačno-technické prostriedky, informačno-technický úkon, trestné konanie, dokazovanie.*

Keywords: criminal-police knowledge, theory of criminal-police knowledge, information-technical means, information-technical act, criminal proceedings, taking of evidence.

Úvod

V súlade s požiadavkami praxe (*spoločnosti*) je možné vysloviť záver, že v reálnom čase je potrebné identifikovať a riešiť rozpory medzi dynamicky sa meniacou bezpečnostnou situáciou a relatívne stabilnými (*niekedy aj zastaranými*) policajnými prístupmi pri jej riešení (*napríklad pretrvajúca dominancia retrospektívneho prístupu v procese kriminálno-policajného poznania je zjavná*). Uvedené skutočnosti sú odborníkom na bezpečnosť (*ale aj pomerne veľkej časti občanov*) zrejmé a preto permanentne hľadajú odpovede na otázky: *„Prečo sa v tomto smere nevykoná náprava?“*, *„Aké dôvody sú využívané pri akceptovaní doteraz preferovaných riešení?“* a iné.

Aplikovaným výskumom sme dospeli k záveru, že v týchto intenciách príslušníci polície si uvedomujú, že pocit a potreba bezpečnosti je základnou spoločenskou potrebou. Rešpektujú, že bez adekvátneho riešenia bezpečnosti nie je možná reálna ekonomická prosperita, zvyšovanie a skvalitňovanie životného štandardu obyvateľov, rozvoj ich slobodných aktivít vo všetkých spoločenských sférach i ochrany ich dôstojnosti. Tieto skutočnosti výrazne ovplyvňujú samotnú ich orientáciu a prístup k plneniu úloh v duchu poslania *„Pomáhať a chrániť“*.[3]

Analogickým výkladom uvedených postulátov je možné vysloviť záver, že dosahovanie úspechu na úseku kontroly kriminality je podmienené funkčnosťou systému policajného konania. Jeho charakteristika je priamo spájaná odpoveďami na otázky: *„Čo je to polícia, a ktoré jej činnosti môžeme označiť prívlastkom policajné?“* Dá sa povedať, že nie je chybou, ak pri hľadaní odpovedí na tieto zdanlivo jednoduché otázky sú vymedzené funkcie polície v spoločnosti

[1] Prof. Ing. Miroslav Lisoň, PhD. Akadémia Policajného zboru v Bratislave, katedra kriminálnej polície, Sklabinská 1, 835 17 Bratislava, e-mail: miroslav.lison@minv.sk.

[2] JUDr. Michal Marko, PhD. Akadémia Policajného zboru v Bratislave, katedra kriminálnej polície, Sklabinská 1, 835 17 Bratislava, e-mail: michal.marko@minv.sk.

[3] LISOŇ, M. – Š. KOČAN a kol. Odhaľovanie a dokazovanie trestných činov v ekonomike. Akadémia PZ v Bratislave, VÝSK. 177.

a zdôvodnená účelová diverzifikácia zodpovednosti policajných subjektov pri plnení zákonom delegovaných úloh. Zjednodušene povedané, skutočnosť, že policajné konanie je charakterizované mimoriadnym bohatstvom obsahu, mnohostrannosťou javov, udalostí a vzťahov, vyžaduje aj zodpovedajúcu rôznorodosť metód, postupov a prostriedkov pri účelovej realizácii jeho činností. Preto je potrebné z metodologického a metodického hľadiska v štruktúre policajného konania generovať určité činností (*kategórie*), ktoré sa od seba líšia tak právnym základom, zameraním, ako aj metódami a prostriedkami.[4] Prax potvrdzuje, že bez spracovanej teórie tieto požiadavky, v súlade s identifikovanými potrebami nie je možné plniť.

1 Kriminálno-policajné poznanie

Spravodajská činnosť, operatívno-pátracia činnosť a policajné vyšetrovanie sú súčasťou štruktúry policajného konania. V policajnej praxi, pri poznávaní určitých trestných činov tieto špeciálne činnosti tvoria systém. Pre potreby policajnej praxe a teórie je vhodné, ak je tento systém skúmaný, vysvetľovaný a projektovaný ako jednotný celok, ktorý je vhodné označiť termínom *kriminálno-policajné poznanie*.

Spravodajská činnosť, operatívno-pátracia činnosť a vyšetrovanie vykazujú charakter techník (*techniky postupu*), ktoré v súlade s identifikovanou potrebou (*účelovo*) sú integrované v systéme kriminálno-policajného poznania. Tieto činnosti pri plnení stanovených úloh predstavujú variantné spôsoby postupov v štruktúre tohto systému. Ich spoločnými realizačnými znakmi (črtami) predovšetkým sú: – súčasť (*prvky*) systému policajného konania; účel – funkcie – špecifické poznávanie; objekty poznávania – kriminálne aktivity, trestné činy, kriminalita; subjekty poznávania – policajné orgány, orgány štátnej správy. Aj preto je možné pri ich skúmaní, hodnotení, vysvetľovaní a projektovaní použiť jednotnú metodológiu.

Praktickú opodstatnenosť kriminálno-policajného poznania potvrdzujú výsledky a efekty, ktoré sú príslušníkmi polície dosahované pri plnení stanovených úloh. Ich analýzou je možné dospieť k záveru, že systémová realizácia kriminálno-policajného poznania (*využívaním kompetencií – právna regulácia + zodpovednosť*) pozitívne ovplyvňuje úroveň objektivity, účinnosti a efektivity pri poznávaní trestných činov. Je tomu tak preto, lebo za určitých situácií v tomto postupe príslušníci polície:

- získavajú informácie, na základe ktorých orgány činné v trestnom konaní môžu začať trestné stíhanie a vzniesť voči konkrétnym osobám obvinenia a vykonávať dokazovanie,
- zhromažďujú informácie o kriminálnej scéne a dôkladnou analytickou prácou vypracovávajú podklady potrebné na systematické, ofenzívne, cieľavedomé pôsobenie proti kriminalite,
- prenikajú do organizačnej štruktúry kriminálnych skupín (*organizované, zločinecké, extrémistické, teroristické*), predovšetkým neobmedzujú sa len na zisťovanie informácií o páchateľoch bezprostredne vykonávajúcich trestný čin, ale predovšetkým o osobách, ktoré stoja v pozadí, riadia trestnú činnosť, o finančníkoch a právnych poradcoch, ktorí zabezpečujú ich ochranu,
- kontrolujú a deštruujú logistiku kriminálnych skupín a zisťujú zámery a plány súvisiace s páchaním ďalšej trestnej činnosti skôr, než je spáchaná.[5]

[4] HOLOMEK, J. – T. ŠIMANOVSKÁ Úvod do metodológie praktických vied: Policajné vedy ako vedy praktické. Bratislava, 2002, s. 42.

[5] MUSIL, J. Použití operativní techniky k důkazním účelům v trestním řízení. In. Trestní právo č. 4–5/1999, s. 19.

Analógiou uvedeného je možné konštatovať, že kriminálno-policajným poznaním sú plnené informačné, sociálne, právne, výchovné, preventívno-represívne, bezpečnostné, policajné, spravodajské, operatívne a v neposlednom rade procesné funkcie. V daných súvislostiach kriminálno-policajné poznanie predstavuje:

- saturáciu potrieb (*spoločenských, občianskych, policajných, operatívnych*, *procesných*, *praktických, teoretických, základných, aplikačných*),
- špecifický podsystém činností (*má svoju osobitú genézu, prvky, vnútorné vzťahy medzi prvkami, vzťahy prvkov k okoliu, je model...*),
- svojou podstatou riešenie problému (*definovanie otázok, východísk, cieľov, postupov, výstupov, hodnotení...*),
- selekciu nových informácií a vytváranie informačných sietí (*zdroje, zber, uchovanie, triedenie, interpretácia – vo vzťahu k využitiu*),
- adekvátnu aplikáciu právom regulovaných postupov (*na základe už skôr spracovaných informácií*),
- špecifický prejav aktivít, ktoré vykonávajú kompetentné orgány štátnej správy (*ich obsah a štruktúru tvoria opatrenia a úkony*),
- prejav účelovo a cieľavedome aplikovaných aktivít (*pri realizácii sa plnia konkrétne úlohy*),
- riadené aktivity (*intencionálna činnosť, na jej aplikáciu sú vytvárané podmienky uľahčujúce sebarealizáciu jej subjektov*) a pod.

K uvedeným tézam je vhodné dodať, že základný predpoklad úspechu pri realizácii tejto špecifickej policajnej činnosti určuje úroveň koordinácie. V teórii, jej význam možno zdôvodniť využitím analytickej a funkcionalistickej (*konštruktivistickej*) charakteristiky jeho realizačného systému. V praxi takto spracované teoretické poznanie je možné využiť pri skúmaní koordinačných vzťahov, hodnotení ich prínosov a projektovaní.

Z empírie vyplýva, že základným znakom systému kriminálno-policajného poznania je neustála transformácia a cirkulácia informácií v dynamike vývoja. Transformácia informácií v tomto systéme prebieha tým spôsobom, že výstup z jedného procesu (*SČ – OPČ – vyšetrovanie*) je zároveň vstupom do ďalšieho. Vznik, kvantitatívna a kvalitatívna zmena informácií (*vznik, rast odumieranie a zánik*) tvoria pevný reťazec vzájomnej väzby, ktorý sa uplatňuje rovnako pri najjednoduchšom (*napríklad údaj*), ako aj pri jeho najzložitejšom organizovanom prvku, ktorý predstavuje výstupný informačný produkt, napríklad spravodajská informácia – operatívna informácia – návrh na obžalobu.[6]

2 Teória kriminálno-policajného poznania

Teória zaujíma významné miesto v samotnom systéme poznávania. Výsledky teoretického poznávania sú predpokladom úspešnej realizácie ľudských činností. 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 policajného konania významným spôsobom prispieva k napĺňaniu princípov slobody, demokracie a práva v súlade s jednotlivými funkciami právneho štátu.

[6] VAŠKO, A. Spravodajská operácia v trestných veciach. In. Aktuálne otázky aplikácie kriminálneho spravodajstva v kontexte nových trendov v Európskej únii, s. 67.

Nový stav pri rozvoji policajných teórií objektívne vzniká tým, že sa mení vedecká situácia, ktorá ovplyvňuje realizáciu vedeckej činnosti a akceptáciu jej výsledkov v teoretickej a praktickej oblasti (*v našom ponímaní veda, ktorá má širokospektrálny rozmer*).

Analogicky uvedené skutočnosti sú rešpektované pri riešení otázok súvisiacich s teóriou kriminálno-policajného poznania, ktorú v podmienkach Slovenskej republiky (*vychádzajúc z identifikovaných potrie policajnej praxe a teórie*) kreujú v systéme policajných vied pracovníci Akadémie PZ v Bratislave.[7] K tejto vedeckej činnosti za dôležité je možné označiť skutočnosť, že kreovaná teória má svojich konkrétnych adresátov. Tými sú príslušníci spravodajských služieb, Policajného zboru a iných policajno-bezpečnostných zložiek, v neposlednom rade pracovníci prokuratúry a justície. Je tomu tak preto, lebo v predmetnej teórii kriminálno-policajného poznania sú vymedzené základné zákonitosti a faktory, ktoré determinujú podstatu a obsah systémovo realizovaných procesov spravodajskej činnosti, operatívno-pátracej činnosti a vyšetrovania. Z hľadiska konkrétnych funkcií predkladanej teórie ide predovšetkým o rozpracovanie otázok základného pojmového aparátu, právnej normatívnej regulácie a explanácie kriminálno-policajného poznania, ako celistvého systému (*kategórie*) pri jeho účelovej realizácii. V záujme naplnenia týchto cieľov sú teóriou kriminálno-policajného poznania:

- špecifikované všeobecné teoreticko-metodologické východiská kriminálno-policajného poznania (*teória, metodológia, poznatky*);
- v nadväznosti na predchádzajúci stupeň poznania a s dôrazom na systémové poňatie analyzované základné faktory determinujúce realizáciu kriminálno-policajného poznania;
- sformulované princípy kriminálno-policajného poznania, ako základné idey odrážajúce ich entity a poslanie v spoločnosti, pri rešpektovaní špecifík objektov pôsobenia;
- vymedzené črty, štruktúra a realizačné možnosti tohto špecifického policajného poznania ako systému;
- vymedzené hlavné organizačno-taktické formy účelovo realizovaných činností v systéme kriminálno-policajného poznania odrážajúce jeho funkcie a obsah (*na základe dosiaľ vykonaného skúmania*);
- vytvorené dostatočné informačné predpoklady na aplikáciu výskumu kriminálno-policajného poznania v systéme policajného konania.

Výber metód využitých pri spracovaní teórie je predestinovaný (*predurčený*) charakterom objektu, ktorý je skúmaný a vysvetľovaný jej špecifickým predmetom. Autori teórie pri ich voľbe rovnako rešpektujú stanovené ciele pri plnení konkrétne vymedzených úloh v oblasti praxe a teórie. Akceptáciou uvedených faktov a obmedzujúcich determinantov aplikujú teoretickú analýzu. Je tomu tak preto, lebo touto metódou je možné pochopiť zložitosť i rozporuplnosť javov prebiehajúcich v oblasti realizácie kriminálno-policajného poznania v systéme policajného konania. Autori pri skúmaní jeho vývoja a rozbore súčasného stavu dôsledne uplatňujú historický a systémový prístup. Ich prezentovaný vyhradený postoj k teoretickému rozpracovaniu problematiky kriminálno-policajného poznania rešpektuje objektívne dané podmienky príslušnej etapy rozvoja spoločnosti. Tieto skutočnosti potvrdzujú, že v obsahu spracovanej teórie sú konkrétne formulované stanoviská, v ktorých sa hlavný dôraz kladie na činnostné poňatie kriminálno-policajného poznania (*napríklad procesy*) rozhodujúce pri plnení stanovených úloh v policajnej praxi. Z ďalších metód využívajú predovšetkým metódy logiky – *analýza, syntéza, dedukcia a indukcia, analógia a iné logické operácie*, bez ktorých nie je možné dosiahnuť adekvátnu úroveň objektívneho poznania. Rovnako aplikujú metódu komparácie, ktorej využitie vy-

[7] LISOŇ, M. – VAŠKO, A. a kol. Teória kriminálno-policajného poznania. Bratislava: Wolters Kluwer, 2018; Bratislava, 389 s., ISBN 978-80-8168-838-6.

kazuje adresnosť predovšetkým pri určovaní identity kriminálno-policajného poznania v Slovenskej republike a iných štátoch – predovšetkým v rámci EÚ. V neposlednom rade v procese kreovania teórie využívajú aj svoje osobné skúsenosti a informácie získané priamym pozorovaním ako základným zdrojom empirickej informácie o objekte skúmania (*kriminálno-policajné poznanie*) v reálnych podmienkach a tiež konzultácie s príslušnými odborníkmi praxe s následným zovšeobecňovaním ich skúseností (*osobitne v priebehu vzdelávania s poslucháčmi Akadémie PZ v Bratislave*).

3 Informačno-technické prostriedky v systéme účelovej realizácie procesov 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 tieto determinujúce faktory príslušníci polície môžu pozitívne ovplyvňovať, predovšetkým použitím 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.[8]

Prostriedky používané v kriminálno-policajnom poznaní predstavujú subjekty, nástroje, pomôcky, zariadenia alebo ich súbory, ktorými je možné dosahovať vyššiu účinnosť a efektivitu práce pri plnení stanovených úloh.[9]

Rešpektujúc súčasnú úroveň poznania pre potreby praxe a teórie kriminálno-policajného poznania prostriedky ITP sú klasifikované do skupiny:

- **operatívno-technických prostriedkov (*prostriedky techniky*)**

V súčasnosti v podmienkach Slovenskej republiky je možné za **operatívno-technické prostriedky KPP** považovať **informačno-technické prostriedky** (*ďalej len ITP*) a **prostriedky ná-**

[8] ŠULC, Vladimír. Možnosti kybernetické bezpečnosti v teorii a praxi. Ústav informatiky. Mendelova univerzita v Brně. Sborník. s. 17 – 18.

[9] Prostriedky kriminálno-policajného poznania:
- Operatívno-informačné – získavaní cieľovej informácie (informácií), resp. pri plnení konkrétnej úlohy používaním operatívno-informačných prostriedkov dochádza k rozloženiu síl a zodpovednosti v rámci koordinácie medzi realizujúcim príslušníkom a prostriedkom (kooperujúci subjekt). 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:
  - Trestný poriadok – zámena obsahu zásielok § 110; kontrolovaná dodávka § 111; predstieraný prevod § 112; sledovanie osôb a vecí § 113; agent § 117,
  - Zákon o PZ – sledovanie osôb a vecí, monitorovanie osôb a dopravných prostriedkov, kontrolovaná dodávka, kriminálne spravodajstvo, používanie krycích dokladov, nástrahová a zabezpečovacia technika a využívanie osôb konajúcich v prospech PZ, objekty a miesta používané pod legendou a predstieraný prevod veci.
- Operatívno-logistické – krycie doklady a objekty a miesta používané pod legendou (zákon o PZ § 39 ods. 1). Používaním týchto prostriedkov sú vytvárané predpoklady pre realizáciu KPP (nie je nimi priamo realizované poznanie).
- Operatívno-technické.

strahovej a zabezpečovacej techniky (*ďalej len PNT*).[10] 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 sťaží.

Príslušníci polície v kriminálno-policajnom poznaní prostriedky operatívnej techniky používajú na účel získania a fixovania informácií o prebiehajúcom konaní alebo stavoch, ktoré toto konanie vyvolalo (*spôsobilo*). Ich účinnosť a efektivita je závislá od výkonnostných parametrov techniky *(technologické zdroje informácií).*

„*Ako funguje používanie ITP v reálnom policajnom prostredí?*"

Niet sporu o tom, že formulácia tejto otázky je účelová. Svojou obsahovou štruktúrou je zosúladená s teoretickou a praktickou potrebou používať tieto prostriedky v tomto špecifickom poznaní. Pri objektivizácii týchto konštatácií akceptujeme, že príslušníci polície pri plnení úloh ITP môžu použiť iba v prípadoch, 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. Ich použitím sa môže obmedziť základné právo alebo sloboda len v nevyhnutnom rozsahu a nie dlhšie, ako je nevyhnutné na dosiahnutie zákonom uznaného cieľa, na ktorý slúži.

Napríklad v Slovenskej republike použitie ITP limituje „*katalóg trestných činov*" (*kriminálno-policajné situácie*), pri riešení ktorých môžu byť vykonané opatrenia a úkony intenzívne zasahujúce do občianskych práv a slobôd. Nasadenie ITP musí byť v každom prípade pod kontrolou, ktorú vykonáva kompetentný orgán. Údaje získané týmito prostriedkami možno použiť výlučne na dosiahnutie účelu pri plnení úloh štátu, ktoré spĺňajú zákonom stanovené podmienky.[11]

Bez ohľadu na úplnosť je možné uviesť, že príslušníci polície v systéme realizácie KPP používaním informačno-technických prostriedkov môžu pozitívne ovplyvniť najmä plnenie úloh pri:

- zisťovaní, upresňovaní a dokumentovaní mechanizmu protispoločenského (*kriminálneho*) konania,
- identifikovaní subjektov, spolupáchateľov a iných zúčastnených osôb na protispoločenskom konaní (*obrazový zvukový záznam, ..., fonoskopia, kriminalistická biomechanika ...*),
- zisťovaní a fixovaní informácií o protispoločenskom konaní, ktoré môžu byť využité ako dôkazy v trestnom konaní (*ktoré by mohli byť zničené alebo nevykonané*),
- zisťovaní informácií o úkrytoch páchateľov, vecí pochádzajúcich z protispoločenského konania (*nástroje, predmet záujmu, ...*),
- identifikovaní komunikácie medzi subjektmi protispoločenského konania (*pozícia a rola subjektov, frekvencia, časopriestor vo vzťahu k štádiám páchania trestného činu, ...*)
- dokumentovaní procesov KPP (*predovšetkým pre potreby dokázania zákonnosti, resp. previerok týchto postupov*),
- zvyšovaní účinnosti a efektivity na úseku ochrany informácií (*zabezpečovaní informačnej ochrany pri realizácii procesov KPP v celom systéme kriminálno-policajného poznania*),

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

[11] VAŠKO, A. Informačné výstupy zo spravodajskej činnosti v trestnom konaní. In. Aktuálne otázky trestného práva v teórii a praxi. 6. ročník interdisciplinárnej celoštátnej vedeckej konferencie s medzinárodnou účasťou. Zborník, Bratislava, 2018, s. 336.

- odhaľovaní manipulácie s predmetom spravodajského (*operatívneho, vyšetrovacieho*) významu (*zisťovaní zásahov, výmeny účtovnej, resp. inej ekonomickej dokumentácie, osobných dokladov, verejných listín a iných dokumentov*, ..., *prienik osoby do záujmového objektu,* ...),
- kontrolovaní aktivít príslušníkov polície, ktorí realizujú KPP,
- kontrolovaní funkcionality používania prostriedkov KPP (*osobitne operatívno-informačných, operatívno-logistických – osôb konajúcich v prospech polície, legalizanta a agenta,* ...),
- zabezpečovaní ochrany určených osôb, strážených objektov, štátnych hraníc,
- poskytovaní ochrany a pomoci ohrozenému svedkovi a chránenému svedkovi,
- zabezpečovaní ochrany príslušníkov polície,
- realizovaní pátrania po osobách a veciach a iné.

Bez ohľadu na úplnosť, to potvrdzuje, že používaním ITP sú plnené rôzne funkcie. Výskum potvrdzuje, že realizátori kriminálno-policajného poznania bez poznania ich prejavu a podstaty nedosahujú požadovanú účinnosť a efektivitu pri ich používaní.[12]

4 Koncepcie a funkcie realizácie informačno-technických úkonov

V praxi príslušníci polície (*pri plnení konkrétnych úloh v systéme KPP*) určené objekty (*napríklad kriminálne aktivity*) poznávajú a hodnotia systémovo (*genéza, prvky, vzťahy,* ...). Pri akceptácii tohto prístupu realizujú opatrenia a úkony, pričom si uvedomujú, že paralelne s ich statickou – normatívnou podobou (*abstraktnou*), existuje aj skutočná (*reálna*), ktorú sú povinní projektovať a používať pri plnení úloh v konkrétnej kriminálno-policajnej situácii.

Výsledky aplikovaného výskumu potvrdzujú, že príslušníci polície na základe informačných výstupov z používania ITP určujú ďalší smer realizácie kriminálno-policajného poznania. Osobitne dosahujú vyššiu úroveň ofenzívnosti (*cieľavedomosť, rýchlosť, aktuálnosť,* ...) pri práci s informáciami, ktorá pozitívne determinuje vykonávanie dôkazov (*dokazovanie – začatie trestného stíhania, vznesenie obvinenia, realizácia neodkladných a neopakovateľných úkonov*) a pod.

Použitie konkrétneho ITP sa realizuje prostredníctvom *informačno-technického úkonu.*

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

Za začiatok použitia prostriedkov operatívnej techniky v konkrétnom prípade sa rozumie čas ich uvedenia do funkčného stavu, zabezpečujúceho získavanie a zhromažďovanie informácií.

Za ukončenie použitia sa považuje moment, ktorým sa znemožní získavanie a zhromažďovanie informácií.

Demontáž je časový úsek, ktorý je nevyhnutne potrebný na odstránenie technického prostriedku z miesta inštalácie.

Výstupom z technického úkonu je záznam v predpísanej forme (*ďalej len „výstup*"), ktorý sa vyhotovuje v jedinom výtlačku a okrem vlastnej informácie obsahuje najmä označenie vyžadujúcej súčasti, stupeň utajenia, registračné číslo zväzku, krycí názov akcie, dátum a čas získania informácie, dátum spracovania výstupu a identifikačnú značku spracovateľa.

Subjektom oprávneným využívať technický úkon sú kompetentní príslušníci polície.

[12] PETRUSEK, M. – A. MILTOVÁ – A. VODÁKOVÁ. Sociologické školy, směry, paradigmata. (ediční řada Sociologické pojmosloví – svazek 4). Praha, 1994. s. 110 – 111. „Funkcia je dôsledkom, ktorý vyvolala určitá aktivita, proces alebo existencia nejakého sociálneho alebo kultúrneho faktu v istom celku sociálnej štruktúry. Funkcia je teda jednoznačne definovaná predovšetkým ako dôsledok činnosti (sociálne a kultúrne fakty sú koniec-koncov samy vždy výsledkom nejakej činnosti), pričom nemusí ísť o zamýšľaný dôsledok.

Používanie operatívnej techniky na účely kriminálno-policajného poznania technicky zabezpečujú policajné servisné pracoviská (*servisné pracoviska*). Tie sú zriadené spravidla v organizačných štruktúrach polície. Ich činnosť je spojená s *realizáciou* informačno-technického úkonu (*ITÚ*) po technickej stránke. To znamená, že ITÚ je parciálnou časťou v systéme realizácie používania ITP.

Kreovaná teória kriminálno-policajného poznania akceptuje tieto skutočnosti pri skúmaní, hodnotení a vysvetľovaní používania ITP pri plnení delegovaných úloh. Osobitne v tomto smere sú spracovávané koncepcie, ktorých obsah vymedzuje nielen právne zásady používania, ale aj filozofiu legislatívnej úpravy. Podľa nášho názoru význam tohto prístupu spočíva okrem iného aj v tom, že akceptáciou koncepcii sú vytvárané predpoklady pre projektovanie tejto špecifickej činnosti v systéme kriminálno-policajného poznania. V konečnom dôsledku s tým je spájaná samotná funkcionalita používania ITP.

Tieto skutočnosti je možné objektivizovať explanáciou obligatórnych realizačných zložiek používania ITP, ktorých programový systém tvoria:

- koncepcie pri ich projektovaní a aplikácii (*všeobecne formulované pre trestné činy určitého druhu kriminality; pre určitý druh trestného činu; vnútroštátne, resp. medzinárodné využitie*),
- komponenty – (*poznávacie a formatívne*),
- cieľové štandardy (*aktuálna adresná zodpovednosť – tvorba a distribúcia (prezentácia) metodík; začlenenie metodík do prípravy príslušníkov a hodnotenie ich akceptácie pri napĺňaní účelu*),
- identita kompetencií vo vzťahu k potenciálnym adresátom,
- programy a ich variabilnosť (*obligatórne a fakultatívne opatrenia v kriminálno-policajných situáciách; účel; prístup – projektovanie, plánovanie*)
- potreba a parametre ich hodnotenia.

Podľa názoru autorov teórie kriminálno-policajného poznania v tomto systéme sa javí, ako vhodné použiť najmä:

1. Personálnu koncepciu – príslušníci polície pri projektovaní ITP využívajú svoju odbornosť, ktorou saturujú identifikované potreby poznania pri dosahovaní stanoveného cieľa (*aj s aplikovaním intuitívnych metód – „cit pre detail"*); uvedomujú si svoju pozíciu a rolu v tomto procese (*sloboda, autonómia, direktíva, sebarealizácia, tvorivosť, zodpovednosť...*). Analogicky uvedené sa vzťahuje aj na orgány, ktoré sú oprávnené schvaľovať použitie ITP.

Táto koncepcia je rozpracovaná v kontexte potreby rešpektovania zásady legality pri zásahoch do základných ľudských práv a slobôd.

2. Sociálno-kognitívnu koncepciu – zainteresované orgány si uvedomujú, že používaním ITP riešia konkrétny problém v spoločnosti (*potreba poznania a význam ITP*) v určenej štrukturálnej schéme. V jej obsahu reflektujú požiadavky vyplývajúce zo zásady proporcionality. Použitie ITP musí byť zosúladené s existujúcimi spoločenskými potrebami.

3. Právno-technologickú (systémovú) koncepciu – do realizačného obsahu ITP implementujú možnosti riešenia, legitimita a legitimizovanie postupu (*existujúci problém je riešiteľný – dispozícia zodpovednosti – miestna a vecná príslušnosť – právna regulácia*), vytvárajú predpoklady na dosiahnutie vyššej úrovne účinnosti a efektivity (*zjednodušenie*).

4. Štrukturálno-obsahovú koncepciu (prakticko-konštrukčnú) – pri preberaní zodpovedností akceptujú konkrétne procedúry výberu, štruktúry a usporiadania, teda to, čo má byť obsahom realizácie (*proces konštruovania, zostavovania na konkrétny účel*). K uvedenému je vhodné dodať, že možnosti používania ITP sú limitované, napríklad zásadou subsidiarity, vymedzeným

objektom a časovým úsekom. Pri používaní ITP je nutná koordinácia, osobitne medzi vyžadujúcim subjektom, servisným pracoviskom a schvaľujúcim orgánom.

5. Komunikatívnu koncepciu – vo vzťahu k práci s ITP vnímajú a akceptujú sprostredkované poznanie, využívajú (*napríklad interdisciplinárne*) overené poznanie, konštruktívne ponúkajú nové riešenia. V daných súvislostiach je vhodné uviesť, že táto koncepcia vo vzťahu k používaniu ITP je v odborných kruhoch stále pertraktovaná. Je tomu najmä preto, lebo jej akceptácia je spájaná s využívaním dosahovaných informačných výstupov z ITP v trestnom konaní.

Z tohto pohľadu pri účelovom používaní ITP za špecifické je možné označiť právne reglementačný obsah jej realizačných komponentov. Je tomu tak preto, lebo tento obsah vytvára základné predpoklady účinnej a efektívnej kontroly realizácie a pod

V tomto zmysle je možné koncepcie používania ITP vysvetľovať a hodnotiť (*vnímať*) v dvoch významových rovinách.

V *„praktickej rovine"* – v zmysle konštruovania a analýzy konkrétnych postupov pri realizácii ITP a ich využívania v reálnych činnostiach KPP – osobitne v dokazovaní. V *„teoretickej rovine"* ako získavanie, zovšeobecňovanie a poskytovanie skúseností. Vo vzťahu k potencionálnemu a reálnemu používaniu ITP význam týchto poznaní je vhodné spájať s možnosťami spracovania používania metodík pre riešenie konkrétnych situácií. Ide napríklad o formálno-právnu a materiálno-právnu akceptáciu zodpovednosti za použitie ITP. V inom prípade ide o abstrahovanie, mnohokrát prezentáciu vízií a postulátov o tom, čo má byť optimálnym obsahom skúseností, ktoré majú ponúkať zásady, metodiky a pod.

Výsledky aplikovaného výskumu potvrdzujú, že v systéme projektovania a používania ITP tieto koncepcie vykazujú širšiu systémovú dimenziu, ktorú je možné využiť pri určovaní a hodnotení ich funkcií. Napríklad z hľadiska potrieb praxe (*zdôrazňujeme, že bez ohľadu na úplnosť*) je možné vymedziť funkcie ITP:

- *akceptácie adresnej zodpovednosti,*
- *organizácie a riadenia postupu* – návod pre príslušníka polície, ktorý je povinný reagovať na konkrétnu kriminálno-policajnú situáciu,
- *poznávania – poznania*,
- *kontroly a hodnotenia,*
- *objektívnej prezentácie získaných a zovšeobecnených informácií* – súbor informácií, ktoré sú ponúkané na praktické využitie, osobitne v dokazovaní a pod.

V týchto intenciách je vhodné zvýrazniť funkciu zložky *„cieľové štandardy"*, ktorá o. i. konkretizuje vzťah teórie a praxe. Napríklad úlohou policajnej teórie je, aby pre potreby praxe vypracovala kritériá, ktoré je možné využiť pri objektívnom hodnotení prínosu ITP (*komunikácia, informovanosť; vzájomné prepojenie teórie a praxe a pod.*), resp. teoretickou explanáciou vymedziť prístupy, zásady, a iné konštrukty a odporúčania na ich spracovanie.

Z toho vyplýva, že poznanie podstaty koncepcií a funkcií ITP, ktoré príslušníci polície používajú pri plnení úloh v určitých kriminálno-policajných situáciách, je *„conditio sine qua non"*. Bez tohto poznania nie je možné reálne uvažovať o ich projektovaní a optimalizácii, a to vo vzťahu k zvyšovaniu účinnosti a efektívnosti ich používania.

Záver

Vzájomná podmienenosť (*prepletanie a doplňovanie*) analýzy a syntézy je typická nielen pre celkovú realizáciu kriminálno-policajného poznania, ale aj parciálne postupy využívané v rámci plnenia konkrétnej úlohy použitím ITP v ich systémovej štruktúre.

Prax permanentne potvrdzuje, že pri používaní ITP sú registrované rezervy. Osobitne, ich eliminácioU je možné zvýšiť účinnosť a efektivitu identifikácie trestných činov (*odhaľovanie a objasňovanie*). Otázkou je: „*Prečo prax nedokáže tieto poznané rezervy odstrániť*?" Zastávame názor, že príčinou tohto stavu je pretrvávajúci konzervativizmus a dogmatizmus v právnickej obci.

Právna prax už dlhodobo nedoceňuje pozíciu a rolu teoretického poznania. Z tohto dôvodu vítame a oceňujeme doteraz dosiahnuté výstupy z plnenia vedecko-výskumnej úlohy: „*Zvyšovania efektívnosti odhaľovania a dokazovania trestných činov prostredníctvom informačno-technických prostriedkov*" realizovanej kolektívom vedecko-výskumných pracovníkov Fakulty práva Paneurópskej vysokej školy pod vedením prof. JUDr. Jozefa Záhoru, PhD.[13]

Literatúra

HOLOMEK, J. – T. ŠIMANOVSKÁ *Úvod do metodológie praktických vied*: *Policajné vedy ako vedy praktické.* Bratislava, 2002, s. 42.

LISOŇ, M. – Š. KOČAN a kol. *Odhaľovanie a dokazovanie trestných činov v ekonomike.* Akadémia PZ v Bratislave, VÝSK. 177.

LISOŇ, M. – VAŠKO, A. a kol. *Teória kriminálno-policajného poznania*. Bratislava: Wolters Kluwer, 2018; Bratislava, 389 s., ISBN 978-80-8168-838-6.

MUSIL, J. *Použití operativní techniky k důkazním účelům v trestním řízení*. In. Trestní právo č. 4–5/1999, s. 19.

PETRUSEK, M. – A. MILTOVÁ – A. VODÁKOVÁ. *Sociologické školy, směry, paradigmata*. (ediční řada Sociologické pojmosloví – svazek 4). Praha, 1994. s. 110 – 111.

ŠULC, Vladimír. *Možnosti kybernetické bezpečnosti v teorii a praxi.* Ústav informatiky. Mendelova univerzita v Brně. Sborník. ISBN 978-80-7509-512-1. s. 17 – 18.

VAŠKO, A. *Spravodajská operácia v trestných veciach*. In. Aktuálne otázky aplikácie kriminálneho spravodajstva v kontexte nových trendov v Európskej únii, ISBN 978-80-8054-760-8, s. 67, 134 s.

VAŠKO, A. *Informačné výstupy zo spravodajskej činnosti v trestnom konaní.* In. Aktuálne otázky trestného práva v teórii a praxi. 6. ročník interdisciplinárnej celoštátnej vedeckej konferencie s medzinárodnou účasťou. Zborník, Bratislava, 2018, ISBN 978-80-8054-764-6, 369 s.

ZÁHORA, J. a kol. *Obrazové a zvukové záznamy v trestnom konaní*. Bratislava: Wolters Kluwer SR, 2018. ISBN 978-80-8168- 957-4, 284 s.

Zákon č. 171/1993 Z. z. o Policajnom zbore 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 č. 301/2005 Z. z. trestný poriadok v znení neskorších predpisov

[13] ZÁHORA, J. a kol. Obrazové a zvukové záznamy v trestnom konaní. Bratislava: Wolters Kluwer SR, 2018. 284 s.

K vybraným otázkám důkazního použití odposlechu pořízeného zpravodajskými službami

Selected Problems of Intelligence Interception as an Evidence in Criminal Proceeding

Ladislav Pokorný[1]

Abstrakt: *Článek se zabývá otázkou možného použití odposlechu pořízeného zpravodajskými službami ČR jako důkazu v trestním řízení. Upozorňuje na Nález Ústavního soudu ČR sp. zn. I. ÚS 3038/07, který vylučuje možnost důkazního použití záznamu odposlechu pořízeného zpravodajskou službou, a dále popisuje současný vývoj, který směřuje k legislativnímu řešení, které by mělo tuto možnost připustit.*

Abstract: *This article deals with issue of possibility of using of intelligence interception used by Intelligent services of Czech Republic as an evidence in criminal proceeding. Furthermore, it deals with decision of Constitutional court, which excludes the possibility of using of intelligence interception. Thereafter it describes contemporary development, which is heading to legislative solution, which should admit this possibility.*

Klíčová slova: *důkaz, trestní řízení, zpravodajské služby, zpravodajský odposlech, ČR*

Key words: *evidence, criminal proceeding, intelligence services, intelligence interception, Czech rep.*

Úvod

Důkazní právo zažívá významný pohyb, posilují se garance zákonnosti a formální požadavky použití jednotlivých druhů důkazních prostředků a zároveň se hledají cesty k efektivnímu postihu nových podob závažné kriminality, na něž klasické důkazní prostředky nejsou dostatečně účinné. Vývoj vyžaduje mj. reagovat na nové jevy v kriminalitě a zajistit potřebu efektivních právních nástrojů k eliminaci závažných podob trestné činnosti.

Ve vybraných oblastech bezpečnostních hrozeb, jakými jsou terorismus, organizovaný zločin, špionáž, hrozby v kyberprostoru aj., plní významnou roli zpravodajské služby, které disponují oprávněním používat, za podmínek stanovených zákonem, specifické prostředky získávání informací, mezi něž patří i odposlech a záznam telekomunikačního, radiokomunikačního a jiného obdobného provozu. Mají tak nástroj, jímž mohou pro plnění v oboru své působnosti získávat informace, které nelze běžnými postupy dosáhnout, a které by mohly být významné pro důkazní použití v trestním řízení. Zpravodajské služby však nejsou orgány činnými v trestním řízení, a v České republice, na rozdíl od mnoha jiných států, včetně Slovenska,[2] není důkazní použití záznamů odposlechu pořízeného zpravodajskou službou přípustné.

Otázka možného důkazního použití zpravodajských informací, zejména pak možnost použití záznamu odposlouchávání, popřípadě zaznamenávání telekomunikačního, radiokomunikačního nebo jiného obdobného provozu, popřípadě zjišťování údajů o tomto provozu, jako jedné z forem použití zpravodajské techniky Bezpečnostní informační službou či Vojenským

[1] Doc. JUDr. Ladislav Pokorný, Ph. D., Právnická fakulta Masarykovy univerzity v Brně, e-mail: 23588@mail.muni.cz.

[2] Srov. Ivor, J. Využitie informácií spravodajských služieb v trestnom konaní. In. Spravodajské služby v demokratickej společnosti. Zborník zo sympózia, Bratislavská vysoká škola práva, Bratislava 2009, s. 66. Aláč, M. Osobitosti použitia ITP v posobnosti Slovenskej informačnej služby. In Záhora, J. (ed.) Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní. Leges, Praha 2017, s. 268–275.

zpravodajstvím na základě zákona o Bezpečnostní informační službě či zákona o Vojenském zpravodajství mimo trestní řízení,[3] je tak jedním z témat, které je v této souvislosti aktuálně diskutováno.

Zejména v případech takových činů a jevů, které se v trestněprávní terminologii označují jako závažné formy kriminality, zejména terorismus, organizovaný zločin, apod., se dosavadní rezervovaný přístup k novým důkazním prostředkům jeví jako hodný diskuse především v otázce použitelnosti prostředků legálně pořízených, avšak za současného statu quo dosud důkazně nepoužitelných. Jako legitimní se tak jeví otázka, má-li stát nechat nevyužity informace relevantní pro trestní řízení, které jsou legálně a legitimně opatřeny a provedeny, a kterými již některý z jeho orgánů legálně disponuje.

Tyto úvahy a záměry jsou v České republice ostatně již formulovány v některých koncepčních materiálech vládních i legislativních – viz dále.

Úloha zpravodajských služeb se v ČR omezuje na *sběr informací a následnou analýzu a interpretaci* tohoto materiálu pro oprávněné adresáty. Veškeré *výkonné funkce náleží řádné policii nebo jiným orgánům*, zpravodajské služby se na trestním řízení nikterak nepodílejí, policie a vnitřní zpravodajské služby jsou důsledně odděleny. Česká republika patří mezi země, kde platí zásadní oddělení informačních a exekutivních pravomocí. Je příkladem užšího vymezení okruhu oprávnění zpravodajských služeb (zejm. absence výkonných pravomocí policejního typu), což vyplývá z jednoznačné aplikace oddělovacího imperativu, užšího pojetí jejich mandátu a nepřiznání postavení orgánu typu law enforcement.

V případě *zpravodajských služeb* je jejich posláním chránit stát a společnost tím, že ústavním činitelům a orgánům státní správy opatřují včasné, objektivní a kvalitní zpravodajské informace, zajišťují analýzu v oblastech významných pro národní bezpečnost. Sféra působnosti zpravodajských služeb není vymezena oblastí trestního práva, činnost zpravodajských služeb není – na rozdíl od represivních složek – podmíněna trestným či protizákonným jednáním zájmového objektu, postačuje, že toto jednání představuje hrozbu pro hodnoty, které jsou do působnosti zpravodajských služeb zákonem svěřeny (bezpečnost, ústavní pořádek, významné ekonomické zájmy, utajované informace …). Předmětem zájmu zpravodajských služeb pak jsou takové aktivity, které tvoří hrozbu pro národní bezpečnost bez ohledu na to, jsou-li právně kvalifikované jako trestný čin či nikoli.

Kromě role důležitého zdroje kvalifikovaných podkladů pro tvorbu bezpečnostní politiky státu, plní zpravodajské služby roli nezastupitelného zdroje informací při průběžném zvládání bezpečnostní situace v zemi.[4] Jedna z rolí spočívá tedy i v poskytování informací pro jiné státní a policejní orgány v oboru jejich působnosti. Tato nalezla odraz v ust. § 8 odst. 3 zákona o zpravodajských službách České republiky, podle kterého zpravodajské služby předávají státním a policejním orgánům informace o zjištěních, která náleží do oboru jejich působnosti; to neplatí, jestliže by poskytnutí ohrozilo důležitý zájem sledovaný zpravodajskou službou.[5]

V případě získání informací vedoucích k důvodnému podezření z naplnění skutkové podstaty trestného činu pak, mají-li být trestněprávně využitelné, musí tedy následovat předání těchto

[3] Viz zákon č. 154/1994 Sb. o Bezpečnostní informační službě (§§ 8 až 12) a zákon č. 289/2005 Sb. o Vojenském zpravodajství (§§ 8 až 12). V dalším textu bude tam, kde to bude z kontextu pochopitelné, pro zjednodušení pro tyto případy používán zkrácený termín „zpravodajský odposlech".

[4] Srov. Duchek, J.: Zpravodajské služby při tvorbě a realizaci bezpečnostní politiky. Vojenské rozhledy. Teoretický časopis armády České republiky, 2005, číslo 1, s. 55.

[5] § 8 odst. 3 zákona č. 153/1994 Sb., o zpravodajských službách České republiky.

informací příslušným orgánům činným v trestním řízení. Dle relevantního nálezu ÚS[6] však těmito informacemi mohou být pouze povšechné informace operativní povahy.

I. Zpravodajské služby a specifické prostředky získávání informací

Za účelem plnění úkolů v oboru jejich působnosti je zpravodajským službám svěřeno oprávnění používat tzv. specifické prostředky získávání informací. Těmito jsou, vedle využívání služeb osob jednajících ve prospěch zpravodajských služeb, tzv. zpravodajské prostředky. Těmito jsou podle zákona o BIS (a obdobně zákona o VZ) zpravodajská technika, sledování a krycí prostředky a krycí doklady.[7]

Podle zákona č. 154/1994 Sb., o Bezpečnostní informační službě (a obdobně i podle zák. č. 289/2005 Sb., o Vojenském zpravodajství ve vztahu k VZ) (§ 7) je Bezpečnostní informační služba oprávněna v oboru své působnosti používat zpravodajské prostředky, kterými jsou a) zpravodajská technika, b) krycí prostředky a krycí doklady, a c) sledování. (2) Bezpečnostní informační služba je povinna zabezpečit ochranu zpravodajských prostředků před vyzrazením, zneužitím, poškozením, zničením, ztrátou a odcizením.

V souvislosti s důkazním použitím se budeme dále věnovat zpravodajské technice a ještě úžeji zpravodajskému odposlechu, a to vzhledem k tomu, že právě důkazní použití tohoto prostředku bylo předmětem posouzení ústavním soudem ČR, které bylo uzavřeno relevantním Nálezem I. ÚS 3038/07, který důkazní použití nepřipouští.

Zpravodajskou technikou se pro účely tohoto zákona rozumějí technické prostředky a zařízení, zejména elektronické, fototechnické, chemické, fyzikálně-chemické, radiotechnické, optické, mechanické anebo jejich soubory, používané utajovaným způsobem, pokud je při něm zasahováno do základních práv a svobod občanů mj. při odposlouchávání, popřípadě zaznamenávání telekomunikačního, radiokomunikačního a jiného obdobného provozu, popřípadě zjišťování údajů o tomto provozu.

Bezpečnostní informační služba může zpravodajskou techniku použít jen po předchozím písemném povolení předsedy senátu vrchního soudu příslušného podle sídla Bezpečnostní informační služby (dále jen „soudce“) a za předpokladu, že by odhalování nebo dokumentování činností, pro něž má být použita, bylo jiným způsobem neúčinné nebo podstatně ztížené nebo v daném případě nemožné. Použití zpravodajské techniky nesmí překročit rozsah povolení soudce podle odstavce 1 a nesmí zasahovat do práv a svobod občanů nad nezbytně nutnou míru.

Povolení k použití zpravodajské techniky vydává soudce na základě písemné žádosti, která obsahuje a) druh zpravodajské techniky, která má být použita, dobu trvání jejího použití, základní identifikační údaje o osobě, vůči které má být zpravodajská technika použita, pokud jsou tyto údaje známy, číslo telefonní nebo jiné obdobné stanice, pokud z ní má být prováděn odposlech, popřípadě záznam, a je-li známo, i místo použití zpravodajské techniky; má-li být zpra-

[6] Viz Nález ÚS ČR sp. zn. 3038/07 z 29. 2. 2008.

[7] Na Slovensku používaný termín „informačně technické prostředky“ není v právním řádu ČR používán. Používány jsou termíny „operativně pátrací prostředky“ (§§ 158b–158f trestního řádu), odposlech a záznam telekomunikačního provozu (§ 88 a 88a trestního řádu), pomocné OPP (§§ 72–77 zák. o Policii ČR – tyto neslouží k důkaznímu použití), zpravodajské prostředky (§§ 7–14a ZoBIS, §§ 7–15 ZoVZ). Stručný přehled zpravodajských prostředků v ČR viz Kloubek, M., Pokorný, L., Michálek, L. Prostředky operativně pátrací a zpravodajské činnosti v podmínkách České republiky. In Jozef STIERANKA, Michal MARKO a kolektiv: Aktuálne otázky aplikácie kriminálneho spravodajstva v kontexte nových trendov v Európskej únii. Akadémia policejného zboru v Bratislave. Bratislava 2018, s. 86–104.

vodajská technika použita vůči ústavnímu činiteli nebo jejím použitím má být zasahováno do práva nedotknutelnosti obydlí, musí být tato informace součástí žádosti, b) důvody pro použití zpravodajské techniky včetně odůvodnění podmínek pro její použití stanovených v § 9 odst. 1, c) informaci o jakékoliv předchozí žádosti o použití zpravodajské techniky vůči osobě uvedené v písmenu a) včetně informace, jak bylo o této žádosti rozhodnuto.

Soudce o žádosti o povolení zpravodajské techniky rozhodne bezodkladně. Rozhodnutí o povolení k použití zpravodajské techniky obsahuje druh zpravodajské techniky, která může být použita, dobu trvání jejího použití, základní identifikační údaje o osobě, vůči které má být zpravodajská technika použita, pokud jsou tyto údaje známy, číslo telefonní nebo jiné obdobné stanice, pokud z ní má být prováděn odposlech, popřípadě záznam, a je-li známo, i místo použití zpravodajské techniky, a odůvodnění.

Použití zpravodajské techniky lze povolit jen na nezbytně nutnou dobu, nejdéle však na dobu tří měsíců.

Rozhodne-li soudce o povolení zpravodajské techniky kladně, vydá současně výpis z tohoto rozhodnutí, který obsahuje nejnutnější identifikační údaje a zda při jejím použití může být zasahováno do práva nedotknutelnosti obydlí; výpis neobsahuje odůvodnění.

Zamítne-li soudce žádost o povolení k použití zpravodajské techniky, obsahuje rozhodnutí odůvodnění.

Proti rozhodnutí o povolení nebo zamítnutí žádosti o povolení k použití zpravodajské techniky není přípustný opravný prostředek.

Soudce je oprávněn požadovat od Bezpečnostní informační služby informace k posouzení, zda důvody pro používání zpravodajské techniky trvají.

Zjistí-li soudce, že důvody používání zpravodajské techniky pominuly, povolení k jejímu použití odejme.

Bezpečnostní informační služba bezodkladně písemně informuje soudce o ukončení používání zpravodajské techniky.

II. Důkazní použití záznamu zpravodajského odposlechu v trestním řízení – Nález ÚS sp. zn. I ÚS 3038/07

Pro posouzení otázky důkazní použitelnosti zpravodajských odposlechů je důležité posoudit především mandát zpravodajských služeb a jejich vztah a odlišnost od orgánů typu law enforcement a dále zákonné podmínky jejich oprávněného použití. Právě odlišný mandát zpravodajských služeb a úprava podmínek použití zpravodajského odposlechu mimo trestní řád, byly argumentem Ústavního soudu v rozhodném nálezu odmítajícím důkazní použití odposlechu pořízeného zpravodajskou službou.

Ústavní soud České republiky vyslovil závěr o nepoužitelnosti záznamu odposlechu pořízeného zpravodajskou službou v nálezu sp. zn. I ÚS 3038/07 ze dne 29. února 2008. Základním argumentem pro tento závěr byl (ad 1.) argument poukazující na odlišný mandát zpravodajských služeb, mandát, který spočívá v jiném účelu než je důkazní použití jimi získaných informací, byť materiálně obsahující relevantní informace, jimiž lze potvrdit či vyvrátit skutečnosti významné pro trestní řízení (tedy mandátem zpravodajských služeb, z něhož vyplývá jiné než důkazní použití) a dále (ad 2.) jeho pořízení na základě jiného zákona než trestního řádu a za jiných zákonných podmínek.

Ústavní soud České republiky ve zmíněném nálezu především konstatoval, že „Odlišný zákonný účel limituje paletu možnosti informací získaných zpravodajskými službami.“ Tímto jed-

noznačně vyjádřil, že rozhodujícím kritériem posuzování těchto institutů není jejich reálná věcná a zákonnými podmínkami daná podobnost, nýbrž jejich zákonný smysl, účel a cíl, který je navíc vyjádřen i úpravou těchto institutů v rozdílných zákonech – v trestním řádu, resp. v příslušném zvláštním zákoně – konkrétně v zákoně o Vojenském zpravodajství. Odlišení zpravodajských služeb a policie je založeno na cílech (účelech) svěřených pravomocí, resp. oprávnění k plnění úkolů v oblasti zákonem vymezené působnosti těchto státních orgánů. Toto kritérium je také, ve spojení však se závažností hrozícího nebezpečí, rozhodujícím v případě posuzování použitelnosti informací obsažených v záznamech zpravodajských odposlechů jako důkazu v trestním řízení.

Důležité je v této souvislosti také posouzení povahy tzv. operativních informací (ať už pořízených zpravodajskými službami či policií) a jejich případného využití v souvislosti s trestním řízením. Je-li tedy např. záznam odposlechu telekomunikačního provozu pořízený zpravodajskou službou nepoužitelný jako důkaz v trestním řízení, protože je v této souvislosti důkazem nezákonným (protože je pořízený podle jiného zákona, než podle trestního řádu), je pak legitimní otázka zákonnosti použití operativních informací jako podkladu pro další postup orgánů činných v trestním řízení. Byť samy jako důkaz neslouží, bez nich by pořízení samotných již použitelných důkazů (provedených podle trestního řádu) nebylo možné, protože by o nich tento orgán prostě nevěděl.[8] Nález ÚS ČR I. ÚS 3038/07 však s odkazem na § 8 odst. 3 zákona č. 153/1994 Sb., o zpravodajských službách České republiky, výslovně formuluje závěr o standardní použitelnosti operativních informací, poskytnutých zpravodajskou službou, pro další postup v trestním řízení, byť nikoli jako samotného důkazu.[9] Jejím použitím tedy lze získat podklady pro nalezení a provedení důkazu (dle trestního řádu) a nelze namítat její nepoužitelnost a neúčinnost s poukazem na to, že byl pořízen podle jiného zákona než podle trestního řádu. V této souvislosti je nicméně třeba zdůraznit nepřípustnost použití informací (ani jako operativních) z důkazů absolutně neúčinných. Možnost využití informací z absolutně neúčinného důkazu jako operativní informace a na jejich základě zajistit již procesně využitelné důkazy by bylo popřením principů právního státu.[10]

Je tedy nepochybné, že zpravodajské informace mohou být orgány činnými v trestním řízení využívány, za současného stavu ale pouze po provedení ve formě stanovené trestním řádem.

Je však nezbytné upozornit, že jako nejdůležitější závěry Ústavního soudu lze shrnout takto: ÚS se (přirozeně) opíral o současnou právní úpravu, a použití informací získaných zpravodajskými službami jako důkazu v trestním řízení nevylučuje absolutně. Pro případ takové změny právní úpravy stanoví nepřímo určité požadavky –

1) především garanční kvality, které vyžaduje trestní řád. Z toho pak plyne nezbytnost nové legislativní úpravy, která by tyto garance zakotvila a
2) úroveň bezprostřední hrozby, kvůli níž by bylo nutné prolomit ústavní garance základních práv za účelem ochrany jiných statků.

---

[8] Je to významné mj. i proto, že podle doktríny plodů z otráveného stromu (fruit of the poisonous tree doctrine), lze považovat informaci, která byla získána nezákonně za nepoužitelnou v trestním řízení. Je třeba poznamenat, že aplikace této doktríny je součástí nového trendu judikatury Ústavního soudu pro trestní řízení [viz Musil, J. Několik otazníků nad judikaturou ÚS ČR v době postmoderny (na příkladu prohlídky jiných prostor a pozemků). Kriminalistika 2011, č. 1, s. 19].

[9] „Zpravodajské služby jsou ve vztahu k trestnímu řízení zákonem o zpravodajských službách (§ 8 odst. 3 viz výše bod 24) zmocněny maximálně k poskytnutí povšechných informací operativního charakteru." Viz Nález ÚS ČR sp. zn. I. ÚS 3038/07, s. 7, bod. 28. „Informace získaná odposlechem provedeným zpravodajskými službami nemůže mít vyšší kvalitu, než jakákoli jiná operativní informace" (tamtéž, bod 29).

[10] Podrobněji viz Herczeg, J. Zásada „nemo tenetur" a práva obviněného v trestním řízení. Bulletin advokacie, 1–2/2010, s. 46.

Ad 1) Podstatné výhrady ÚS k důkaznímu použití zpravodajských odposlechů za současné právní úpravy lze shrnout takto:

Stíhání trestných činů je ústavně aprobovatelným veřejným zájmem, avšak jen pohybuje-li se veřejná moc uvnitř rámce předvídaného zákonem.[11]

Zpravodajské odposlechy (§ 12 až 16 zákona č. 67/1992 Sb., o Vojenském obranném zpravodajství, ve znění pozdějších předpisů, resp. § 7 až 12 a 15 zákona č. 289/2005 Sb., o Vojenském zpravodajství, či § 8 až 12 a 14 zákona č. 154/1994 Sb., o Bezpečnostní informační službě, ve znění pozdějších předpisů) a trestněprávní odposlechy (§ 88 a 158d tr. ř.) mají zcela odlišný zákonný režim a zákonem vymezený účel.[12]

Odlišný zákonný účel limituje paletu použitelnosti informací získaných zpravodajskými službami. Odlišnost od trestněprávních zásad plyne i z faktu, že do procesu poskytnutí informací jsou začleněny špičky výkonné moci (které Ústava České republiky vymezuje jako orgány politické). Zákon konkrétně stanoví ingerenci ministra obrany [srov. § 8 odst. 5 zákona č. 153/1994 Sb. a § 3 odst. 1 písm. b) zákona č. 67/1992 Sb.].[13]

Trestní řád tam, kde upravuje důkazní použití informací získaných prolomením svobody soukromí (zejm. § 88 a 158d tr. ř.), mlčí o možnosti použít jako důkazu odposlechů získaných na základě jiných zákonů.[14]

Trestní řád stanoví, jakým (jedině možným) způsobem lze dospět k závěru o vině či nevině obviněného a jak lze získávat potřebné důkazy, přičemž jeho ustanovení musí vyhovovat nárokům plynoucím z požadavku co nejšetrnějšího zásahu do základních práv jednotlivých osob v různých procesních postaveních. Použití zpravodajského odposlechu v trestním řízení jako důkazu viny nepředvídá ani trestní řád a ani zákon o Vojenském obranném zpravodajství.[15]

Zpravodajské služby jsou ve vztahu k trestnímu řízení zákonem o zpravodajských službách České republiky (§ 8 odst. 3 viz výše bod 24) zmocněny maximálně k poskytnutí povšechných informací operativního charakteru.[16]

Informace získaná odposlechem provedeným zpravodajskými službami nemůže mít vyšší kvalitu než jakákoli jiná operativní informace. Nejde přitom o formalistní závěr, nýbrž o aplikaci ústavní zásady, že zásahy do základních práv musí být předvídány zákonem, který pro dosažení svého účelu musí volit co nejšetrnější prostředky. Tajné sledování telefonických hovorů a shromažďování takových informací veřejnou mocí je přitom velmi vážným zásahem do základních práv. Zpravodajské odposlechy nedosahují garančních kvalit, které vyžaduje trestní řád (z rozhodnutí Rt 19/2004 nelze dovodit použitelnost takového důkazu), a proto (jak svrchu již uvedeno) jich nelze použít jako důkazu v trestním řízení, neboť v tomto smyslu nebyly získány zákonným způsobem.[17]

Ad 2) Možnost opačného závěru nastínil Ústavní soud v tomtéž Nálezu zároveň pro případ, že by Česká republika čelila bezprostřední hrozbě např. teroristického útoku, kvůli níž by bylo možné prolomit ústavní garance základních práv za účelem ochrany jiných statků.

Ústavní soud zde považuje za vhodné podotknout, že si je plně vědom, že terorismus [zmíněný Ministerstvem vnitra ve stanovisku citovaném výše v bodu 8.e)] představuje vážnou hrozbu,

[11] Nález ÚS ČR sp. zn. I ÚS 3038/07 z 29. 2. 2008, bod 16.
[12] Tamtéž, bod 23.
[13] Tamtéž, bod 24.
[14] Tamtéž, bod 25.
[15] Tamtéž, bod 26.
[16] Tamtéž, bod 28.
[17] Tamtéž, bod 29.

avšak v projednávané věci nečelila Česká republika bezprostřední hrozbě, kvůli níž by snad bylo nutné široce prolomit ústavní garanci základních práv za účelem ochrany jiných statků.[18]

Zájem na obraně státu je rovněž veřejným zájmem aprobovatelným ve smyslu čl. 4 odst. 4 Listiny. Mírnější podmínky, které zpravodajské zákony na průlom do soukromí kladou, jsou tolerovatelné jednak přísným omezením účelu použití získaných informací a jednak závažností konkrétně hrozícího nebezpečí [např. terorismus zmíněný in 8.e)].[19]

III. Možná řešení a doporučení

Nové podněty k přípravě nové právní úpravy obsahují především koncepční vládní materiály, zpracované a schválené v souvislosti s mapováním bezpečnostních hrozeb, a schopnosti státu jím čelit, především v oblasti terorismu a dalších závažných hrozeb. Těmito materiály jsou zejm. tzv. „Protiteroristický balíček"[20] a „Audit národní bezpečnosti",[21] resp. „Legislativní návrhy v oblasti vnitřní bezpečnosti," které jsou součástí „Akčního plánu pro boj proti terorismu na léta 2016 až 2018."[22]

Audit národní bezpečnosti měl za cíl ověřit schopnost státu identifikovat konkrétní bezpečnostní hrozbu a přijmout vůči ní preventivní opatření a schopnost reagovat na nastalou krizi, mj. odpovědět na otázku, zda je dostatečná stávající legislativa. Jako cíl si stanovil zjistit, jak je stát připraven čelit bezpečnostním hrozbám ve vytipovaných nejzávažnějších oblastech a jaká je jeho odolnost při přímé konfrontaci s nebezpečím. Posuzoval, zda je dobře nastavena legislativa a jak pružně je bezpečnostní systém schopný reagovat. Na závěr každé kapitoly pak vznesl doporučení, mj. právě legislativní návrhy od obecných až po velmi konkrétní návrhy dílčích změn. V souvislosti s tématem důkazní použitelnosti zpravodajských informací pak doporučuje dosáhnout jejich použitelnosti v oblasti *terorismu* („zpravodajské informace jako důkaz" – s. 25, a jako další opatření dokonce navrhnout změnu legislativy, která by v neodkladných případech umožnila zpravodajským službám a orgánům činným v trestním řízení na základě konkrétních informací nasadit úkony podléhající za normálních okolností schválení jiného státního orgánu /soudu/ ihned, přičemž by žádost o povolení byla předložena v dodatečné lhůtě /např. 48 hodin/ – s. 26), *organizovaného zločinu* („využití zpravodajských informací jako důkazu v trestním řízení" – s. 48 a jako další opatření „Prohloubit důvěru, kontakty a možnosti sdílení informací mezi zpravodajskými službami a útvary Policie ČR, aby docházelo k častější spolupráci v boji proti organizovanému zločinu a předávání takových informací, které budou všemi stranami tohoto vztahu využitelné." – s. 49) a *působení cizí moci* („Návrhy do oblasti trestního práva hmotného i procesního: možnosti využití zpravodajských poznatků v trestním řízení aj." – s. 61).

Posléze zmíněný materiál – Akční plán pro boj proti terorismu – zaměřený speciálně na *oblast boje proti terorismu,* zdůrazňuje nezbytnost toho, aby měly orgány činné v trestním řízení dostatečné procesní nástroje k zajištění důkazů. Konkrétně se věnuje tématu zpravodajských informací jako důkazu.[23] Uvádí situaci, kdy zpravodajská služba zjistí konkrétní informace k osobě podezřelé z určitého trestného činu, avšak prostředky, kterými toto jednání zdokumentuje, budou pro policii důkazně nepoužitelné a trestně právní postih takové osoby bude značně pro-

[18] Tamtéž, bod 31.
[19] Tamtéž, bod 17.
[20] Materiál podléhá utajení podle zákona č. 412/2005 Sb., o ochraně utajovaných informací, nebyl tedy publikován.
[21] Audit národní bezpečnosti. Schválený usnesením vlády č. 1125 dne 14. 12. 2016. Dostupný z www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf.
[22] Dostupné z www.mvcr.cz/cthh/clanek/akcni-plan-pro-boj-proti-terorismu-pro-leta-2016-az-2018.aspx.
[23] Tamtéž, s. 6.

blematický až vyloučený. Uvádí příklad odposlechu telekomunikačního provozu, který je ze své podstaty neopakovatelným úkonem, a uzavírá, že informace získané zpravodajskou službou by měly být využitelné v souladu s trestním řádem jako důkaz. Navrhuje, při respektování nálezu Ústavního soudu (I. ÚS 3038/07), „analyzovat, zda a jakým způsobem legislativně dosáhnout možnosti využití informací získaných v souladu se zákony o zpravodajských službách pro trestní řízení".

Záměry formulované ve zmíněných dokumentech však stanoví, a to poměrně obecně, toliko kýžený (žádoucí) výsledek. Tomuto však nezbytně bude muset předcházet nová legislativní úprava provedená v trestním řádu, a samozřejmě také v samotných zákonech upravujících oprávnění zpravodajských služeb ČR, která by případně mohla být důkazně v trestním řízení použitelná.

III.1. Varianty legislativního řešení

ANB se v řadě bodů zmiňuje o zpravodajských službách a obsahuje návrhy na legislativní změny směřující k důkaznímu použití informací pocházejících ze zpravodajských služeb a návrhy na další (organizační) opatření rozšiřující efektivitu využití informací pocházejících z činnosti zpravodajských služeb a spočívající ve spolupráci a součinnosti s orgány činnými v tr. řízení.

Úvahy a návrhy směřují k umožnění důkazního využití zákonem stanovených informací získaných zpravodajskými službami v trestním řízení za předpokladu, že úprava zároveň poskytne dostatečnou ochranu základním právům a svobodám jednotlivců. Předpokládá se, že poskytnutí informací zpravodajských služeb by mělo být omezeno na vybrané informace získané s použitím zpravodajské techniky podléhajícímu předchozímu soudnímu povolení a na trestné činy představující bezprostřední a vážnou hrozbu pro zájmy České republiky a pro její obyvatele. Zachován by přitom měl být princip výhrady důležitého zájmu sledovaného zpravodajskou službou (§ 8 odst. 3), tedy že zpravodajská služba zváží, zda informace pro účely trestního řízení předá, či zda upřednostní ochranu zpravodajského zájmu a zpravodajské informace. Tímto tedy odpadá i možná obava z negativních dopadů na bezpečnost nebo obranu ČR.

Důležitý a bezvýhradný je také požadavek na zachování souladu s ústavními principy, judikaturou Ústavního soudu i judikaturou ESLP. Zde nelze než zopakovat, že stanovení podmínek přípustnosti důkazů v trestním řízení spadá do pravomoci vnitrostátních orgánů. Nicméně z hlediska Evropské úmluvy o ochraně lidských práv a základních svobod je třeba především zajistit splnění požadavků čl. 8 odst. 2 na zásah do práva na soukromý život, tedy zejména požadavky na existenci a kvalitu zákona, který musí být dostupný, předvídatelný a musí jasně vymezit pravomoci příslušných orgánů.

Podle předpokládané nové právní úpravy by bylo možné předat konkrétně důkazně využitelnou informaci, která bude dále zpracována orgány činnými v trestním řízení pro účely trestního řízení. Nová úprava by tedy nevyloučila možnost použití zpravodajských informací jako důkazu v trestním řízení, jako je tomu dosud. Nové pravomoci zpravodajským službám, ani orgánům činným v trestním řízení by přiznány nebyly.

V kontextu s legislativními návrhy v oblasti vnitřní bezpečnosti předložil Odbor bezpečnosti a prevence kriminality MV ČR spolu s Legislativním odborem MS ČR k připomínkovému řízení návrh variant komplexního řešení dané problematiky.[24] Pokud jde o vymezení trestních věcí, u nichž by byly zpravodajské informace použitelné jako důkaz byly stanoveny tyto varianty: Varianta č. 1 – novelizace § 89 TŘ, jež by umožnila procesní použitelnost zpravodajských informa-

[24] Viz Budka, I. Využití nástrojů pro potírání organizovaného zločinu. Institut pro kriminologii a prevenci, Praha 2017. s. 97: dostupné z www.ok.cz/iksp/docs/444.pdf.

cí bez jakéhokoliv omezení (u všech trestných činů) Varianta č. 2 – novelizace § 89 TŘ, jež by umožnila procesní použitelnost zpravodajských informací jen u trestných činů podle hlavy IX trestního zákoníku (trestné činy proti České republice, cizímu státu a mezinárodní organizaci) Varianta č. 3 – novelizace § 89 TŘ, jež by umožnila procesní použitelnost zpravodajských informací zvlášť závažných zločinů (úmyslné trestné činy s horní hranicí trestní sazby nejméně 10 let) a trestných činů podle hlavy IX trestního zákoníku (trestné činy proti České republice, cizímu státu a mezinárodní organizaci).

V otázce stanovení druhu zpravodajské informace použitelné jako důkaz v trestním řízení pak tyto: Varianta č. 1 – novelizace § 89 TŘ spočívající v procesní použitelnosti jakékoliv zpravodajské informace získané v souladu se zákonem upravující činnost zpravodajských služeb Varianta č. 2 – novelizace § 89 TŘ spočívající v procesní použitelnosti zpravodajské informace získané na základě povolení soudce v souladu se zákonem upravující činnost zpravodajských služeb – informace získané prostřednictvím odposlechu a záznamu telekomunikačního provozu, nakládání se zásilkou, sledování osob a věcí, při kterém je zasahováno do práva nedotknutelnosti obydlí Varianta č. 3 – novelizace § 88 TŘ spočívající v procesní použitelnosti zpravodajských informací získaných na základně odposlechu a záznamu telekomunikačního provozu.

Závěr

Je zjevné, že i v České republice existuje vážná vůle a zadání směřující k umožnění důkazního použití zpravodajského odposlechu v trestním řízení. Práce na legislativní úpravě, která by tuto možnost připustila, je však stále ještě ve stadiu před zahájením legislativního procesu, a na podobu výsledného návrhu lze jen usuzovat. I v tomto okamžiku je nicméně již vyslovit předpoklad, že – s cílem zajistit stejné garanční kvality ochrany základních práv a svobod jako v trestním řádu – bude přesně vymezen okruh zpravodajských informací důkazně v trestním řízení použitelných, vymezen okruh trestních věcí, v nichž bude možné zpravodajské informace důkazně využít, a také že bude zachován princip, podle kterého bude umožněno příslušné zpravodajské službě využít již existujícího institutu tzv. výhrady důležitého zájmu, tedy informaci v odůvodněných případech, brání-li tomu významný zájem sledovaný zpravodajskou službou, neposkytnout.

Literatura

Aláč, M. *Osobitosti použitia ITP v posobnosti Slovenskej informačnej služby.* In Záhora, J. (ed.) Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní. Leges, Praha 2017, s. 268–275.

Audit národní bezpečnosti. Schválený usnesením vlády ČR č. 1125 dne 14. 12. 2016. Dostupný z www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf.

Budka, I. *Využití nástrojů pro potírání organizovaného zločinu*. Institut pro kriminologii a prevenci, Praha 2017. s. 97: dostupné z www.ok.cz/iksp/docs/444.pdf

Duchek, J.: *Zpravodajské služby při tvorbě a realizaci bezpečnostní politiky*. Vojenské rozhledy. Teoretický časopis armády České republiky, 2005, číslo 1.

Herczeg, J. *Zásada „nemo tenetur" a práva obviněného v trestním řízení.* Bulletin advokacie, 1–2/2010.

Ivor, J. *Využitie informácií spravodajských služieb v trestnom konaní.* In *Spravodajské služby v demokratickej společnosti*. Zborník zo sympózia, Bratislavská vysoká škola práva, Bratislava 2009.

Kloubek, M., Pokorný, L., Michálek, L. *Prostředky operativně pátrací a zpravodajské činnosti v podmínkách České republiky.* In Jozef STIERANKA, Michal MARKO a kolektiv: Aktuálne otázky aplikácie kriminálneho spravodajstva v kontexte nových trendov v Európskej únii. Akadémia policejného zboru v Bratislave. Bratislava 2018, s. 86–104.

Musil, J. *Několik otazníků nad judikaturou ÚS ČR v době postmoderny (na příkladu prohlídky jiných prostor a pozemků)*. Kriminalistika 2011, č. 1.

Nález ÚS ČR sp. zn. I ÚS 3038/07 z 29. 2. 2008.

K některým otázkám týkajícím se odposlechu, zjišťování údajů z telekomunikačního provozu

Selected Questions Concerning Interception of Telecommunication, Ascertainment Data of Telecommunication

Miroslav Růžička[1]

Abstrakt: *Příspěvek se věnuje sporným otázkám výkladu ustanovení § 88 trestního řádu o odposlechu a záznamu telekomunikačního provozu. Zaměřuje pozornost především na výkladové stanovisko č. 1/2018 Sbírky výkladových stanovisek Nejvyššího státního zastupitelství. Týká se spíše praktických problémů vztahujících se k odposlechu a záznamu telekomunikačního provozu.*

Abstract: *The contribution dealt with questionable problems of interpretation section 88 of the Criminal Procedure Code on the Interception and Recording of Telecommunications in the Czech Republic. The article concentrated attention generally to the Opinion No. 1/2018 of the Collection of opinions of the Supreme Public Prosecutor's Office. I tis connected to practical problems regarding the Interception and Recording of Telecommunications*

Klíčová slova: *Právo na soukromí, odposlech a záznam telekomunikačního provozu, aplikační praxe orgánů činných v trestním řízení, pokyny obecné povahy nejvyššího státního zástupce.*

Keywords: *Protection of Privacy, Interception and Recording of Telecommunications, Practice of the Law enforcement authorities (involved in Criminal Proceedings), General Instructions of the Supreme Public Prosecutor.*

I. Úvod

Tento příspěvek je – shodně jako ten, který byl přednesen na konferenci konané dne 23. 3. 2017 – zaměřen na institut odposlechu a záznamu telekomunikačního provozu (§ 88a tr. ř.), a to v úzké souvislosti se zjišťováním údajů telekomunikačního provozu (§ 88a tr. ř.) a sledováním osob a věcí (§ 158d tr. ř.). Na konferenci v březnu 2017 to bylo v úzké návaznosti na tehdy velmi aktuální stanoviska vydaná Nejvyšším státním zastupitelstvím v souladu s ustanovením § 12 odst. 2 zákona o státním zastupitelství, č. 4/2005 Sb. v. s. NSZ a č. 1/2015 Sb. v. s. NSZ, proti nimž byly vyslovovány četné oponentní názory.

V mezidobí se znovu ukázalo, jak je tématika úkonů podle § 88, § 88a a § 158d tr. ř. vysoce dynamická a aktuální a jak se stále objevují nové výzvy a nové aplikační problémy.[2]

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

[2] Srov. např. webové odkazy: https://www.ceska-justice.cz/blog/prezident-zneuzivani-moci-vrchnim-statnim-zastupitelstvim/
https://www.ceska-justice.cz/2019/03/terorismus-organizovana-kriminalita-ministerstvo-zvazuje-povoleni-odposlechu-bez-souhlasu-soudu/
https://www.ceska-justice.cz/2019/03/nalehavych-pripadech-by-mohl-soud-povolit-odposlechy-ramci-predbezneho-opatreni-mini-unie-obhajcu/
https://www.ceska-justice.cz/2019/03/analyza-proc-soudy-odmitaji-pouzit-prostorove-odposlechy-obydli-za-dukaz-jinych-trestnich-kauzach/
https://www.ceska-justice.cz/2019/03/poslanci-jsou-zdrzenlivi-k-odposlechum-bez-souhlasu-soudu-podle-bendy-jsou-protiustavni/
https://www.ceska-justice.cz/2019/03/soud-zalobce-nemuze-pouzit-odposlechy-rittiga-kauze-jizdenek/

Účelem tohoto příspěvku rozhodně není zabývat se všemi problémy spojenými s tím, že se např. objevují úvahy o tom, že by ve zcela výjimečných a naléhavých případech (zejména ve věcech terorismu nebo organizovaného zločinu) bylo možno provádět odposlech a záznam telekomunikačního provozu, popř. získávat údaje z takového provozu (a obdobně realizovat sledování osob a věcí, je-li zasahováno do nedotknutelnosti obydlí, do listovního tajemství nebo zjišťován obsah jiných písemností a záznamů uchovávaných v soukromí za použití technických prostředků, ve všech těchto případech bez příkazu či souhlasu soudce.[3, 4]

Stejně tak se tento příspěvek nebude blíže zaobírat problematikou tzv. prostorových odposlechů.[5] Je možno pouze poznamenat, že Ministerstvo spravedlnosti zpracovalo návrh novely trestního řádu, která by měla uvedený problém vyřešit, avšak příslušný návrh novely nebyl zatím předložen ani do připomínkového řízení.

Nejvyšší státní zastupitelství vypracovalo návrh pokynu obecné povahy,[6] který se týká oblasti pro výkon působnosti státního zastupitelství (aniž by byla podceňována mimotrestní oblast působnosti státního zastupitelství) zcela zásadní, tedy trestního procesu. Tento návrh se zaměřuje i na problematiku odposlechu a záznamu telekomunikačního provozu, zjišťování údajů z takového provozu a sledování osob a věcí, v podstatě v souladu s citovanými výkladovými stanovisky. Od samého počátku však vyvstávají četné polemiky ohledně konkrétní podoby interní úpravy, v příštím týdnu proběhne vypořádání připomínek k uvedenému návrhu. Tyto diskuse vlastně opakují to, co zaznívá v protikladných vyjádřeních k tomuto tématu už delší dobu. Dalo

https://www.ceska-justice.cz/2019/03/ustavni-soud-rozhoduje-zda-omezi-shromazdovani-vyuzivani-udaju-telekomunikacnim-provozu/
https://www.ceska-justice.cz/2019/03/ustavni-soud-chce-verejne-projednat-provozni-lokalizacni-udaje/.

[3] Jistou obdobu – od nabytí účinnosti novely provedené s účinností od 1. 1. 2012 zákonem č. 459/2011 Sb. – představuje prohlídka jiných prostor a pozemků. Z úpravy v § 82 odst. 2 a § 83a odst. 2 a 3 tr. ř. vyplývá, že je-li důvodné podezření, že v prostorách nesloužících k bydlení (jiných prostor) a pozemků, pokud nejsou veřejně přístupné, je věc nebo osoba důležitá pro trestní řízen, lze vykonat prohlídku jiných prostor a pozemků. Bez příkazu může policejní orgán provést prohlídku jiných prostor nebo pozemků, jestliže vydání příkazu nelze předem dosáhnout a věc nesnese odkladu. Policejní orgán je však povinen si bezodkladně dodatečně vyžádat souhlas orgánu oprávněného k vydání příkazu; v přípravném řízení tak činí prostřednictvím státního zástupce. Pokud oprávněný orgán souhlas dodatečně neudělí, nelze výsledek prohlídky použít v dalším řízení jako důkaz. Bez příkazu může policejní orgán provést prohlídku jiných prostor nebo pozemků také tehdy, pokud uživatel dotčených prostor nebo pozemků písemně prohlásí, že s prohlídkou souhlasí, a své prohlášení předá policejnímu orgánu. O tomto úkonu však musí policejní orgán bezodkladně vyrozumět předsedu senátu oprávněného k vydání příkazu a v přípravném řízení státního zástupce. Dlužno dodat, že od plenárního nálezu Ústavního soudu ze dne 8. 6. 2010 sp. zn. Pl. ÚS 3/09, publikovaného pod č. 219/2010 Sb., není možné, aby prohlídku jiných prostor a pozemků nařizoval státní zástupce.

[4] Takto by např. mohlo být stanoveno, že „…Nesnese-li věc odkladu, může být provádění odposlechu a záznamu telekomunikačního provozu zahájeno i bez předchozího příkazu. Návrh na vydání příkazu však musí být bezodkladně dodatečně podán, a pokud příkaz není do 48 hodin od zahájení provádění odposlechu a záznamu telekomunikačního provozu vydán, provádění odposlechu a záznamu telekomunikačního provozu musí být neprodleně ukončeno, záznam musí být zničen a informace, které se v této souvislosti orgány činné v trestním řízení dozvěděly, nesmějí být nijak použity." Obdobně by tomu mohlo být i u dalších naznačených úkonů. Proti navrhovanému řešení se však – jak o tom svědčí i webové odkazy zmíněné v poznámce pod čarou č. 1 – zvedla vlna odporu.

[5] K nim srov. např. velice pozoruhodný článek Jelínek J. K chybějící právní úpravě tzv. prostorového odposlechu v trestním řádu, Bulletin advokacie. 2018, č. 7–8, s. 13.

[6] Pokyny obecné povahy (jistou obdobu představovaly v podmínkách prokuratury příkazy generálního prokurátora, kde však dosah úpravy byl s ohledem na jiné postavení prokuratury oproti státnímu zastupitelství zpravidla výrazně širší) podle § 12 odst. 1 zákona o státním zastupitelství vydává nejvyšší státní zástupce ke sjednocení a usměrnění postupu státních zástupců při výkonu působnosti státního zastupitelství nebo k zajištění jednotné vnitřní organizace státního zastupitelství a jednotného výkonu spisové služby; tyto pokyny jsou závazné pro státní zástupce, a pokud tak nejvyšší státní zástupce stanoví, i pro další zaměstnance státního zastupitelství.

by se tak říci, že v uvedené oblasti přetrvává stále velké množství aplikačních problémů, otázkou je, zda se je podaří beze zbytku vyřešit legislativní změnou.[7]

Ještě je nutno uvést, že – s ohledem na omezený rozsah příspěvku – nebude možno pozornost soustředit na dvě, také zcela zásadní témata (jichž se rovněž zčásti dotýká níže citované výkladové stanovisko), a to problematiku odposlechu a záznamu telekomunikačního provozu mezi advokátem a jeho klientem, nejde-li ještě o postavení obhájce a obviněného (toto téma by si bezesporu zasluhovalo samostatný příspěvek), resp. problematiku informování o odposlechu (zjišťování údajů), kde zejména v poslední době se nezřídka namítá, že počet výjimek z povinnosti orgánů činných v trestním řízení je příliš široký, počet poskytnutých informací je velmi nízký, a objevují se nejrůznější návrhy jak naznačený problém řešit.

A tento příspěvek se samozřejmě nevztahuje na další evergreen posledních 10 let – úniků ze spisů, právě pokud jde o obsah odposlechů.[8] Snad na to nemůže mít ani ambici, jak to tedy doopravdy bylo a jak to je. Pozoruhodné spíše je, že se tento problém objevil právě před asi 12 lety v souvislosti s tzv. „fotbalovou kauzou" a posléze i tzv. „Kuřimskou kauzou", která bezprostředně vyvolala legislativní změnu starou právě 10 let („náhubkový zákon", později zmírněný).

II. Výkladové stanovisko č. 1/2018 Sb. v. s. NSZ – některé problémy

Výkladové stanovisko č. 1/2018 Sb. v. s. NSZ ze dne 11. 5. 2018 sp. zn. 1 SL 719/2017,[9] se vztahuje k problematice pořizování a nakládání s odposlechem a záznamem telekomunikačního provozu.

Bylo zjištěno, že aplikační praxe policejních orgánů a státních zástupců není v některých směrech jednotná a může mít vliv na posuzování zákonnosti záznamu telekomunikačního provozu soudem při hodnocení důkazů.[10]

Vychází se především z toho, že obligatorní náležitosti návrhu státního zástupce na vydání příkazu k odposlechu a záznamu telekomunikačního provozu jsou kromě dalších podstatných údajů požadovaných platnou právní úpravou také

- uvedení a odůvodnění doby, po kterou bude odposlech a záznam telekomunikačního provozu prováděn, která nesmí být delší než čtyři měsíce;
- účel odposlechu a záznamu telekomunikačního provozu, jakož i odůvodnění, proč nelze sledovaného účelu dosáhnout jinak, nebo proč by bylo jinak jeho dosažení podstatně ztížené;
- ve fázi před zahájením trestního stíhání rovněž odůvodnění neodkladnosti nebo neopakovatelnosti úkonu ve smyslu § 160 odst. 4 tr. ř.

Obsahové náležitosti příkazu k odposlechu a záznamu telekomunikačního provozu jsou vymezeny v § 88 odst. 2 tr. ř. Příkaz soudce musí být vydán písemně, musí být odůvodněn a musí

[7] Mnohdy totiž platí, že další a další legislativní změny situaci spíše ještě více zkomplikují.

[8] Srov. již starší příspěvek: www.ceska-justice.cz/blog/medialni-uniky-ze-zivych-spisu-vytvareji-obraz-sprostych-podezrelych/. Jakkoli je poněkud tendenční. Znovu se ovšem tento problém vyskytl v nedávné době – kauza mýto, Úřad pro ochranu hospodářské soutěže, brněnská kauza – srov. např. https://www.novinky.cz/domaci/499643-faltynkovy-pletichy-kolem-kapsche-co-zjistila-policie.html
https://www.novinky.cz/domaci/500917-rafajova-otocka-v-mytnem-babis-zeman-kellner.html
https://www.novinky.cz/domaci/500962-co-se-delo-na-antimonopolnim-uradu.html.

[9] Jeho zpracovatelem byl kolega Tomáš Foldyna, okresní státní zástupce v Břeclavi.

[10] Srov. ostatně usnesení NS ČR vydané ve věci, v níž Vrchní soud v Praze zrušil odsuzující rozsudek Krajského soudu v Praze, hojně přetřásané médii, v níž posléze NS ČR rozhodoval pod sp. zn. 6 Tz 3/2017 o stížnosti pro porušení zákona ve věci D. R. a spol. vztahující se k náležitostem příkazů k povolení odposlechu a záznamu telekomunikačního provozu. Ale bylo by možno uvést i další významná judikatorní rozhodnutí obecných soudů či Ústavního soudu.

obsahovat uživatelskou adresu či zařízení, osobu uživatele, pokud je její totožnost známa, dobu, po kterou bude odposlech a záznam telekomunikačního provozu prováděn, která nesmí být delší než čtyři měsíce a v odůvodnění musí být uvedeny konkrétní skutkové okolnosti, které vydání příkazu, včetně doby jeho trvání, odůvodňují. Navíc musí příkaz obsahovat konkrétní odkaz na vyhlášenou mezinárodní smlouvu v případě, že se vede trestní řízení pro úmyslný trestný čin, k jehož stíhání tato mezinárodní smlouva zavazuje.

V důsledku vývoje judikatury je však v současné době vyžadováno, aby nad rámec náležitostí uvedených v § 88 odst. 2 tr. ř. příkaz k odposlechu a záznamu telekomunikačního provozu obsahoval také účel odposlechu a záznamu telekomunikačního provozu, jakož i odůvodnění, proč nelze sledovaného účelu dosáhnout jinak nebo proč by bylo jinak jeho dosažení podstatně ztížené (srov. též zásadu zdrženlivosti, vyjádřenou v § 2 odst. 4 větě druhé tr. ř.).

Ve fázi před zahájením trestního stíhání rovněž musí být do příkazu zahrnuto i odůvodnění neodkladnosti a/nebo neopakovatelnosti úkonu ve smyslu § 160 odst. 4 tr. ř. a výslovné označení, že se má jednat o úkon neodkladný anebo neopakovatelný.[11]

Má se dokonce za to, že ačkoli § 88 odst. 2 tr. ř. nestanoví obsahové náležitosti návrhu státního zástupce na vydání příkazu k odposlechu a záznamu telekomunikačního provozu, je zcela zjevné, že návrh musí po obsahové stránce splňovat nároky kladené v § 88 odst. 2 tr. ř. a také příslušnou judikaturou na tento typ příkazu soudu, dokonce se usuzuje, že návrh státního zástupce by měl být podrobnější a argumentačně obsáhlejší než samotný příkaz, neboť je úkolem státního zástupce dostatečně pádně vyargumentovat svůj návrh a přesvědčit soud o jeho důvodnosti.

Interní úprava obsažená v pokynu obecné povahy č. 8/2009 o trestním řízení tyto náležitosti podrobně vyjmenovává. A obdobně z toho vychází i návrh nového pokynu obecné povahy, o němž byla zmínka v úvodu tohoto příspěvku.

Vzhledem k rozhodovací praxi soudů, zejména Nejvyššího soudu a Ústavního soudu, je však zcela zřejmé, že uvedení účelu, jenž má být odposlechem sledován, jakož i odůvodnění, proč nelze stejného účelu dosáhnout jinak nebo proč by bylo jeho dosažení podstatně ztížené, stejně jako zdůvodnění neodkladnosti anebo neopakovatelnosti, pokud má být tento úkon prováděn před zahájením trestního stíhání, je nutno považovat za obligatorní náležitosti příkazu soudu k odposlechu a záznamu telekomunikačního provozu. Stejně tak je tyto požadavky s argumentem a maiori ad minus nutno vztáhnout také k návrhu státního zástupce na vydání příkazu a potažmo i k podnětu policejního orgánu k podání návrhu adresovaného státnímu zástupci.[12] I přes doktrínu materiálního právního státu[13]) je nutno považovat absenci uvedených náležitostí v návrhu státního zástupce za podstatnou vadu. Proto je také stanovisko zvlášť zdůraznilo (a na tom bude založena i nová interní úprava pro státní zástupce – viz výše).

V další své části stanovisko vychází z toho, že vyhodnocení odposlechů provádí policejní orgán; státní zástupce se s vyhodnocením seznamuje průběžně (v pravidelných intervalech) v rámci výkonu dozoru nad zachováváním zákonnosti v přípravném řízení. Pokud státní zástupce předkládá soudu spisový materiál, jehož součástí je i záznam odposlechu telekomunikačního provozu, odpovídá za jeho náležité vyhodnocení.

Odposlech a záznam telekomunikačního provozu provádí pro všechny orgány činné v trestním řízení, zejména pro policejní orgány konající trestní řízení (§ 12 odst. 2 a § 88 odst. 1 věta

[11] Srov. příspěvek přednesený na konferenci konané dne 23. 3. 2017, který se tímto požadavkem rovněž obsáhle zabýval, a lze na něj plně odkázat.

[12] Viz právě citované rozhodnutí Nejvyššího soudu ze dne 7. 6. 2017 sp. zn. 6 Tz 3/2017.

[13] Např. usnesení velkého senátu trestního kolegia Nejvyššího soudu ze dne 26. 6. 2013 sp. zn. 15 Tdo 510/2013 a nález Ústavního soudu ze dne 7. 5. 2014 sp. zn. Pl. ÚS 47/13, ale k tomuto tématu se vztahují i četná další judikatorní rozhodnutí obecných soudů i Ústavního soudu.

druhá tr. ř.) Útvar zvláštních činností Služby kriminální policie a vyšetřování Policie ČR. Odpovědným za vyhodnocení odposlechu a záznamu telekomunikačního provozu je tedy vždy policejní orgán, který vede ve věci trestní řízení, neboť pouze ten má k pořízenému záznamu přímý a prvotní přístup.

Policejní orgán je také tím orgánem činným v trestním řízení, který jako první selektuje záznamy odposlechů telekomunikačního provozu na záznamy důkazně významné, jež budou, nebo by mohly být, v dalších fázích trestního řízení využity jako důkaz, a to ať již ve prospěch nebo v neprospěch pachatele, a záznamy důkazně bezvýznamné (§ 88 odst. 6 tr. ř.), jež mají být vedeny odděleně od spisu.

I přes výraznou procesní samostatnost, kterou při vyhodnocení záznamu odposlechu policejní orgán z podstaty této činnosti má,[14] zůstává garantem zákonnosti přípravného řízení a rozsahu dokazování státní zástupce,[15] který v dalších fázích trestního řízení záznam odposlechu používá buďto jako důkaz na podporu obžaloby, případně jako důkaz na podporu jiných svých procesních návrhů adresovaných soudu, event. jako podklad pro své vlastní rozhodnutí. Z tohoto důvodu nelze připustit, aby státní zástupce z jakéhokoli důvodu rezignoval na svou dozorovou činnost vůči policejnímu orgánu, a je nezbytné, aby se v pravidelných intervalech odvislých od délky trestního řízení, jeho náročnosti i závažnosti věci, seznamoval s vyhodnocením záznamu odposlechu. Může tak činit různou formou, přičemž v úvahu přichází seznámení se samostatnou zprávou policejního orgánu, kterou policejní orgán vyhodnocuje nejen pořízené záznamy odposlechů, ale také ostatní opatřené důkazy a zjištěné skutečnosti, což státnímu zástupci umožňuje získat komplexní náhled na celkový vývoj trestního řízení, nebo přichází v úvahu seznámení se s přepisy záznamů odposlechů, nebo se státní zástupce může se záznamem odposlechu seznámit poslechem samotného zvukového záznamu. V této souvislosti je nutno zdůraznit, že garantem náležitého vyhodnocení záznamu odposlechu vůči soudu, je vždy státní zástupce, a nikoli policejní orgán.

Odpovědnost za způsob, jakým se státní zástupce seznámí a ověří správnost vyhodnocení záznamu odposlechu, zůstává vždy na státním zástupci, a to i ve věcech méně skutkově a důkazně složitých, plně se to však vztahuje na věci mimořádně právně a důkazně složité.

V neposlední řadě výkladové stanovisko v další své části konstatuje, že státní zástupce v rámci výkonu dozoru nad zachováváním zákonnosti v přípravném řízení odpovídá za to, aby archivní nosič obsahující kompletní záznam odposlechu byl veden odděleně od trestního spisu. Součástí

[14] K procesní samostatnosti policejního orgánu a osoby v něm služebně činné (vzhledem k tomu, že tento pojem nelze omezovat pouze na policejní orgán chápaný v institucionálním pojetí) srov. Růžička, M. K otázce procesní samostatnosti policejního orgánu, Trestněprávní revue, 2010, č. 2, s. 35.

[15] Lze jen stručně rekapitulovat, že státní zástupce v přípravném řízení zajišťuje ochranu veřejného zájmu (nikoli úzce pojatého zájmu státu na potrestání pachatele trestného činu). Již jen z tohoto pohledu je státní zástupce důležitým činitelem výkonu mj. i trestní spravedlnosti. Státní zástupce přímo odpovídá za ochranu lidských práv v souvislosti s tím, že se dozvěděl o tom, že v určité věci bylo zahájeno trestní řízení (prověřování), a dále i zahájením trestního stíhání proti konkrétní osobě a za ochranu těchto práv při provádění vyšetřovacích úkonů, které po zahájení trestního stíhání následují (vyšetřování). V rozsahu své ústavně i zákonem vymezené působnosti nese odpovědnost za výsledky přípravného řízení, dodržování základních práv a svobod v jeho průběhu i za to, že nikdo nebude postaven před soud nedůvodně a žádná osoba též nebude v průběhu přípravného řízení bezdůvodně omezována na svých právech. Zdůrazňuje se tu zásadní skutečnost, že je to státní zástupce (veřejný žalobce), který musí mít dominantní roli v přípravném řízení. Státní zástupce je totiž orgánem, jehož činnost do značné míry prolíná, prostupuje všemi stadii trestního procesu, v nichž se nejprve zjišťují potřebné podklady, zajišťují a provádějí důkazy a posléze se rozhoduje o vině, trestu, popř. navazujících otázkách trestního řízení. Dominantní postavení státního zástupce v přípravném řízení je důsledkem toho, že vyšetřování podle české trestněprocesní úpravy nekoná vyšetřující soudce, ale policejní orgány (ty ostatně konají i prověřování a zkrácené přípravné řízení) požívající při plnění úkolů v trestním řízení, vystupují-li jako orgány činné v trestním řízení, a nikoli jako „servisní" orgány pro orgány činné v trestním řízení, procesní samostatnosti.

trestního spisu může být jen datový nosič obsahující záznamy odposlechu, jež mají být v trestním řízení použity jako důkaz, který se k trestnímu spisu přikládá spolu s protokolem o odposlechu a záznamu telekomunikačního provozu (§ 88 odst. 6 tr. ř.).

Postup pro použití záznamu odposlechu jako důkazu, jakož i postup pro nakládání se záznamem odposlechu, který žádný důkazní význam nemá, vyplývá právě z § 88 odst. 6 tr. ř. Útvar zvláštních činností vyhotovuje po skončení odposlechu dva datové nosiče, jeden s úplnými záznamy všech odposlechů („archivní nosič") a druhý na základě zadání policejního orgánu, obsahující pouze výběr záznamů odposlechů, které mají důkazní hodnotu a mají být v dalších fázích řízení vyžity jako důkaz (dále jen „důkazní nosič"). Oba datové nosiče předává Útvar zvláštních činností policejnímu orgánu konajícímu trestní řízení.

Podle § 88 odst. 6 tr. ř. má-li být záznam telekomunikačního provozu užit jako důkaz, je třeba k němu připojit protokol s uvedením údajů o místě, času, způsobu a obsahu provedeného záznamu, jakož i o orgánu, který záznam pořídil. Ostatní záznamy je povinen policejní orgán označit, spolehlivě uschovat tak, aby byla zajištěna ochrana před neoprávněným zneužitím záznamů, a v protokolu založeném do spisu poznamenat, kde jsou uloženy. Ostatními záznamy je nutno rozumět veškeré další záznamy uložené na archivním nosiči, které nebyly uloženy na důkazní nosič.

Je povinností státního zástupce, aby dbal o to, aby policejní orgán založil do trestního spisu protokol o odposlechu a záznamu telekomunikačního provozu. Vychází se přitom z toho, že je třeba odlišit zvukový záznam rozhovoru účastníků odposlouchávané stanice pořízený automatickým záznamovým zařízením, zaznamenaný na nepřepisovatelném přenosném datovém médiu, které obsahuje veškerou komunikaci vedenou prostřednictvím odposlouchávané stanice za rozhodné období, a tu část zvukového záznamu, která je na základě rozhodnutí státního zástupce a policejního orgánu důležitá pro trestní řízení a má být použita jako důkaz a ohledně níž se pořídí samostatný zvukový nosič, který je opatřen protokolem s uvedením údajů o místě, času, způsobu a obsahu provedeného záznamu, jakož i označením Útvaru zvláštních činností, který záznam pořídil. Od uvedeného je dále nutno odlišit přepis zvukového záznamu, který slouží jen k orientaci policejního orgánu nebo státního zástupce o obsahu zvukového záznamu.

Není správný postup, jestliže se do trestního spisu založí spolu s protokolem Útvaru zvláštních činností o pořízení záznamu odposlechu archivní nosič, případně se do spisu založí jak důkazní nosič, tak i archivní nosič. To pak vede k situaci, kdy další osoby zúčastněné na trestním řízení získávají přístup k záznamu odposlechu bez důkazního významu, čímž dochází k porušení práva na ochranu soukromí třetích osob, jež jsou na těchto záznamech zachyceny, aniž by to mělo význam pro další průběh trestního řízení. Takový postup je tedy nejen v rozporu s § 88 odst. 6 tr. ř., ale i v rozporu s čl. 8 Úmluvy o ochraně lidských práv a základních svobod, a státní zástupce má na takové pochybení policejního orgánu reagovat v rámci výkonu dozoru nad zachováváním zákonnosti v přípravném řízení pokynem, kterým policejnímu orgánu uloží, aby zjednal nápravu.

Na místě je tedy postup, kdy se do trestního spisu založí pouze datový nosič obsahující záznamy odposlechů, které mají být v dalších fázích řízení použity jako důkaz, tedy důkazní nosič. Archivní nosič policejní orgán vede odděleně od spisu, do kterého pouze poznamená, kde je uložen. Dodržování tohoto postupu podléhá výkonu dozoru státního zástupce, který v okamžiku, kdy předkládá spis spolu se záznamem odposlechu soudu, také odpovídá za to, že spis obsahuje pouze datový nosič se záznamem výlučně těch odposlechů, jež mají důkazní význam a mají být užity jako důkaz (důkazní nosič).

Na to pak navazuje postup při provádění důkazu odposlechem a záznamem telekomunikačního provozu, který je na území ČR u různých orgánů činných v trestním řízení velice rozdílný,

přičemž ve věcech, v nichž je v I. stupni příslušný k rozhodování okresní soud, se takový důkaz provádí nejčastěji postupem podle § 213 odst. 1 tr. ř., tedy tak, že protokol o odposlechu a záznamu telekomunikačního provozu spolu s důkazním datovým nosičem se během hlavního líčení předloží stranám k nahlédnutí a pokud žádná ze stran nenavrhne provedení důkazu přehráním a poslechem zvukového záznamu odposlechu, je důkaz proveden. Faktickým přehráním a poslechem se tento důkaz provádí spíše výjimečně a zpravidla pouze v těch nejzávažnějších trestních věcech, v nichž rozhoduje v I. stupni krajský soud. Byla také zaznamenána praxe, že se tento důkaz provádí přečtením doslovného přepisu zvukového záznamu odposlechu.

S tím souvisí také různé postupy policejních orgánů a požadavky státních zástupců vůči nim, ohledně úrovně a kvality pořizovaných přepisů záznamů odposlechů. Přepisy se tak provádí od velmi kusých obsahových, jejichž hodnota je ryze orientační, přes podrobné obsahové, jež sice ne doslovně, ale přesto velmi podrobně zachycují obsah pořízeného záznamu odposlechu, až po zcela doslovné přepisy. Forma, v jaké je přepis pořizován, pak zpravidla závisí na dohodě mezi policejním orgánem a státním zástupcem, eventuálně na pokynu státního zástupce.

V řízení před soudem by se k návrhu stran měl důkaz záznamem odposlechu telekomunikačního provozu provádět zásadně faktickým přehráním a poslechem zaznamenané nahrávky telefonického rozhovoru (§ 213 odst. 2 tr. ř.). Toto je základní způsob provádění důkazu. Provádění listinných a věcných důkazů v řízení před soudem je upraveno v § 213 tr. ř.

Ustanovení § 213 odst. 1 tr. ř., ve znění po novele provedené zákonem č. 41/2009 Sb., umožňuje v zájmu rychlosti a hospodárnosti trestního řízení považovat za provedený listinný či věcný důkaz, který byl stranám během hlavního líčení předložen k nahlédnutí a žádná ze stran nežádá jeho podrobnější provedení např. přečtením, poslechem atd. Má se tedy za to, že procesní strany jsou s daným důkazem dostatečně obeznámeny a jeho obsah nezpochybňují (což samozřejmě neznamená, že by nemohly zpochybňovat zákonnost jeho pořízení, jeho použitelnost, interpretaci jeho obsahu druhou procesní stranou atd.). Obdobně se postupuje v případě SMS zpráv.

Vzhledem k tomu, že protokol o pořízeném odposlechu a záznamu telekomunikačního provozu podle § 88 odst. 6 tr. ř. je listinným důkazem, a to i s připojeným důkazním nosičem, je přípustné jeho provedení v hlavním líčení postupem podle § 213 odst. 1 tr. ř., pokud žádná ze stran nepovažuje za nezbytné faktické přehrání zvukového záznamu odposlechu a takový způsob provedení tohoto důkazu nepožaduje. Státní zástupce musí při rozhodování ohledně navrhovaného procesního postupu při provádění tohoto důkazu pečlivě zvážit nejen důkazní hodnotu zaznamenaných odposlechů telekomunikačního provozu, ale také celkovou důkazní situaci obžaloby, sílu a důkazní hodnotu všech důkazů, závažnost a složitost věci, postoj obviněného a jeho obhajobu a veškeré další faktory, které mohou ovlivnit soud nejen při rozhodování o vině, ale rovněž při rozhodování o druhu a výši trestu, jenž má být obviněnému uložen. Platí tak, že postup podle § 213 odst. 1 tr. ř. při provádění záznamu odposlechu jako důkazu by měl státní zástupce navrhovat jen za situace, kdy přímý poslech záznamu odposlechu nemůže mít vliv na rozhodnutí soudu o vině ani o druhu a výši trestu. V této souvislosti nelze pominout ani vliv, jaký může mít na rozhodnutí soudu např. i způsob vyjadřování obviněného zachycený na záznamu odposlechu, jeho mluva, intonace apod.

Pokud tedy státní zástupce dospěje k názoru, že důkaz záznamem odposlechu telekomunikačního provozu je nutno provést podrobněji, navrhne jeho přehrání a poslech. Není přitom vyloučeno, aby takový důkaz (podporující obžalobu) provedl se souhlasem předsedy senátu nebo na jeho pokyn sám (§ 180 odst. 3, § 203 odst. 1 a § 215 odst. 2 tr. ř.), a to případně i v součinnosti s příslušníkem policejního orgánu – zpracovatelem (ten může zajistit zapůjčení kvalitnější zvukové aparatury, než má k dispozici soud, může pomoci s technickou stránkou provedení tohoto důkazu, může asistovat při vyhledávání a spouštění záznamu konkrétního hovoru atd.).

S procesním postupem při provádění tohoto druhu důkazu bezprostředně souvisí potřeba pořizování přepisů záznamů odposlechů, které mají význam z hlediska obeznámení státního zástupce, soudu, ale i obviněného a jeho obhájce s obsahem zaznamenaných odposlechů telekomunikačního provozu.

Vzhledem k tomu, že přepisy záznamu odposlechu nejsou samy o sobě důkazem, jeví se jako neekonomické a neúčelné pořizování přepisů doslovných, ale pro základní orientaci zcela postačují přepisy obsahové, tj. přepisy, které pouze zachycují či parafrázují obsah hovoru, jeho téma, smysl apod. Pochopitelně i k pořizování obsahových přepisů lze přistupovat s různou mírou podrobnosti s přihlédnutím zejména k důkaznímu významu zaznamenaného hovoru. Opakovaně je však nutno zdůraznit, že pořizování doslovných přepisů je z hlediska dokazování zbytečné, a je tak v rozporu s principem ekonomiky trestního řízení a rovněž je nadbytečnou zátěží policejního orgánu, neboť důkazem zůstává pouze protokol o provedeném odposlechu a záznamu telekomunikačního provozu, který vyhotovuje Útvar zvláštních činností, spolu s důkazním nosičem, a to bez ohledu na to, v jaké kvalitě a jak podrobný byl vyhotoven přepis zaznamenaných odposlechů.[16]

To platí s jedinou výjimkou, kterou jsou záznamy odposlechů hovorů vedených v cizím jazyce, u nichž je nutno pořizovat jejich doslovný překlad, a tedy i přepis.

III. Závěr

Tento příspěvek se tentokráte zaměřil na poněkud odlišný okruh sporných otázek vztahujících se k institutu odposlechu a záznamu telekomunikačního provozu, než tomu bylo v případě konference věnované stejným problémům, dne 23. 3. 2017. Šlo spíše o některé procesní postupy, zejména státních zástupců, policejních orgánů, popř. i soudů, ve vztahu k tomuto úkonu. Ty se pak promítají spíše do obsahu interních úprav, tj. v daném případě do pokynu obecné povahy (u policejních orgánů by se obdobně mohlo jednat o pokyny policejního prezidenta). Tato skutečnost však nikterak nesnižuje jejich důležitost.

[16] Samozřejmě je zásadně nepřípustné, aby přepis podstatně měnil obsah a smysl toho, co bylo řečeno (např. „ano“ se zamění za „ne“ atd.). Čas od času média na takovou praxi poukazují, bez znalosti konkrétních okolností nelze dovodit, zda tomu tak v těchto věcech bylo, či nikoli.

Perspektívy akceptácie informácie zabezpečených mimoprocesným použitím ITP

Perspectives of Acceptance of Information Provided not Criminal Proceedings Use of Information and Technical Means

Adrián Vaško[1]

Abstrakt: *Príspevok je zameraný na otázky súvisiace s použitím informačno-technických prostriedkov mimo trestného konania. Autor venuje pozornosť otázkam právnej regulácie, charakteristike procesu použitia informačno-technických prostriedkov, prezentuje štatistické ukazovatele v tejto oblasti a prezentuje úvahy o ďalšom rozvoji v tejto oblasti.*

Abstract: *The paper focuses on issues related to the use of information and technical means outside criminal proceedings. The author pays attention to issues of legal regulation, characteristics of the process of using information and technical means, presents statistical indicators in this area and presents the reflections on further development in this field.*

Kľúčové slová*: informačno-technické prostriedky, trestné konanie, dokazovanie, operatívno-pátracia činnosť.*

Keywords: *information and technical means, criminal proceedings, evidence, operative-investigation activities.*

Úvod

Tak ako je to v iných demokratických krajinách, aj v podmienkach Slovenskej republiky je používanie informačno-technických prostriedkov (ďalej len ITP) pri zabezpečovaní úloh na úseku kontroly kriminality viazané na osobitné, v zákonoch stanovené podmienky. V Slovenskej republike sú právne charakteristiky informačno-technických prostriedkov vymedzené v Trestnom poriadku a v zákone č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím ITP a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním).

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*) upravuje podmienky použitia ITP bez predchádzajúceho súhlasu toho, komu sa zasahuje do súkromia orgánom štátu, ktorý informačno-technický prostriedok používa. Ide o použitie ITP mimo trestného konania, pre plnenie úloh príslušných štátnych orgánov vyplývajúcich pre ne z osobitného zákona. V praxi policajných a bezpečnostných orgánov sú prípady použitia ITP pomerne frekventované, osobitne v súvislosti s organizovanou kriminalitou a násilnými trestnými činmi.

1 Právna charakteristika ITP v zmysle zákona č. 166/2003 Z. z.

V zmysle ustanovení § 2 zákona č. 166/2003 Z. z. sa Informačno-technickými prostriedkami rozumejú: „*Informačno-technickými prostriedkami na účely tohto zákona sú najmä elektrotech-*

[1] JUDr. Adrián Vaško, PhD., Akadémia Policajného zboru v Bratislave, asistent katedry kriminálnej polície, Sklabinská 1, 835 17 Bratislava, adrian.vasko@gmail.com.

nické, rádiotechnické, 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."

ITP sú oprávnené používať Policajný zbor, Slovenská informačná služba, Vojenské spravodajstvo, Zbor väzenskej a justičnej stráže a Colná správa (*rozumej Finančnú správu SR*) 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 štátu, pre ktorý sa použitie ITP zabezpečuje. Používanie ITP podľa odseku 1 písm. b) zákona pre Vojenské spravodajstvo na základe písomnej žiadosti a po predložení písomného súhlasu zákonného sudcu technicky zabezpečuje Policajný zbor.

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 súlade s ustanovením § 2 ods. 7 zákona č. 166/2003 Z. z. nesmú orgány územnej samosprávy, súkromné bezpečnostné služby ani iné fyzické osoby alebo právnické osoby mať v držbe ani použiť informačno-technický prostriedok.

ITP 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; ITP možno v pôsobnosti Slovenskej informačnej služby a Vojenského spravodajstva použiť aj mimo územia Slovenskej republiky v rozsahu úloh podľa osobitných predpisov. Údaje získané ITP možno použiť výlučne na dosiahnutie účelu pri plnení úloh štátu, ktoré spĺňajú podmienky uvedené v zákone.

Podmienky použitia ITP predmetný zákon upravuje v § 4.: „*Informačno-technické prostriedky možno použiť iba na základe predchádzajúceho písomného súhlasu zákonného sudcu len na nevyhnutný čas, najdlhšie však na šesť 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 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.*".

V prípade Policajného zboru zákon zakotvuje v § 5 možnosť použitia ITP v odlišnom režime a to: „*Policajný zbor vo výnimočnom prípade, ak existuje dôvodné podozrenie z páchania trestného činu, pri ktorom možno použiť informačno-technický prostriedok na plnenie úloh Policajného zboru, vec neznesie odklad a súhlas zákonného sudcu nemožno vopred získať, môže použiť informačno-technický prostriedok aj bez predchádzajúceho súhlasu. Policajný zbor je povinný oznámiť začatie použitia informačno-technického prostriedku zákonnému sudcovi do jednej hodiny od začatia použitia informačno-technického prostriedku a predložiť zákonnému sudcovi žiadosť podľa § 4 ods. 3 do šiestich hodín od začatia použitia informačno-technického prostriedku; žiadosť musí obsahovať aj čas začatia použitia informačno-technického prostriedku. Ak Policajný zbor nedostane dodatočný písomný súhlas zákonného sudcu do 12 hodín od začiatku použitia informačno-tech-*

nického prostriedku alebo ak zákonný sudca nevyhovie 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.".

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 možností 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 zasielatelia a ich zamestnanci, povinní kompetentným orgánom štátnej správy poskytnúť nevyhnutnú súčinnosť; pritom sa nemôžu dovolávať povinnosti mlčanlivosti podľa osobitných zákonov.

Konkrétne metódy a formy práce, špeciálne technické prostriedky používané pri informačno-technickom úkone a písomná dokumentácia sú utajované skutočnosti.

ITP predstavujú významný nástroj, ktorým je možné získať relevantné informácie pre plnenie úloh na úseku kriminálno-policajného poznania a trestného konania (osobitne dokazovania). 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 sprostredkovane 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.

Informácie získané technickými úkonmi nemajú len charakter operatívnych informácií, ktoré slúžia na odhalenie trestných činov, zistenie ich páchateľov, ale aj sú dôležitým inštrumentom pri dokazovaní.

2 Prehľad stavu praktického mimoprocesného používania ITP oprávnenými subjektami v Slovenskej republike

2.1 Slovenská informačná služba

Zo Správy o činnosti Slovenskej informačnej služby za rok 2017 vyplýva, že Slovenská informačná služba v roku 2017 podala 311 žiadostí o použitie ITP, z toho zákonný sudca odmietol, resp. vrátil 7 žiadostí SIS o použitie ITP. Z uvedených 7 žiadostí SIS, ktoré sú vykázané v časti „odmietnuté žiadosti sudcom", bola rozhodnutím zákonného sudcu zamietnutá 1 žiadosť o použitie ITP a zvyšných 6 žiadostí bolo vrátených sudcom bez rozhodnutia (pre vecnú nepríslušnosť sudcu). V termíne prípravy správy (ku dňu 8. 2. 2018) bolo z hľadiska dosiahnutia zákonom uznaného účelu a cieľa z 304 súdom schválených žiadostí o ITP vyhodnotených 197 prípadov použitia ITP. Zákonom uznaný účel a cieľ bol dosiahnutý pri 183 vyhodnotených prípadoch

a nebol dosiahnutý v 14 prípadoch použitia ITP. K termínu predloženia podkladov tejto správy nebolo možné vyhodnotiť zvyšných 107 realizovaných prípadov použitia ITP, ktoré sú stále aktuálne alebo im plynie 30-dňová lehota na vyhodnotenie po ukončení použitia ITP.

Používanie ITP v podmienkach SIS v plnom rozsahu zodpovedá podmienkam ustanoveným zákonom č. 46/1993 Z. z. a zákonom č. 166/2003 Z. z.

Všetky prípady použitia ITP v roku 2017 boli podložené potrebným súhlasom zákonného sudcu a v žiadnom prípade nedošlo k nezákonnému použitiu ITP.[2]

Počet použitia ITP, z ktorých boli informácie použité ako dôkaz v trestnom konaní je 0 v roku 2017.

2.2 Vojenské spravodajstvo

V Správe o činnosti Vojenského spravodajstva za rok 2017 sa uvádza, že Vojenské spravodajstvo v období od 1. 1. 2017 do 31. 12. 2017 predložilo zákonným sudcom celkom 65 žiadostí na použitie ITP. Zákonnými sudcami bolo vydaných 65 súhlasov na použitie ITP. Z celkového počtu 65 vydaných písomných súhlasov zákonného sudcu na použitie ITP bol zákonom uznaný účel a cieľ dosiahnutý v 54 prípadoch. Informácie získané použitím ITP v roku 2017 boli v 2 prípadoch poskytnuté orgánom činným v trestnom konaní. Ani v jednom prípade nedošlo k nezákonnému použitiu ITP.[3]

2.3 Policajný zbor

Jednotlivé žiadosti na použitie ITP podľa zákona č. 166/2003 Z. z. v znení neskorších predpisov sa v roku 2017 realizovali takto:

1. Podľa § 4 ods. 1 bolo uplatnených 979 žiadostí na použitie ITP, pričom zákonný sudca udelil súhlas v 941 prípadoch a v 38 prípadoch nevydal súhlas na použitie ITP.
2. Žiadosti o predĺženie doby použitia ITP podľa § 4 ods. 2 boli predložené v 113 prípadoch, súhlas na použitie ITP bol vydaný v 97 prípadoch a v 16 prípadoch súhlas na použitie ITP vydaný nebol.
3. Žiadosť o dodatočný súhlas zákonného sudcu vo výnimočnom prípade, keď vec neznesie odklad podľa § 5 ods. 1 a 2 bola predložená v 1 prípade, pričom zákonný sudca udelil v tomto prípade súhlas.
4. Dosiahnutý zákonom uznaný účel a cieľ použitia ITP podľa § 3 a § 7 bol v 883 prípadoch a v 156 prípadoch nebol tento účel a cieľ dosiahnutý.
5. Informácie získané použitím ITP boli využité ako dôkaz v trestnom konaní v 30 prípadoch.
6. Nezákonné použitie ITP Policajným zborom v roku 2017 nebolo zákonným sudcom zistené.[4]

[2] Správa o činnosti Slovenskej informačnej služby za rok 2017. [online] [cit. 2019-03-03] dostupné na internete: <http://www.sis.gov.sk/pre-vas/sprava-o-cinnosti-2017.html>.

[3] Správa o činnosti Vojenského spravodajstva za rok 2017. [online] [cit. 2019-03-03] dostupné na internete: <http://vs.mosr.sk/sprava-o-cinnosti-vs-2017/>.

[4] Správa Výboru Národnej rady Slovenskej republiky pre obranu a bezpečnosť o stave použitia informačno-technických prostriedkov za rok 2017. [online] [cit. 2018-04-10] dostupné na internete: <http://www.nrsr.sk/web/Dynamic/Download.aspx?DocID=449691>.

2.4 Finančná správa

Finančná správa predložila v roku 2017 zákonnému sudcovi celkom 85 prvotných písomných žiadostí podľa § 4 ods. 1 zákona č. 166/2003 Z. z., z ktorých bol v 79 prípadoch písomne vydaný súhlas zákonného sudcu na použitie ITP. Finančná správa eviduje 6 odmietnutých žiadostí zákonného sudcu na použitie ITP.

Finančná správa predložila zákonnému sudcovi v 7 prípadoch opakovanú žiadosť na predĺženie doby použitia ITP podľa § 4 ods. 2 zákona č. 166/2003 Z. z. Vo všetkých 7 prípadoch bol zákonným sudcom vydaný písomný súhlas s predĺžením doby použitia ITP.

Finančná správa neeviduje žiadny prípad použitia ITP podľa § 5 ods. 1 a 2 zákona č. 166/2003 Z. z.

Z celkového počtu súhlasov vydaných zákonným sudcom bol v 72 prípadoch dosiahnutý zákonom uznávaný účel a cieľ, ktorý bol povolený zákonným sudcom, s väzbou na ustanovenia § 3 a 7 zákona č. 166/2003 Z. z., v súlade s ktorými možno ITP použiť 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, teda zistili sa skutočnosti významné na dosiahnutie zákonom ustanoveného účelu použitia ITP. Finančná správa eviduje 1 prípad použitia ITP, u ktorého nebol dosiahnutý zákonom uznávaný cieľ.

Finančná správa eviduje 2 prípady, v ktorých informácie získané použitím ITP boli použité ako dôkaz v trestnom konaní.

Z celkového počtu prípadov nebol zaznamenaný žiadny prípad nezákonného použitia ITP.[5]

2.5 Zbor väzenskej a justičnej stráže

Zbor väzenskej a justičnej stráže nepodal za rok 2017 žiadnu žiadosť o vydanie súhlasu na použitie ITP podľa § 4 ods. 1 a § 4 ods. 2 zák. č. 166/2003 Z. z.[6]

3 Využitie informácií získaných mimoprocesným použitím v trestnom konaní

V období po celospoločenských zmenách v bývalom Československu v roku 1989 prišlo v nadväznosti k zmenám v štruktúre, stave a dynamike kriminality ako aj v záujme právnej istoty občanov postupne k zavedeniu do trestného konania nových dôkazných prostriedkov a spôsobov zabezpečovania informácií dôležitých pre trestné konanie.

Môžeme konštatovať, že tradičné prístupy k riešeniu kriminality, ktoré nachádzajú odraz v aj v Trestnom práve sú v kontexte nových bezpečnostných výziev (medzinárodná organizovaná trestná činnosť, terorizmus, kyberkriminalita a pod.) takmer vyčerpané a prekonané. Uvedené sa v plnej miere prejavuje aj v trestnom práve procesnom, osobitne v trestnom konaní. V súčasnosti platná právna úprava v Slovenskej republike v ustanovení § 119 ods. 2 zákona č. 301/2005

[5] Správa Výboru Národnej rady Slovenskej republiky pre obranu a bezpečnosť o stave použitia informačno-technických prostriedkov za rok 2017. [online] [cit. 2018-04-10] dostupné na internete: <http://www.nrsr.sk/web/Dynamic/Download.aspx?DocID=449691>.

[6] Správa Výboru Národnej rady Slovenskej republiky pre obranu a bezpečnosť o stave použitia informačno-technických prostriedkov za rok 2016. [online] [cit. 2018-04-10] dostupné na internete: <http://www.nrsr.sk/dl/Browser/Document?documentId=259062>.
Správa Výboru Národnej rady Slovenskej republiky pre obranu a bezpečnosť o stave použitia informačno-technických prostriedkov za rok 2017. [online] [cit. 2018-04-10] dostupné na internete: <http://www.nrsr.sk/web/Dynamic/Download.aspx?DocID=449691>.

Z. z. Trestný poriadok uvádza len príkladmo výpočet dôkazných prostriedkov a teda a priori nevylučuje využitie aj iných za dodržania zákonných požiadaviek.

Máme za to, že v súčasnosti nie je možné vždy rekonštruovať a zachytiť priebeh skutkového deja za využitia „tradičných" dôkazných prostriedkov". Zabezpečenie neodvratnosti trestného postihu páchateľov trestnej činnosti si bezpochyby vyžiada akceptáciu informácií ako dôkazov, získaných aj z výsledkov spravodajskej činnosti – teda spravodajských informácií. Podľa nášho názoru toto tvrdenie má oporu aj v súčasnosti platnej legislatíva v Slovenskej republike. Jedným z míľnikov v tomto smere bolo prijatie zákona č. 166/2003 Z. z., ktorý výslovne zakotvuje možnosť použitia takto získaných informácií ako dôkazov v trestnom konaní.

Na tomto mieste by sme chceli uviesť niekoľko poznámok k otázke prípustnosti a zákonnosti dôkazov. Prípustnosť dôkazov je odbornej literatúre často označovaná aj ako zákonnosť dôkazov. Oba uvedené pojmy sú vzájomne previazané, spojené a ich dôsledné rozlíšenie nie je vždy možné. Prípustnosť dôkazov je charakterizovaná významovo širšie ako zákonnosť dôkazov. Nie každý nezákonne získaný dôkaz je neprípustný, ale nie každý neprípustný dôkaz je nezákonný. Neprípustnosť v sebe zahŕňa nie len neprípustnosť vyplývajúcu z nezákonného dôkazu, ale aj neprípustnosť danú prameňom dôkazu a neprípustnosť z formálneho dôvodu časovej preklúzie preloženia dôkazov procesnými stranami na súd.

Trestný poriadok Slovenskej republiky používa pojem zákonnosť. Zákonnosť v danom prípade znamená, že určitý dôkazný prostriedok je prípustný podľa zákona a bol získaný postupom orgánu činného v trestnom konaní a súdu, ktorý je v súlade s právnymi predpismi. Za dôkaz, ktorý bol získaný nezákonným spôsobom, sa považuje nielen dôkaz, pri ktorom bola nezákonnosť spôsobená, ale aj každý dôkaz získaný na základe takého dôkazu. Dôkazy získané nezákonným zásahom do ústavných práv fyzických osôb sú v trestnom konaní nepoužiteľné, pretože nespĺňajú podmienky ustanovení v § 119 ods. 2 Trestného poriadku.

V právnej teórii sa uplatňuje aj 5 kritérií hodnotenia zákonnosti dôkazu uvádzaných Repíkom:

1. či bol dôkaz získaný z prameňa, ktorý stanoví prípadne pripúšťa zákon,
2. či bol dôkaz získaný a vykonaný procesným subjektom k tomu zákonom oprávneným,
3. 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. j. také dôkazy, ktoré môžu byť podkladom pre rozhodnutie v trestnom stíhaní najmä pre rozhodnutie súdu,
4. či sa získaný a vykonaný dôkaz týka predmetu dokazovania v danom proces, t. j. či sa týka skutku o ktorom sa vedie konanie prípadne otázok, o ktorých je potrebné podľa zákona v súvislosti s týmto skutkom rozhodovať,
5. či bol dôkaz získaný a vykonaný spôsobom, ktorý ustanovuje, prípadne pripúšťa zákon.

Dávame do pozornosti, že z judikatúry Európskeho súdu pre ľudské práva okrem iného vyplýva – Dohovor o ochrane ľudských práv a základných slobôd dokazovanie ako také neupravuje, pričom sa priamo dotýka len niektorých jeho aspektov. K otázke prípustnosti dôkazov opakovane zdôraznil, že Dohovor neupravuje otázky prípustnosti dôkazov a táto oblasť patrí do pôsobnosti vnútro štátneho práva subjektov. Európsky súd pre ľudské práva ďalej konštatoval, že znenie čl. 6 ods. 1 Dohovoru nestanovuje žiadne pravidlá prípustnosti dôkazu a je úlohou súdu 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 vyslovil záver, že použitie určitého dôkazu voči obvinenému porušilo jeho právo na spravodlivý proces.

ITP sú spôsobované intenzívne zásahy do práva na súkromie. Ide o právo, ktoré je v našich podmienkach garantované ústavnoprávne (čl. 16 ods. 1 Ústavy Slovenskej republiky). V rozhodovacej činnosti Európskeho súdu pre ľudské práva v ostatnej dobe môžeme sledovať posun od princípu zachovávania absolútnej ochrany ľudských práv a slobôd k zvýrazňovaniu ochrany verejného záujmu.

Štátne orgány sú oprávnené do tohto práva zasahovať ak je takýto zásah v súlade so zákonom a je nevyhnutný v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom alebo zločinnosti, ochrany zdravia alebo morálky alebo ak je to potrebné na ochranu práv a slobôd iných.

Na tomto mieste je vhodné uviesť, že zásahy štátnych orgánov do práva na súkromie sú ESĽP posudzované na základe troch hľadísk:

- legalita,
- legitimita,
- proporcionalita.

Legalita znamená, že príslušné orgány môžu toto právo obmedziť výhradne len na základe zákona, čo vyplýva priamo z čl. 8 ods. 2 Dohovoru. Pri posudzovaní splnenia podmienky legality sa vychádza z toho, či bola rešpektovaná dostupnosť a predvídateľnosť zákona.

V článku 8 ods. 2 Dohovoru je priamo stanovená aj legitímnosť zásahu do práva na súkromie. To znamená, že do práva na súkromie možno zasiahnuť len vtedy, ak je to v záujme štátnych orgánov z dôvodu ochrany národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom alebo zločinnosti, ochrany zdravia alebo morálky alebo ak je to potrebné na ochranu práv a slobôd iných. Pri posudzovaní legitimity je skúmaná otázka či vykonané opatrenie zodpovedalo prípustnému cieľu, ako je vyššie uvedené.

Proporcionalita 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 dosiahnuť legitímny cieľ, možnosť uplatniť voľnú úvahu, pričom sú limitované tým, že zásah do práva na súkromie vykonajú len vtedy, keď je to nevyhnutné, teda v duchu požiadaviek kladených na demokratickú spoločnosť. Inými slovami, štátne orgány môžu k zásahu prikročiť len vtedy, keď je to nevyhnutné a sledovaný cieľ nemožno dosiahnuť miernejšími prostriedkami.

Z uvedeného vyplýva, že zásahy do práva na súkromie môžu byť realizované len vtedy, ak sú legálne, legitímne a proporcionálne, pričom podmienky musia byť splnené súčasne.

Domnievame sa, že je vhodné upriamiť pozornosť vo vzťahu k používaniu informačno-technických prostriedkov na niektoré legislatívne rozpory medzi právnou úpravou v zákone č. 301/2005 Z. z. Trestný poriadok a v 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).

Trestný poriadok uvádza stanovuje obligatórny obsah príkazu na použitie informačno-technického prostriedku, avšak zákon o ochrane pred odpočúvaním používa pojem súhlas a stanovuje náležitosti žiadosti o vydanie súhlasu.

Obdobne je rozdielny prístup zákonodarcu aj v otázke ex post notifikačného mechanizmu vo vzťahu k osobám dotknutým použitím ITP. Pri odpočúvaní realizovanom mimo trestného konania podľa zákona č. 166/2003 Z. z. právna úprava za žiadnych okolností neukladá príslušným orgánom povinnosť oboznámiť dotknutú osobu o tom, že bola odpočúvaná.

Zásadný rozdiel zaznamenávame medzi Trestným poriadkom a zákonom o ochrane pred odpočúvaním aj pri úprave použitia získaných informácií v inej trestnej veci. V zmysle ustanovenia § 115 ods. 7 Trestného poriadku získané informácie, je možné využiť v tom konaní, v ktorom

sa použitie tohto prostriedku nariadilo. Ich použitie v inej trestnej veci je možné za podmienky, že sa súčasne aj v tejto inej trestnej veci vedie trestné stíhanie pre taký trestný čin, pre ktorý je možné využiť tento prostriedok v trestnom konaní (§ 115 ods. 1 Trestného poriadku). 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. V zmysle zákona č. 166/2003 Z. z. (mimoprocesná rovina), sa nestanovujú žiadne takéto obmedzenia pre použiteľnosť získaných dôkazov. Ak sa prostredníctvom ITP, 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 používania týchto prostriedkov alebo až po ich ukončení a v čase používania záznamov z nich získaných, muselo byť v trestnej veci vedené trestné stíhanie. 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.[7]

Máme za to, že informácie získané mimoprocesným použitím ITP môžu byť vo vzťahu k trestnému konaniu využité v rôznych smeroch. Jedno z delení by podľa nás mohlo byt nasledovné:

a) operatívno-taktické informácie,
b) podnet pre trestné konanie,
c) dôkaz v trestnom konaní.

Ad. a): informácie získané použitím ITP a zákonným spôsobom poskytnuté orgánom činným v trestnom konaní môžu byť nimi využité aj pri plánovaní úkonov a opatrení ako aj taktiky ďalšieho postupu. Môžu slúžiť na orientáciu orgánu činného v trestnom konaní pri vedení výsluchu, vyhľadávaní vecných a listinných dôkazov, svedkov a podobne.

Ad. b): V zmysle ustanovení § 196 ods. 1 zákona č. 301/2005 Z. z. Trestný poriadok orgány činné v trestnom konaní zisťujú skutočnosti nasvedčujúce tomu, že bol spáchaný trestný čin z trestného oznámenia. Avšak podnety na začatie trestného konania môžu pochádzať aj z vlastných zistení orgánov činných v trestnom konaní, či z informácií (aj z použitia ITP), ktoré im odovzdali príslušné služby Policajného zboru, Zbor väzenskej a justičnej stráže, Finančná správa SR, alebo aj spravodajské služby.

Ad. c): Ako sme už uviedli, dokazovanie má v trestnom konaní nezastupiteľné miesto. V zmysle § 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.

Záver

Vychádzajúc z poznania vyššie uvedeného, je zrejmé, že v historickom kontexte dochádza k postupnému rozširovaniu množstva dôkazných prostriedkov akceptovaných v trestnom konaní. Máme za to, že v súčasnej dobe jednak z hľadiska prudkého rozvoja informačných a digitálnych technológií a jednak z hľadiska nových bezpečnostných hrozieb a výziev, predovšetkým organizovaného zločinu a terorizmu, bude postupne nevyhnutné zavedenie a pripustenie nových dôkazných prostriedkov ako zdrojov dôkazov.

[7] TITTLOVÁ, M.: Teoretické a praktické problémy odpočúvania a záznamu telekomunikačnej prevádzky v trestnom konaní. ZÁHORA, J. (ed.): Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní. Praha: Leges, 2017, 148 s.

Informácie získané mimoprocesným použitím ITP v zmysle 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) majú v trestnom konaní svoje nezastupiteľné miesto a ich význam a frekvencia použitia, predovšetkým v procese dokazovania, bude narastať.

Problematika mimoprocesného použitia ITP bude v blízkej dobe pravdepodobne opätovne preskúmavaná v kontexte úvah o novej právnej úprave operatívno-pátracej činnosti a najmú jej prostriedkov. V súčasnosti je však nemožné vyvodiť exaktné závery akým smerom sa zákonodarca v tejto citlivej oblasti (z hľadiska rešpektovania ľudských práv a slobôd) oblasti vyberie. Sú realizované vedecko-výskumné aktivity, v podmienkach Akadémie Policajného zboru v Bratislave výskum č. 231 „Národný model kriminálneho spravodajstva" realizovaný kolektívom odborníkov pod vedením prof. Stieranku.

Riešenie uvedených okruhov problémov si vyžiada odbornú diskusiu a podľa nášho názoru následne aj určité legislatívne, organizačné a logistické zmeny.

Literatúra

IVOR, J. a kol.: Trestné právo procesné. Druhé, doplnené a prepracované vydanie. Bratislava: Iura Edition, 2010, s. 419. ISBN 9788080783099.

IVOR, J. – POLÁK, P. – ZÁHORA, J.: Trestné právo procesné 1. Bratislava: Wolters Kluwer, 2017, 528 s. ISBN 978-80-8168-593-4.

LISOŇ, M.: Odhaľovanie a objasňovanie trestných činov všeobecnej kriminality. Bratislava: Akadémia PZ v Bratislave, 2016, 248 s. ISBN 978-80-8054-673-1.

LISOŇ, M. – VAŠKO, A. a kol.: Teória kriminálno-policajného poznania. Bratislava: Wolters Kluwer, 2018. 392 s. ISBN 978-80-8168-838-6.

MARKO, M. – KOHAN, P.: Legislatívna úprava operatívno-pátracej a spravodajskej činnosti v Slovenskej republike. In: STIERANKA, J. – MARKO, M. a kol.: Aktuálne otázky aplikácie kriminálneho spravodajstva v kontexte nových trendov v Európskej únii. Bratislava: Akadémia PZ v Bratislave, 2018, 134 s. ISBN 978-80-8054-760-8.

STIERANKA, J. a kol.: Spravodajská činnosť. Bratislava: Akadémia PZ v Bratislave, 2013. 316 s. ISBN 9788080545499.

TITTLOVÁ, M.: Teoretické a praktické problémy odpočúvania a záznamu telekomunikačnej prevádzky v trestnom konaní. ZÁHORA, J. (ed.): Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní. Praha: Leges, 2017, 288 s. ISBN 978-80-7502-206-6.

Správa o činnosti Slovenskej informačnej služby za rok 2017. [online] [cit. 2019-03-03] dostupné na internete: <http://www.sis.gov.sk/pre-vas/sprava-o-cinnosti-2017.html>.

Správa Výboru Národnej rady Slovenskej republiky pre obranu a bezpečnosť o stave použitia informačno-technických prostriedkov za rok 2017. [online] [cit. 2018-04-10] dostupné na internete: <http://www.nrsr.sk/web/Dynamic/Download.aspx?DocID=449691>.

Správa Výboru Národnej rady Slovenskej republiky pre obranu a bezpečnosť o stave použitia informačno-technických prostriedkov za rok 2016. [online] [cit. 2018-04-10] dostupné na internete: <http://www.nrsr.sk/dl/Browser/Document?documentId=259062>.

Správa Výboru Národnej rady Slovenskej republiky pre obranu a bezpečnosť o stave použitia informačno-technických prostriedkov za rok 2017. [online] [cit. 2018-04-10] dostupné na internete: <http://www.nrsr.sk/web/Dynamic/Download.aspx?DocID=449691>.

Správa o činnosti Vojenského spravodajstva za rok 2017. [online] [cit. 2019-03-03] dostupné na internete: <http://vs.mosr.sk/sprava-o-cinnosti-vs-2017/>.

Správa Výboru Národnej rady Slovenskej republiky pre obranu a bezpečnosť o stave použitia informačno-technických prostriedkov za rok 2017. [online] [cit. 2018-04-10] dostupné na internete: <http://www.nrsr.sk/web/Dynamic/Download.aspx?DocID=449691>.

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).

Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

Zákon č. 46/1993 Z. z. o Slovenskej informačnej službe v znení neskorších predpisov.

Zákon č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov.

Zákon č. 198/1994 Z. z. o Vojenskom spravodajstve v znení neskorších predpisov.

Zákon č. 4/2001 Z. z. o Zbore väzenskej a justičnej stráže v znení neskorších predpisov. Zákon č. 35/2019 Z. z. o finančnej správe a o zmene a doplnení niektorých zákonov.

Použitie informačno-technických prostriedkov a nezodpovedané otázky

Using of Information Technical-intelligence Measures and Unanswered Questions

Michal Aláč[1]

Abstrakt: *Podmienky použitia informačno-technických prostriedkov sú predmetom častých diskusií. Ide o oblasť, kde sa stretávajú vedy právne, technické a politické. Odborníci tak z akademickej obce ako aj odborníci z aplikačnej praxe väčšinou vnímajú problematiku použitia informačno-technických prostriedkov cez prizmu svojho vedného odboru, čo spôsobuje, že vznikajú v predmetnej problematike šedé zóny a objavuje sa čoraz väčšie množstvo nezodpovedaných a často veľmi citlivých, ba až nepríjemných otázok. V predmetnom príspevku sa pokúsime poukázať na niekoľko z nich.*

Abstract: *The conditions for using information technical-intelligence measures are subject to frequent discussions. This is an area where legal, technical and political science meet. Experts from both academia and application practice mostly perceive the use of technical-intelligence measures through the prism of their science, causing gray areas to emerge in the subject matter and an increasing number of unresponsive and often very sensitive, even unpleasant, issues. questions. In this paper, we will try to highlight a few of them.*

Kľúčové slová: *informačno-technický prostriedok, operátor, legalita, legitimita, bezpečnostné riziko.*

Key words: *technical-intelligence measure, provider, legality, legitimity, security risk.*

1. Zmeny podľa zákona č. 404/2015 Z. z.

V rámci tzv. teroristického balíčka zákonov[2] bol prijatý 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, ktorý nadobudol účinnosť od 1. 1. 2016 a priniesol niekoľko, prevažne dôležitých zmien. Prvou zmenou bola zmena definície pojmu informačno-technický prostriedok. Podľa § 2 ods. 1 cit. zákona sa informačno-technickými prostriedkami rozumejú elektrotechnické, rádiotechnické, 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] JUDr. Michal Aláč, PhD., Trnavská univerzita v Trnave, Právnická fakulta, Katedra správneho práva, práva životného prostredia a finančného práva, Hornopotočná 23, 917 01 Trnava, e-mail: michal.alac@truni.sk.

[2] Zákon č. 397/2017 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, 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, zákon 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.

Došlo v podstate k zjednoteniu terminológie, kedy zákon o ochrane pred odpočúvaním prevzal v písmene b) terminológiu zákona č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov (ďalej len „zákon o elektronických komunikáciách"). V písmene c) zákonodarca reflektoval na skutočnosť, že cit. ustanovenie obsahuje len fakultatívny výpočet prostriedkov, ktoré môžu byť používané utajovaným spôsobom na získavanie informácií, a preto bolo potrebné precizovať okruh výsledkov použitia informačno-technických prostriedkov. V dôvodovej správe predkladateľ návrhu predmetného zákona, ktorým bolo Ministerstvo vnútra Slovenskej republiky, uviedol, že vzhľadom na technologický vývoj sa navrhuje precizovať definíciu informačno-technických prostriedkov tak, aby zahŕňala aj softvérové prostriedky a zariadenia a získavanie obsahu správ prenášaných prostredníctvom elektronických komunikačných sietí.[3]

Zákonom 404/2015 Z. z. došlo aj k rozšíreniu zákazu podľa § 2 ods. 7, kedy zákonodarca ustanovil, že orgány územnej samosprávy, súkromné bezpečnostné služby ani iná fyzická osoba alebo právnická osoba nesmie mať v držbe ani použiť informačno-technický prostriedok. Pôvodne sa zákaz vzťahoval len na použitie informačno-technického prostriedku. V kontexte znenia definície pojmu informačno-technický prostriedok podľa ust. § 2 ods. 1 ide však o obsolentný zákaz, pretože, či daný prostriedok je informačno-technickým prostriedkom nezávisí od jeho technickej konštrukcie, ale od spôsobu jeho použitia, a teda nie je možné ustanoviť, na držbu ktorého prostriedku sa zákaz vzťahuje, pretože každá osoba má v držbe prostriedok, ktorý napr. možno použiť na vyhotovenie obrazových záznamov. Ide totiž o ľubovoľný fotoaparát, mobilný telefón s fotoaparátom, videovrátnika alebo iný technický prostriedok konštrukčne spôsobilý vyhotoviť obrazový alebo obrazovo-zvukový záznam. Iná situácia je v prípade použitia informačno-technického prostriedku, ktoré by mohlo byť subsumované pod cit. zákaz. Uvedený zákaz použitia by sa mohol vzťahovať na konanie, ktorým by nejaká fyzická osoba, právnická osoba alebo orgán územnej samosprávy utajovaným spôsobom zasahovala do súkromia inej fyzickej osoby napríklad skrytým vyhotovovaním obrazových záznamov. Za porušenie uvedenej povinnosti zdržať sa takéhoto konania však zákon neukladá žiadnu sankciu. Z čisto teoretického hľadiska by ako jediná konzekvencia mohlo byť konštatované, že predmetný záznam by nemohol byť použitý ako dôkaz v súdnom alebo správnom konaní, keďže ide o záznam vyhotovený v rozpore so zákonom.

Ďalšia zmena sa týkala dikcie ust. § 3 ods. 1 prevej vety, ktorej cieľom bolo posilniť zásadu legality, legitimity a proporcionality použitia informačno-technických prostriedkov. Podľa cit. ustanovenia možno informačno-technický prostriedok 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; informačno-technické prostriedky možno v pôsobnosti Slovenskej informačnej služby a Vojenského spravodajstva použiť aj mimo územia Slovenskej republiky v rozsahu úloh podľa osobitných predpisov. Najdôležitejšou zmenou tohto ustanovenia je rozšírenie účelov, na ktoré možno použiť informačno-technické prostriedky, a to na získavanie informácií zo zahraničných zdrojov. Zároveň predmetné ustanovenie *expressis verbis* ustanovilo oprávnenie Slovenskej informačnej služby a Vojenského spravodajstva aj mimo územia Slovenskej republiky. Zákonodarca však opomenul ustanoviť za akých podmienok. Určil len, že sú oprávnené použiť v rozsahu úloh

[3] Osobitná časť dôvodovej správy k návrh zákona, 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.

podľa osobitných predpisov, avšak neustanovil či sa na daný postup vzťahujú ďalšie ustanovenia zákona o ochrane pred odpočúvaním, a to najmä, či je na použitie informačno-technických prostriedkov mimo územia Slovenskej republiky potrebný súhlas súdu. Keďže zákonodarca neustanovil žiadnu výnimku, ust. § 4 cit. zákona by sa na uvedené použitie informačno-technických prostriedkov malo aplikovať, avšak legitimita takejto súdnej aprobácie použitia informačno-technického prostriedku v zahraničí by mohla byť otázna. Avšak v nadväznosti na aktuálne svetové bezpečnostné hrozby a v záujme poskytnutia čo najvyššej možnej miery ochrany súkromia dotknutých fyzických osôb na jednej strane a ochrany záujmov Slovenskej republiky zákonným spôsobom na druhej strane, je viac než žiaduce, aby príslušný súd preskúmal a následne odsúhlasil, že došlo k splneniu všetkých podmienok na použitie informačno-technického prostriedku mimo územia Slovenskej republiky, aby nebolo možné spochybniť legalitu a legitimitu takéhoto postupu.

Najvýraznejšia zmena nastala v oblasti kontroly použitia informačno-technických prostriedkov. Kontrolu používania informačno-technických prostriedkov vykonáva Národná rada Slovenskej republiky, ktorá na účely výkonu kontroly zriaďuje komisiu na kontrolu používania informačno-technických prostriedkov (ďalej len „komisia"). Komisia sa skladá z predsedu komisie a ďalších siedmich členov komisie. Ide o model kontroly, pri ktorom by na kontrolnej činnosti okrem poslancov Národnej rady Slovenskej republiky participovali aj odborníci z praxe. Šiestich členov komisie totiž volí Národná rada Slovenskej republiky spomedzi členov Osobitného kontrolného výboru Národnej rady Slovenskej republiky na kontrolu činnosti Slovenskej informačnej služby, členov Osobitného kontrolného výboru Národnej rady Slovenskej republiky na kontrolu činnosti Vojenského spravodajstva a členov výboru Národnej rady Slovenskej republiky pre obranu a bezpečnosť, a to dvoch členov z každého z uvedených výborov, a to tak, aby zo zvolených členov komisie traja boli zástupcami navrhnutými politickými stranami alebo politickými hnutiami, ktoré majú zastúpenie vo vláde Slovenskej republiky, a traja zástupcami navrhnutými politickými stranami alebo politickými hnutiami, ktoré nemajú zastúpenie vo vláde Slovenskej republiky, a súčasne, aby predseda komisie bol zástupcom navrhnutým politickými stranami alebo politickými hnutiami, ktoré nemajú zastúpenie vo vláde Slovenskej republiky. Ďalších dvoch členov komisie volí Národná rada Slovenskej republiky spomedzi kandidátov na členov komisie, ktorých predkladá Národnej rade Slovenskej republiky predseda výboru Národnej rady Slovenskej republiky pre obranu a bezpečnosť, po predchádzajúcej dohode s predsedom Osobitného kontrolného výboru Národnej rady Slovenskej republiky na kontrolu činnosti Slovenskej informačnej služby a predsedom Osobitného kontrolného výboru Národnej rady Slovenskej republiky na kontrolu činnosti Vojenského spravodajstva. Takýmto členom môže byť len občan Slovenskej republiky, ktorý je držiteľom platného osvedčenia Národného bezpečnostného úradu na oboznamovanie sa s utajovanými skutočnosťami stupňa utajenia „Prísne tajné", dosiahol vek 40 rokov, vykonával funkciu sudcu, prokurátora, príslušníka spravodajskej služby alebo Policajného zboru alebo inú funkciu, povolanie alebo zamestnanie v oblasti právnej a bezpečnostnej teórie a praxe alebo medzinárodných vzťahov a diplomacie najmenej 10 rokov a má vysokoškolské vzdelanie druhého stupňa.

Z teoreticko-právneho hľadiska ide o model kontroly, ktorý môže byť veľmi efektívny, kedy najmä odborníci z praxe by mali vedieť posúdiť relevanciu a nevyhnutnosť použitia informačno-technických prostriedkov na vyššej úrovni ako členovia Národnej rady Slovenskej republiky, ktorí pravdepodobne za sebou nemajú žiadnu bezpečnostnú prax. Z hľadiska aplikačnej praxe sa však vynárajú dve základné otázky.

Prvou je, či osoba, ktorá má byť odborníkom z praxe môže aj paralelne s výkonom funkcie člena komisie vykonávať bezpečnostnú prax. Napríklad, či za člena komisie môže byť zvolená

osoba, ktorá je ešte stále v služobnom pomere policajta podľa 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 v znení neskorších predpisov alebo osoba, ktorá v súčasnosti vykonáva povolanie v oblasti diplomacie. V ust. § 8a ods. 4 zákona o ochrane pred odpočúvaním zákonodarca použil minulý čas: „...vykonával funkciu sudcu, prokurátora, príslušníka spravodajskej služby alebo Policajného zboru alebo inú funkciu, povolanie alebo zamestnanie v oblasti právnej a bezpečnostnej teórie a praxe alebo medzinárodných vzťahov a diplomacie najmenej 10 rokov...". Podľa ust. § 8a ods. 1 tretia veta je funkcia člena komisie čestnou a neplatenou funkciou, a preto je viac než pravdepodobné, že dotknutý odborník z praxe bude musieť mať iný spôsob zárobkovej činnosti.

Druhou otázkou je reálna efektivita kontroly používania informačno-technických prostriedkov komisiou, keďže predmetná právna úprava, ako už bolo uvedené, nadobudla účinnosť 1. 1. 2016, avšak do dňa spracovania tohto príspevku (4. 4. 2019) komisia nebola zriadená. Aj keď v čase spracovania tohto príspevku Národná rada Slovenskej republiky vo svojom pléne prerokovala správy vyššie uvedených výborov o stave použitia informačno-technických prostriedkov, reálna kontrola, a to aspoň v minimálnom rozsahu raz ročne, vykonaná nebola.

2. Rozsah ničenia záznamov a iných výsledkov

Zákon o ochrane pred odpočúvaním v § 7 ustanovuje za splnenia určitých podmienok povinnosť štátnych orgánov, oprávnených používať informačno-technické prostriedky, zničiť záznamy z použitia informačno-technických prostriedkov. Ak sa nedosiahol zákonom ustanovený účel, t. j. použitím sa nezistili 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 o ochrane pred odpočúvaním (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 prostriedku 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. Z pohľadu právnej teórie, ako aj praxe, je totiž 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 alebo kriminálneho spravodajstva, resp. operatívnych zložiek Policajného zboru.

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. Písomnosti, ktoré sú výsledkom spravodajsko-analytickej činnosti, sú sekundárnym výsledkom.

Zároveň je však potrebné poukázať aj na opačný prípad, a to keď sa použitím informačno-technického prostriedku dosiahol zákonom sledovaný účel a orgán, ktorý použil informačno-technický prostriedok, resp. ktorý žiadal o použitie informačno-technického prostriedku, musí záznam alebo iný výsledok po stanovenú dobu uchovať. V súčasnosti najmä technologický pokrok spôsobil, že záujmové osoby sú prostredníctvom použitia informačno-technických prostriedkov zdrojom neuveriteľného objemu dát, ktoré je po ich zaznamenaní potrebné spracovať a následne predpísaným spôsobom uchovať. A práve uchovávanie uvedených dát, t. j. záznamov a iných výsledkov bude *pro futuro* znamenať pre Slovenskú republiku značný problém, pretože úložné kapacity budú postupne dochádzať. Je však potrebné konštatovať, že v rámci členských štátov Európskej únie nejde o výnimočný problém a bezpečnostné zložky väčšiny štátov sa s ním musia vysporiadať.

3. Odpočúvanie a záznam telekomunikačnej prevádzky a povinnosti operátora podľa zákona o elektronických komunikáciách

Zákon o elektronických komunikáciách ustanovuje podmienky na poskytovanie elektronických komunikačných sietí a elektronických komunikačných služieb, v rámci ktorých ustanovuje aj rozsah súčinnosti, ktorú je osoba prevádzkujúca elektronické komunikačné siete a elektronické komunikačné služby (ďalej len „operátor") povinná poskytnúť oprávneným štátnym orgánom.

Podľa § 63 ods. 14 písm. a) je operátor povinný prevádzkovať verejné siete alebo poskytovať verejné služby takou technológiou vrátane jej jednotlivých častí a softvérového vybavenia, ktorá umožní pripojenie a prevádzkovanie zariadenia na odpočúvanie a zaznamenávanie prevádzky v sieti vo vlastníctve štátu a on-line prístup pre oprávnené orgány. Zároveň je operátor podľa § 63 ods. 14 písm. b) povinný umožniť pripojenie zariadenia na odpočúvanie a zaznamenávanie prevádzky v sieti podľa technickej špecifikácie tohto pripájaného zariadenia; náklady na zaobstaranie zariadenia na odpočúvanie a zaznamenávanie prevádzky v sieti vrátane jeho softvérového vybavenia a na zabezpečovanie servisnej podpory tohto zariadenia znáša orgán štátu, ktorý požiadal o pripojenie zariadenia na odpočúvanie a zaznamenávanie prevádzky v sieti. Z uvedených ustanovení vyplýva, že operátor je povinný zabezpečiť rozhranie tak, aby sa oprávnené štátne orgány mohli pripojiť na jeho technológiu.

Zákon o elektronických komunikáciách však neustanovuje povinnosť operátora prevádzkovať verejné siete alebo poskytovať verejné služby technológiou, ktorá sa nachádza na území Slo-

venskej republiky. Operátor má zabezpečiť len, aby sa oprávnené orgány mohli pripojiť na jeho technológiu a aby údaje, ktoré im je zo zákona povinný poskytnúť, boli v „čitateľnej forme“, t. j. vo formáte, ktorý oprávnené orgány dokážu spracovať. V praxi to môže znamenať bezpečnostné riziko, pretože v prípade, že sa operátor rozhodne poskytovať služby na území Slovenskej republiky prostredníctvom technológie nachádzajúcej sa v zahraničí, bude sa v zahraničí nachádzať aj tzv. „target list“, t. j. zoznam účastníckych staníc/koncových zariadení, ktorých telekomunikačná prevádzka je odpočúvaná a zaznamenávaná. Z bezpečnostného hľadiska ide o veľké riziko, pretože bezpečnostné orgány Slovenskej republiky a orgány činné v trestnom konaní poskytujú informácie o záujmových osobách na územie iného štátu bez výraznejšej možnosti kontroly nakladania s týmito údajmi. Aj akýkoľvek únik informácií bude na území iného štátu náročnejšie zistiť, eliminovať alebo vyvodiť trestnoprávnu zodpovednosť. Zároveň existuje zvýšené riziko, že k údajom o záujmových osobách slovenských bezpečnostných orgánov, nachádzajúcim sa v štáte „A“ sa budú snažiť dostať spravodajské služby štátu „B“ a možnosti spravodajskej ochrany týchto údajov zo strany Slovenskej republiky bude značne obmedzená.

V záujme ochrany spravodajských záujmov Slovenskej republiky by bolo vhodné preskúmať rozsah zaradenia technológie na prevádzkovanie verejných telekomunikačných sietí a poskytovanie verejných telekomunikačných služieb a jej príslušných softwarových a hardwarových častí pod prvky kritickej infraštruktúry podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších predpisov, čím by sa dosiahol stav, že technológia operátora by sa musela nachádzať na území Slovenskej republiky, čo by zamedzilo postupovaniu údajov do cudziny.

Povoľovací mechanizmus vo vzťahu k ITP[1]

Authorization Mechanism in Relation to Information Technology Means

Marcela Tittlová[2]

Abstrakt: *Požiadavky na efektívnosť a účinnosť odhaľovania a dokazovania závažnej trestnej činnosti smerovali nie len na národnej, ale aj na nadnárodnej úrovni, k tomu, že do právnych úprav sa inkorporovali viaceré moderné, ale súčasne ofenzívne a utajeným spôsobom realizované trestno-procesné i neprocesné inštitúty. Ich zmyslom je podporiť boj so závažnou trestnou činnosťou a ochranu garantovaných práv, hoci samé o sebe sa spájajú s určitým zásahom do nich. Ak majú demokratické a právne poriadky využívať prostriedky tajného dohľadu nad jednotlivcami, nutne musia obsahovať tieto právne úpravy aj dostatočné záruky ochrany dotknutých práv a ich garancie. Práve jednou z takýchto záruk je formulovaný povoľovací mechanizmus pri každom z informačno-technických prostriedkov. Zahŕňa tak časové súvislosti využívania týchto inštitútov, ako aj subjekty oprávnené rozhodnúť o ich použití, druh rozhodnutia, jeho formu a obsahové náležitosti. Je vidieť, že zákonodarca nie je v súvislosti s úpravou týchto požiadaviek vždy jednotný a osobitne je rozdiely možné vidieť v rámci procesnej a neprocesnej roviny použitia.*

Abstract: *The requirements for the efficiency and effectiveness of detection and proving of serious crime were directed not only at national but also at transnational level, as several modern but at the same time offensive and non-procedural institutes were incorporated into the legislation. Their main purpose is to support the fight against serious crime and the protection of guaranteed rights, although they themselves have some interference with them on the part of the persons concerned. If democratic and legal codes are to use the means of secret supervision of individuals, they must necessarily include sufficient safeguards for the protection of the rights in question and their guarantee. One of these guarantees is a formulated authorization mechanism for each of the information and technical means. It covers both the temporal use of these institutes as well as the entities authorized to decide on their use, the type of decision, its form and content. It can be seen that the legislator is not always consistent with the adaptation of these requirements, and in particular the differences can be seen within the procedural and non-procedural levels of use.*

Kľúčové slová*: informačno-technické prostriedky, časti a štádiá trestného konania, návrh na použitie, príkaz, súhlas s použitím, žiadosť, zásada judiciarity.*

Keywords: *information and technical means, parts and stages of criminal proceedings, application for use, order, consent to use, request, principle of judiciary.*

Úvod

Odhaľovanie a dokazovanie závažnej trestnej činnosti v podmienkach informačnej a technologicky vyspelej spoločnosti, v podmienkach integrovanej Európy, globalizovaného sveta a enormného rozvoja informačných a komunikačných technológií nie je možné efektívne a účinne realizovať cestou klasických prostriedkov, ktoré boli na tieto účely využívané v minulosti. Tak, ako sa vyvíja a modernizuje spoločnosť, tak ako sa prvky informačného a technického pokroku prejavujú v jej jednotlivých oblastiach, tak našli uplatnenie aj v *mode operandi* tých najzávažnejších trestných činov. Nejde pritom výhradne o prvok, s ktorým sa stretávame v súvislosti s odhaľova-

[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] Doc. PhDr. JUDr. Marcela Tittlová, PhD., Paneurópska vysoká škola, Fakulta práva, Ústav verejného práva, e-mail: marcela.tittlova@paneurouni.com.

ním a dokazovaním závažnej trestnej činnosti. Prvky informačnej spoločnosti, jej pokrok a modernizácia presahujú do kriminálneho správania sa akéhokoľvek charakteru. Mnohé, najmä tie najzávažnejšie druhy trestných činov, sa prirodzene spájajú s rovnako intenzívnymi následkami vo vzťahu k trestnoprávne relevantným objektom. Osobitne je vidieť pri týchto druhoch trestnej činnosti to, ako intenzívne zasahujú do oblasti garantovaných práv, ako ohrozujú a poškodzujú piliere právneho a demokratického štátu a ako zasahujú do koncepcie základných ľudských práv.

Modernizácia a inovácia na jednej strane predstavujú pozitívny prvok, element života našej spoločnosti. Ako neoddeliteľná súčasť trestnoprávne relevantného konania významne tieto prvky komplikujú samotné možnosti odhaľovania a následné dokazovanie tejto trestnej činnosti. S cieľom ochrany ľudských práv, demokratického a právneho zriadenia štátov je tak nutné, využívať moderné, veľmi ofenzívne trestno-procesné inštitúty, ktoré na jednej strane síce zefektívňujú boj s trestnou činnosťou, no na strane druhej zasahujú do niektorých relatívne chránených (teda nie absolútnych) základných ľudských práv. Je to štát, ktorý sa svojou činnosťou a funkciami, ktoré plní prostredníctvom svojich orgánov, podujal k ochrane práv a právom chránených záujmov jednotlivcov. Na jednej strane je garantom ochrany práv a právom chránených záujmov jednotlivcov, vrátane ochrany zákonom chránených druhov informácií, na strane druhej nutne k zabezpečeniu svojich činností, k plneniu svojich funkcií určité druhy informácií potrebuje získavať. Nutne ide aj o také, ktoré získava spravodajským spôsobom, utajene a pomerne intenzívnou mierou resp. formou, spôsobom zásahu do garantovaných práv, ku ktorých všeobecnej ochrane takto smeruje.

Aj ESĽP vo svojej rozhodovacej činnosti pripustil, že hoci prostriedky tajného dohľadu nad jednotlivcami a telekomunikáciami predstavujú nástroje policajných štátov, na účely ochrany práv a právom chránených záujmov, na dosahovanie proporcionálnych a legitímnych cieľov je možné ich do právnych úprav inkorporovať. Súčasne ale vyslovil požiadavku, že v takomto prípade musia právne poriadky obsahovať aj zodpovedajúce garancie, záruky nezneužívania takýchto prostriedkov a záruky práv jednotlivcov pred ich nezákonným, neoprávneným a nedôvodným používaním.[3]

V podmienkach nášho trestného konania ide najmä o sústavu zaisťovacích inštitútov, ktoré majú povahu informačno-technických prostriedkov, ktoré k takémuto cieľu majú smerovať. S cieľom dôslednej ochrany štátu, jednotlivcov a ich práv je priamo nutné, nevyhnutné doslova „obetovať" niektoré ľudské práva a pripustiť zásahy do nich v určitej miere a to za predpokladu stanovania jasných a presných podmienok, za ktorých sú takéto zásahy možné. Jednou z garancií ochrany práv a právom chránených záujmov jednotlivcov je súčasne povoľovací mechanizmus vo vzťahu k jednotlivým informačno-technickým prostriedkom (ITP), ktorý vymedzuje nie len možnosti využitia týchto prostriedkov v konkrétnych častiach a štádiách trestného konania, ale súčasne aj subjekty oprávnené rozhodnúť o použití týchto prostriedkov a druh rozhodnutia, ktorým sa tieto zásahy do garantovaných práv majú realizovať resp. na podklade ktorého sa majú realizovať, jeho formu a taktiež aj obsahové náležitosti.

1. Použitie ITP v rámci trestného konania a subjekty rozhodovania

V súlade s § 10 ods. 21 TP (Trestný poriadok; zákon č. 301/2005 Z. z. v znení neskorších predpisov, ďalej len „Trestný poriadok" alebo „TP") sa za informačno-technické prostriedky v trestnom konaní považujú *elektrotechnické, rádiotechnické, fototechnické, optické, mechanické, che-*

[3] Záhora, J. a kol.: Obrazové a zvukové záznamy v trestnom konaní. Bratislava: Wolters Kluwer, 2018, s. 41 a nasl.

mické 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. Uvedené ustanovenie determinuje povahu a rozsah informačno-technickej činnosti resp. prostriedkov, ktoré sa využívajú na účely:

- vyhotovovania obrazových, zvukových, obrazovo-zvukových záznamov (§ 114 TP)
- odpočúvania a záznamu telekomunikačnej prevádzky (§ 115 TP)
- oznámenia údajov o telekomunikačnej prevádzke (§ 116 TP) a
- zadržania a otvorenia zásielok (§ 108–109 TP).

V súvislosti s povoľovacím mechanizmom, ak ide o možnosti využitia týchto prostriedkov v rámci trestného konania, je dôležité uviesť, že využitie týchto prostriedkov je možné v zásade v celkom priebehu trestného konania, teda tak v konaní predsúdnom, ako aj v konaní pred súdom a rovnako tak aj v jeho častiach, kde je potrebné získavať informácie o možnom ďalšom postupe vo veci a na účely meritórneho rozhodnutia v nej (osobitne v rámci postupu pred začatím trestného stíhania i v prípravnom konaní).

Vyhotovovanie obrazových, zvukových a obrazovo zvukových záznamov *(§ 114 TP)* je možné v rámci celého trestného konania. V závislosti od štádia či fázy trestného konania sa odlišuje aj subjekt, ktorý je oprávnený povoľovať použitie tohto inštitútu. Jeho využitie je tak možné v:

a) postupe pred začatím trestného stíhania, kde použitie tohto prostriedku povoľuje sudca pre prípravné konanie,
b) v prípravnom konaní, kde jeho použitie povoľuje sudca pre prípravné konanie a
c) v konaní pred súdom, kde použitie povoľuje predseda senátu.

Ak by sa nespájalo vyhotovovanie záznamov so vstupom do obydlia a vec by nezniesla odklad, pričom v takejto časovej tiesni by sa nedal získať príkaz od sudcu pre prípravné konanie, prokurátor ho môže vydať aj sám. Ide však o prípady skutočne ojedinelé, typické časovou tiesňou, kedy sú splnené podmienky na vydanie príkazu a teda možno predpokladať, že aj sudca pre prípravné konanie by príkaz vydal, ale v takejto časovej tiesni nie je možné dosiahnuť jeho vydanie. Aby sa predišlo zmareniu získania dôležitých informácií v trestnom konaní, s týmto cieľom teda príkaz vydá aj prokurátor. Do 24 hodín od vydania však musí príkaz potvrdiť sudca pre prípravné konanie, aby bola aj tu zabezpečená nestranná a nezávislá súdna kontrola. Ak by sa tak nestalo, stráca príkaz prokurátora platnosť, je nutné ukončiť záznamovú činnosť a takéto záznamy sa predpísaným spôsobom zničia. Bez ohľadu na to, aké informácie by sa tatko získali, nie je možné ich použitie v trestnom konaní.

Prokurátor má v tomto prípade len návrhové oprávnenie vo vzťahu k príkazu, ktorý v predsúdnom konaní vydáva sudca pre prípravné konanie. Zasahuje sa do jeho pozície pána prípravného konania, lebo povolenie takto zásadných zásahov do základných ľudských práv je zverené nestrannému a nezávislému súdu. V každom prípade, prokurátorovi je zverené významné oprávnenie, keďže aj tu je jediným subjektom, ktorý je oprávnený navrhovať vydanie príkazu na použitie tohto inštitútu. Nie sú riešené náležitosti podávaného návrhu a tak možno aj na tomto mieste, že by bolo potrebné a vhodné ich sem zaviesť s cieľom posilnenia zodpovednosti prokurátora za podávaný návrh.[4]

V súvislosti *s odpočúvaním a záznamom telekomunikačnej prevádzky (§ 115 TP)* možno povedať, že trestno-procesná úprava tiež diferencuje možné použitie tohto prostriedku z hľadis-

[4] Tittlová, M.: Korupcia. Vybrané kriminologické a trestnoprávne aspekty. Bratislava: Wolters Kluwer, 2015, s. 167 a nasl.

ka častí a štádií 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 stretneme s názorom, že takto sa do určitej miery oslabuje postavenie prokurátora, ktoré je v predsúdnom konaní charakterizované ako *dominus litis*.[5] 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.

Ak vec neznesie odklad a v takto krátkej lehote, v časovej tiesni, nebude možné docieliť 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,

[5] Ivor, J., Polák, P., Záhora, J.: Trestné právo procesné. II. časť. Bratislava: Wolters Kluwer, 2017, s. 344 a nasl.

d) odpočúvane a záznam telekomunikačnej prevádzky sa v tomto prípade nemôže spájať so vstupom do obydlia,
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.

V súvislosti ***s oznámením údajov o telekomunikačnej prevádzky*** *(§ 116 TP)* je potrebné mať na zreteli nedávne novelizácie tohto inštitútu, kedy sa umožnilo v utajenom režime aj smerom do budúcna získavať tzv. prevádzkové údaje o uskutočnenej telekomunikačnej prevádzke. Táto možnosť sa doplnila popri možnosti oznamovania údajov o už uskutočnenej komunikácii (teda smerom do minulosti).[6] V súvislosti s povoľovaním mechanizmom možno povedať, že podľa fázy a štádia trestného konania sa odlišuje aj subjekt, ktorý je oprávnený povoliť použitie tohto inštitútu:

a) v postupe pred začatím trestného stíhania v prípravnom konaní vydáva takýto príkaz sudca pre prípravné konanie (znova na písomný a skutkovými okolnosťami odôvodnený návrh prokurátora),
b) v konaní pred súdom ho vydáva predseda senátu.

2. Príkaz smerujúci k použitiu ITP v trestnom konaní

Použitie informačno-technických prostriedkov v trestnom konaní sa viaže na vydanie príkazu, ktorý nasleduje po splnení zákonných podmienok pre použitie konkrétneho inštitútu. Vyššie uvedená zásada judiciarity zabezpečuje, že rozhodovanie o použití konkrétneho prostriedku nevychádza a neostáva na úrovni orgánov činných v trestnom konaní, ale že takto intenzívne zásahy do garantovaných práv povoľuje vždy a výhradne súd (sudca pre prípravné konanie na návrh prokurátora) alebo predseda senátu. Vo vzťahu k sudcovi pre prípravné konanie má prokurátor významné návrhové oprávnenie.

Pokiaľ ide o formou rozhodnutia, použitie informačno-technických prostriedkov sa viaže na vydanie príkazu ako formy rozhodnutia, pre ktorú sa v týchto prípadoch stanovujú osobné formálne i obsahové požiadavky. Tieto ale zákonodarca nestanovuje vôbec jednotne a ani dôsledne vzhľadom na prehľad uvedených inštitútov a návrhové oprávnenia prokurátora vo vzťahu k sudcovi pre prípravné konanie.

V prípade ***vyhotovovania obrazových, zvukových, obrazovo-zvukových záznamov*** *(§ 114 TP)*, tu nie sú vôbec riešené náležitosti podávaného návrhu. S cieľom posilnenia zodpovednosti prokurátora za podávaný návrh by ich bolo vhodné formulovať.

Príkaz musí byť písomný a musí byť odôvodnený (hoci inak sa to pri príkazoch nevyžaduje). V príkaze je nutné uviesť aj podozrenie z konkrétnej trestnej činnosti, pre ktoré sa použitie tohto prostriedku nariaďuje. Keďže ako forma rozhodnutia v trestnom konaní, sa príkaz stáva právoplatný a účinný momentom vydania, nie je voči nemu možný opravný prostriedok, práve odôvodnenie tohto príkazu má garantovať preskúmateľnosť tejto formy rozhodnutia. Vždy je potrebné, aby sa v príkaze uviedli aj konkrétne údaje o osobách alebo o veciach, na ktoré sa má záznamová činnosť vzťahovať. Identifikačné údaje o osobách a poznávacie znaky vecí sa uvá-

[6] Čentéš, J. a kol.: Trestný poriadok. Veľký komentár, III. aktualizované vydanie. Bratislava: Eurokódex, 2017, s. 471 a nasl.

dzajú v prípadoch, ak sú známe. Ak by neboli, je ich možné nahradiť aj typickými poznávacími znameniami ako sú jazvy, znamienka, anomálie a pod.

V príkaze sa tiež uvádza čas, na ktorý sa použitie tohto prostriedku nariaďuje. Ani tu nejde o jednorazovú záležitosť, ale o použitie tohto prostriedku dlhodobo, najviac na 6 mesiacov tak, ako to povoľuje trestno-procesná úprava. Aj tu existuje možnosť predĺženia používania tohto prostriedku a to aj opakovane, o ďalšie dva mesiace.

Pri odpočúvaní a zázname telekomunikačnej prevádzky *(§ 115 TP),* v tomto ustanovení 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 (Zákon č. 166/2003 Z. z. v znení neskorších predpisov), 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,[7] 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

[7] Perhács, Z. Perhácsová, A.: Právna úprava používania informačno-technických prostriedkov (2. časť). In Justičná revue č. 5/2013, s. 708

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.

V súvislosti s oznámením údajov o telekomunikačnej prevádzke (§ 116 TP) sa taktiež požaduje povinne písomná a odôvodnená forma príkazu, to ostalo zachované z pôvodnej úpravy § 116 TP. Navyše sa však stanovuje, že príkaz musí obsahovať aj spôsob, rozsah a lehotu na oznámenie požadovaných údajov. Ak sa vzťahuje príkaz na konkrétneho používateľa, potom musí obsahovať aj údaje o jeho totožnosti, ak je známa. Stanovuje sa aj požiadavka, že ak nejde o zistenie a oznámenie údajov o už uskutočnenej telekomunikačnej prevádzke, tak zisťovanie a následne oznamovanie údajov môže najviac trvať 6 mesiacov. V prípravnom konaní, na podklade písomného a odôvodneného návrhu môže toto trvanie sudca pre prípravné konanie aj predĺžiť a to aj opakovane, vždy najviac o 2 mesiace. Maximálna doba použitia tohto prostriedku a ani maximálny počet možných predlžovaní tu však nie sú vôbec riešené. Je tak možné aj smerom do budúcna vydať príkaz na zisťovanie a následne na oznámenie týchto údajov a nie je určený maximálny časový limit a obmedzenie pre takúto aktivitu. Teda počas určitej doby, uvedenej v príkaze, sa budú tieto údaje zisťovať a následne oznamovať. V tomto prípade by sa uvedený prostriedok mal využívať spravodajským spôsobom, keďže len toto dokáže zabezpečiť, že sa jeho použitím získajú informácie dôležité pre trestné konanie.

Vydaný písomný a odôvodnený príkaz sa doručuje podniku, ktorý poskytuje verejné siete alebo služby. Na podklade doručenia príkazu sú podniky povinné v určenej lehote, stanoveným spôsobom a v určenom rozsahu oznámiť požadované údaje.

3. Problematické aspekty príkazu na použitie ITP

V súvislosti s príkazom ako formou rozhodnutia v trestnom konaní treba poukázať na niektoré posledné novelizácie trestných predpisov. Rovnako tak možno poukázať na určitý nesúlad slovenskej procesnej úpravy s európskou obsiahnutou v Dohovore o ochrane ľudských práv a základných slobôd (ďalej len „Dohovor“) a v nadväznosti na to aj na judikatúru ESĽP. Ako sme už naznačili, príkaz predstavuje osobitnú formu rozhodnutia, ktorá sa využíva v prípadoch, kedy to priamo zákon stanovuje. V tomto prípade ide jednak o príkaz, ktorý môže vydávať prokurátor, ako aj sudca pre prípravné konanie a v konečnom dôsledku aj predseda senátu v konaní pred súdom. Ide o formu rozhodnutia, ktorá sa priamo vyhradzuje pre intenzívne zásahy do základných ľudských práv a slobôd a je nutné o tom rozhodnúť v pomerne operatívnej dobe tak, aby sa nezmaril účel tohto úkonu a prípadne aj trestného konania.[8] Na jednej strane sa preto nutne vyžaduje rozhodnutie orgánu činného v trestnom konaní alebo súdu, avšak rozhodnutie v podobe uznesenia by nebolo pre tieto prípady vhodné. Pre príkaz ako formu rozhodnutia je typické, že sa môže vydávať aj ústne, pričom písomná forma sa požaduje len v prípade, ak to zákon priamo stanovuje.

Okrem tohto je pre príkaz typické, že voči nemu nie je možné podať žiadny opravný prostriedok. Ustanovenia Trestného poriadku nijakým spôsobom neriešia doručovanie príkazu v prípade sledovania osôb a vecí, keďže je zrejmé, že je určený len pre subjekty, ktoré žiadajú o jeho vy-

[8] Ivor, J. a kol.: Trestné právo procesné. Druhé, doplnené a prepracované vydanie. Bratislava: Iura Edition, 2010, s. 530.

danie a následne pre tie, ktoré realizujú sledovanie osôb a vecí.[9] Momentom vydania sa príkaz stáva právoplatný a vykonateľný a to bez možnosti podania opravného prostriedku voči nemu. Ak by prokurátor, sudca pre prípravné konanie či predseda senátu na podklade písomnej žiadosti alebo návrhu odmietol vydať príkaz, taktiež voči tomuto rozhodnutiu nie je možné podať žiadny opravné prostriedok a cesta nariadenia použitia tohto prostriedku sa realizuje cestou podania nového návrhu alebo novej písomnej žiadosti. Ani dotknutá osoba výkonom sledovania osôb a vecí nemá právo podávať voči príkazu na použitie tohto prostriedku žiadny opravný prostriedok. Na jednej strane utajený spôsob použitia tohto prostriedku má smerovať k tomu, že dotknuté osoby nevedia, že sa voči nim tento prostriedok vykonáva a na podklade tohto sa získavajú cenné poznatky pre trestné konanie. Takže právna úprava priamo počíta s tým, že o vydaní príkazu dotknutá osoba v čase realizácie inštitútu nemá vedomosť. Aj keby sa nejakým spôsobom predsa len dozvedela, že voči nej bol vydaný takýto príkaz, aj tak voči nemu v tomto čase nemá možnosť využiť žiadny opravný prostriedok, v zásade nemá voči nemu možnosť namietať. Odhliadnuc od tohto, v našej justičnej praxi sa táto forma rozhodnutia v trestnom konaní využíva pomerne často.[10]

Práve tieto skutočnosti, že voči príkazu ako forme rozhodnutia v trestnom konaní, nie je prípustný žiadny opravný prostriedok,[11] sú jedným z ďalších nedostatkov tejto procesnej úpravy. Prirodzene, že každý má s cieľom ochrany svojich ústavných a garantovaných práv možnosť obrátiť na s cieľom dosiahnutia ochrany na Ústavný súd.

Ustanovenie čl. 13 Dohovoru garantuje každému, koho práva a právom chránené slobody boli dotknuté (porušené), právo na účinné právne prostriedky nápravy pred národnými (vnútroštátnymi) orgánmi.[12] Týmto spôsobom sa posilňuje právo každého podávať opravné prostriedky na vnútroštátnej úrovni a to bez ohľadu na to, akú povahu bude mať tento opravný prostriedok. V každom prípade by však národné úpravy mali opravný prostriedok voči príkazu umožňovať. Nie je v rozpore s úpravou práv obsiahnutých v Dohovore, ak vnútroštátne úpravy umožňujú zasiahnuť do nich. Tieto zásahy sa však musia realizovať tak, aby sa vtesnali pod podmienky možných zásahov do garantovaných práv Dohovorom. Vnútroštátne úpravy, tak ako aj naša trestno-procesná úprava umožňuje vykonanie tajného sledovania osôb a vecí na účely získanie dôležitých poznatkov pre trestné konanie (o osobách i veciach), no súčasne by mala zabezpečovať pre dotknuté osoby aj možnosti adekvátne a efektívne sa domáhať ochrany týchto dotknutých práv pred ich prípadným zneužívaním.[13] Rovnako tak aj ÚS SR konštatoval, že akékoľvek očividné zásahy do práva na súkromný život dotknutých osôb, sa nemôžu dostať mimo sféru dosahu bezprostrednej (či už preventívnej alebo následnej) súdnej kontroly a v nasledujúcom odkázal na predošlé rozhodnutie ESĽP.[14] Ak sa teda vnútroštátne orgány nezaoberajú námietkami (žiadosťami či sťažnosťami) dotknutých osôb, že ich práva garantované Dohovorom, boli porušené, už len samotná táto skutočnosť zakladá rozpor s čl. 13 Dohovor a to bez ohľadu na to, či v konečnom dôsledku ESĽP konštatuje porušenie práv garantovaných Dohovorom alebo nie. Pre rozpor s čl. 13 je teda dostačujúce, ak sa dotknuté osoby nemajú právo domáhať ochrany svojich dotknutých práv cestou podania opravného prostriedku voči určitému rozhod-

[9] Záhora, J.: Príkaz v trestnom konaní a možnosti jeho revízie. In Rozhodnutia súdov v trestnom konaní. Zborník príspevkov vydaný v rámci grantového projektu „Revízia rozhodnutí v trestnom konaní". Trnavská univerzita v Trnave, 2014, s. 21.

[10] Šimovček, I.: Revízia rozhodnutí v prípravnom konaní trestnom. In Záhora a kol.: Aktuálne problémy prípravného konania trestného. Leges: Praha, 2003, s. 78.

[11] Záhora, J.: Príkaz v trestnom konaní. In Justičná revue, roč. 56, č. 5/2004, s. 540.

[12] Rozhodnutie ESĽP Case of Boyle and Rice vs. Spojené Kráľovstvo, 1988.

[13] Rozhodnutie ESĽP Case of Camenzind vs. Švajčiarsko, 1997.

[14] I. ÚS 290/2015.

nutiu (v tomto prípade voči príkazu na sledovanie osôb a vecí v trestnom konaní), a takto nemôžu dosiahnuť účinnú a efektívnu ochranu svojich práv.[15] V tejto rovine sa tak trestno-procesná úprava niektorých informačno-technických prostriedkov jednoznačne dostáva do rozporu s čl. 13 Dohovoru a následnou judikatúrou ESĽP týkajúcou sa jeho výkladu. Predmetný rozpor z čl. 13 Dohovoru sa v tomto prípade sa predmetom záujmu pri procesnej úprave dvoch informačno-technických prostriedkov a to pri odpočúvaní a zázname telekomunikačnej prevádzky podľa § 115 TP a pri oznámení údajov o telekomunikačnej prevádzke podľa § 116 TP, ktoré boli s účinnosťou od 1. 1. 2016 novelizované. Okrem iného sa tieto zmeny dotkli práve aj možnosti podávania opravného prostriedku voči príkazu na realizáciu odposluchov a oznamovanie údajov o uskutočnenej prevádzke. Vo vzťahu k nim sa zaviedol nový osobitný spôsob konania a to konanie pred Najvyšším súdom SR, konkrétne v podobe Konania o preskúmanie zákonnosti príkazu na odpočúvanie a záznam telekomunikačnej prevádzky a príkazu na zistenie a oznámenie údajov o telekomunikačnej prevádzke (§ 362f TP). Toto ustanovenie umožňuje každej osobe (uvedenej v § 115 ods. 9 TP alebo § 116 ods. 4 TP) podať návrh na preskúmanie príkazu vydaného na odposluch a na oznámenie údajov o uskutočnenej telekomunikačnej prevádzke.[16] Pred rozhodnutím si vyžiada stanovisko od orgánu, ktorý vydal príkaz na použitie týchto prostriedkov a podľa povahy výsledkov, ktoré zistí vlastným prieskumom následne rozhodne formu uznesenia, voči ktorému nemožno podať opravný prostriedok, o tom, že:

a) príkaz bol vydaný v rozpore so zákonom, alebo že bol vykonaný v rozpore so zákonom a teda že došlo k porušeniu zákona,
b) príkaz bol vydaný a vykonaný v súlade so zákonom a teda nedošlo k porušeniu zákona.

Táto možnosť sa, paradoxne, dotkla len dvoch inštitútov smerujúcich k zaisteniu informácií v trestnom konaní a to odpočúvania a záznamu telekomunikačnej prevádzky, ktorý je prirodzene svojou povahou veľmi intenzívnym zásahom do základných ľudských práv a slobôd a následne aj oznámenia údajov o telekomunikačnej prevádzke, pri ktorom však dochádza k oznámeniu týchto údajov smerom do minulosti a rovnako tak sa dá tento inštitút využiť aj smerom do budúcna (budú sa zisťovať tieto údaje). V uvedenom druhom prípade však ide o prevádzkové údaje o dátumoch hovorov, o vysielajúcej a prijímajúcej linke, o dĺžke resp. o trvaní hovorov a pod. a teda nepochybne ide o menej intenzívny zásah do základných ľudských práv a slobôd dotknutých osôb. A teda viac menej nesystematicky umožnil zákonodarca domáhať sa prieskumu príkazu len v uvedených dvoch prípadoch a zrejme pozabudol na ďalšie zaisťovacie inštitúty, ktoré sa realizujú utajeným spôsobom, na podklade príkazu, voči ktorému nie je prípustné podanie opravného prostriedku. Jednoznačne tak možno odporúčať, na účely odstránenia vyššie uvedeného nesúladu s čl. 13 Dohovoru a následnou judikatúrou ESĽP, aby zákonodarca rozšíril možnosti dosiahnuť preskúmania príkazu v prípadoch, kedy sa na podklade neho realizuje zásah do základných ľudských práv utajeným spôsobom.

4. Využitie ITP v neprocesnej rovine a povoľovací mechanizmus

Použitie informačno-technických prostriedkov tak, ako sme vyššie naznačili ich povoľovací mechanizmus, sa viaže na trestné konanie a teda odvíja sa od procesnej úpravy. V neprocesnej rovi-

[15] Perhács, Z.: O lehota na podanie sťažnosti vo veciach tajného sledovania osôb orgánmi verejnej moci. In Bulletin slovenskej advokácie, č. 10/2013, s. 28.

[16] Tittlová, M.: Kritické zhodnotenie trestnoprávnej úpravy odpočúvania a záznamu telekomunikačnej prevádzky. In Jutičná revue č. 6–7/2016, s. 748 a nasl.

ne je však taktiež možné využitie informačno-technických prostriedkov, konkrétne na podklade vyššie uvedeného Zákona o ochrane súkromia pred odpočúvaním.

Ustanovenie § 2 ods. 1 Zákona o ochrane pred odpočúvaním priamo vymedzuje pojem „informačno-technické prostriedky" na účely tohto zákona. Ide však len o výpočet exemplifikatívny s ohľadom na „*najmä*" v úvode definície, hoci ide o veľmi podobnú definíciu, ako je obsiahnutá v § 10 ods. 21 TP. Konštatuje, že ide o *najmä (elektrotechnické, rádiotechnické, fototechnické, optické, mechanické, chemické a iné prostriedky a zariadenia alebo ich súbory používané utajeným spôsobom s cieľom:*

a) vyhľadávania, otvárania, skúmania a vyhodnocovania poštových zásielok a iných dopravovaných zásielok
b) získavania obsahu správ prenášaných prostredníctvom elektronických komunikačných sietí vrátane odpočúvania telefónnej komunikácie,
c) vyhotovovanie obrazových, zvukových, obrazovo-zvukových alebo iných záznamov.

Informačno-technické prostriedky podľa tohto zákona môže využiť pomerne široké spektrum štátnych orgánov. Zákonodarca tu stanovuje možnosti využitia na konkrétny účel okruhom oprávnených štátnych orgánov, ku ktorým sa zaraďuje:

a) Policajný zbor SR,
b) Slovenská informačná služba,
c) Vojenské spravodajstvo,
d) Zbor väzenskej a justičnej stráže a
e) Colná správa (resp. Finančná správa).

Možnosť využitia informačno-technických prostriedkov podľa tohto zákona je z pohľadu týchto štátnych orgánov limitovaná rozsahom ich pôsobnosti, ktorú upravujú osobitné predpisy. Takto sa pozitívne vymedzuje okruh subjektov oprávnených na využívanie týchto inštitútov (§ 2 ods. 1 Zákona o ochrane pred odpočúvaním). Negatívne vymedzenie nachádzame v § 2 ods. 7 tohto zákona, ktorý konštatuje, že orgány územnej samosprávy, ani súkromné bezpečnostné služby a ani iné fyzické či právnické osoby nemôžu mať v držbe a ani používať informačno-technické prostriedky.

Použitie informačno-technických prostriedkov neprocesne podľa tohto ustanovenia je možné len na s ohľadom na konkrétny, taxatívne formulovaný účel. To, že použitie takýchto inštitútov na vymedzené účely je nevyhnuté, to je potrebné posudzovať v kontexte konkrétnej situácie tak, ako použitie nutné, nutne potrebné. Použitie informačno-technických prostriedkov podľa tohto zákona je možné len v prípade, ak dosiahnutie tohto účelu inak by bolo neúčinné alebo podstatne sťažené a súčasne, ak je to v demokratickej spoločnosti nevyhnuté z dôvodu:

a) zabezpečenia ochrany ústavného zriadenia,
b) zabezpečenia vnútorného poriadku a zahraničnopolitických záujmov štátu,
c) zaistenia bezpečnosti a obrany štátu,
d) získavania informácií zo zahraničných zdrojov,
e) predchádzania a objasňovania trestnej činnosti alebo
f) ochrany práv a slobôd iných

Použitie informačno-technických prostriedkov je podľa Zákona o ochrane pred odpočúvaním možné výhradne na stanovený účel a po splnení požiadavky subsidiarity využívať primárne na území Slovenskej republiky. Takto majú možnosť využívať informačno-technické prostriedky Policajný zbor, Zbor väzenskej a justičnej stráže, orgány Colnej správy, Slovenská informačná služba a Vojenské spravodajstvo. V prípade Slovenskej informačnej služby a Vojenského spravodajstva sa povoľuje, aby tieto subjekty využívali informačno-technické prostriedky aj mimo nášho územia, a to v rozsahu úloh, ktoré majú podľa ich zákonnej úpravy plniť.

Použitie je navyše možné výhradne na základe *súhlasu zákonného sudcu.* Je to odraz zásady judiciarity, v zmysle ktorej o tých najzávažnejších zásahoch do garantovaných práv môže rozhodovať výhradne súdu. Ide o princíp súdnej kontroly využívania takto ofenzívnych a do základných ľudských práv zasahujúcich inštitútov. Zabezpečuje sa súdny (nestranný a nezávislý) prieskum návrhu príslušného orgánu, ktorý má podľa Zákona o ochrane pred odpočúvaním možnosť používať informačno-technické prostriedky. Tento súhlas zákonného sudcu musí byť:

a) vydaný vopred, teda pred reálnym použitím inštitútu,

b) písomný so zákonom predpokladanými minimálnymi náležitosťami.

V súvislosti s obsahovými náležitosťami súhlasu je zákonodarca pomerne stručný, keď v § 4 ods. 1 povinne požaduje, aby v súhlase bol uvedený:

a) čas, počas ktorého sa konkrétny prostriedok môže používať resp. počas ktorého sa daný prostriedok môže využívať,

b) súhlas s použitím v miestach a priestoroch, ktoré nie sú verejne dostupné.

Je zrejmé, že súhlas zákonného sudcu a jeho obsahové spracovanie nadväzuje na obsahové vymedzenie žiadosti oprávneného orgánu na použitie tohto-ktorého inštitútu. Tieto náležitosti prirodzene determinujú vydanie súhlasu zákonného sudcu.

Ad a) V súhlase na použitie konkrétneho prostriedku musí byť povinne uvedený čas, resp. doba, počas ktorej sa tento prostriedok bude používať. Je zrejmé, že použitie takých prostriedkov nie je činnosťou jednorazovou. Je to činnosť, ktoré je realizovaná počas určitej doby, spravidla dlhodobejšie alebo dlhodobo. Limitujúcim faktorom je, že používanie konkrétneho prostriedku je možné odsúhlasiť len na čas, ktorý je nevyhnutný na dosiahnutie účelu. Zákonodarca limituje použitie každého z informačno-technických prostriedkov podľa tohto zákona, maximálnou dobou šiestich mesiacov. V súhlase musí byť uvedený konkrétny čas, resp. doba, počas ktorej je možné konkrétny inštitút používať, najviac však 6 mesiacov od udelenia súhlasu. Lehota platnosti vydaného súhlasu začína plynúť už dňom, kedy sa súhlas udelil. Odo dňa vydania súhlasu začína plynúť v súhlase uvedená lehota na použitie konkrétneho prostriedku.[17] Ak sa aj povoľuje použitie viacerých informačno-technických prostriedkov jedným súhlasom zákonného sudcu (a na podklade návrhu oprávneného orgánu), je potrebné v súhlase výslovne vymedziť rozsah, v ktorom sa môže použiť každý z nich.

Ad b) Použitie inštitútov podľa ustanovení Zákona o ochrane pred odpočúvaním sa môže vzťahovať na priestory, ktoré sú verejne dostupné, teda sú prístupné širokému okruhu subjektov. Rovnako je však možné tieto prostriedky využiť v priestoroch, ktoré verejne prístupné nie sú, teda v priestoroch súkromných, do ktorých môžu vstupovať len určité osoby na základe svojich subjektívnych práv a oprávnení. Ak sa majú konkrétne informačno-technické prostriedky v priestoroch, ktoré verejne prístupné nie sú, táto skutočnosť musí priamo a výslovne uvedená v súhlase zákonného sudcu na použitie konkrétneho inštitútu.

V súhlase sa uvádza konkrétna doba použitia inštitútu. Maximálne môže byť súhlas udelený na 6 mesiacov, avšak s možnosťou predĺženia platnosti pôvodného súhlasu na základe novej žiadosti oprávneného štátneho orgánu (§ 4 ods. 2). Ak sú sústavne splnené podmienky nutnosti, účelnosti, subsidiarity, je možné predĺžiť používanie inštitútu (predĺžiť dobu jeho použitia uvedenú v pôvodnom súhlase) na základe novej žiadosti zákonnému sudcovi. Najviac možno predĺžiť túto dobu o 6 mesiacov a to aj opakovane. Súhlas, resp. súhlas s predĺžením používania inštitútu musí byť udelený najneskôr v posledný deň pôvodnej doby použitia uvedenej v pôvodnom súhlase.

[17] Tittlová, M.: Zákon o ochrane súkromia pred odpočúvaním. Komentár. Bratislava: Wolters Kluwer, 2017, s. 31 a nasl.

Súhlas na použitie informačno-technických prostriedkov podľa Zákona o ochrane pred odpočúvaním, sa vydáva na základe písomnej žiadosti oprávneného štátneho orgánu. Ide o žiadosť, ktorá musí byť povinne písomná, musí byť podaná vecne a miestne príslušnému súdu a navyše, ustanovenie § 4 ods. 3 vyžaduje, aby žiadosť mala aj konkrétne obsahové náležitosti:

a) údaje týkajúce sa druhu používaného prostriedku, miesta a času použitia, údaje týkajúce sa dotknutých osôb:
   – konkrétny druh informačno-technického prostriedku
   – miesto použitia prostriedku, ak to umožňuje povaha veci, vrátane skutočnosti, či sa vyžaduje použitie inštitútu len na verejných priestranstvách, alebo aj na takých, ktoré nie sú verejnosti dostupné,
   – navrhovaný čas použitia (najviac na 6 mesiacov),
   – údaje o osobe, voči ktorej sa má konkrétny prostriedok použiť
b) informácie o predchádzajúcom neúčinnom alebo podstatne sťaženom odhaľovaní a dokumentovaní činnosti, pre ktorú sa podáva žiadosť, ktoré preukazujú naplnenie požiadavky nevyhnutnosti použitia takto intenzívnych zásahov a súčasne, ktoré preukazujú splnenie požiadavky subsidiarity ich použitia (ak nemožno účel dosiahnuť inak alebo by bolo jeho dosahovanie podstatne sťažené
c) dôvody použitia, ktoré sa opierajú o konkrétny účel využitia v § 2 Zákona o ochrane pred odpočúvaním.

Možnosť použitia informačno-technických prostriedkov podľa Zákona o ochrane pred odporúčaním sa zakladá na rozhodnutí súdu, ktoré má povahu súhlasu. Ustanovenie čl. 13 Európskeho dohovoru uvádza, že každý, koho práva a slobody priznané týmto Európskym dohovorom boli porušené, má právo na účinný opravný prostriedok pred vnútroštátnym orgánom bez ohľadu na to, že porušenie spôsobili osoby pri plnení ich úradných povinností. Je tak vidieť, že nepripustenie opravného prostriedku (bez ohľadu na jeho označenie, druh a povahu) zakladá rozpor s predmetným ustanovením Dohovoru. Na uvedené problémy reagoval aj ESĽP vo svojom rozhodnutí Camenzind proti Švajčiarsku (1997), keď uviedol, že ak vnútroštátne úpravy umožňujú vykonanie tajného sledovania osôb a vecí z dôvodu získania dôležitých poznatkov (o osobách aj veciach), súčasne musia zabezpečovať pre dotknuté osoby aj možnosti adekvátne a efektívne sa domáhať ochrany týchto dotknutých práv pred ich prípadným zneužívaním.

Záver

Požiadavky na zefektívnenie procesu odhaľovania a dokazovania závažnej trestnej činnosti vedú cestou využívania moderných, no ofenzívnych a do garantovaných práv v určitej miere zasahujúcich inštitútov. K nim popri prostriedkoch operatívno-pátracej činnosti možno zaradiť práve informačno-technické prostriedky a to tak v ich procesnej, ako aj v neprocesnej rovine ich použitia. V tej neprocesnej predstavujú nástroj smerujúci k odhaľovaniu latentnej časti kriminality a sú súčasťou širšej stratégie boja s trestnou činnosťou resp. kontroly kriminality. V rovine procesnej sú typické pre trestné konania (teda smerujú k preverovaniu konkrétnych podozrení z trestnej činnosti) v rôznych častiach a štádiách, v závislosti od čoho sa diferencujú podmienky a pravidlá nariaďovania používania takýchto prostriedkov.

Na jednej strane ide o prostriedky, bez ktorých si odhaľovanie a dokazovanie mnohých trestných činov len ťažko možno predstaviť, na strane druhej sú to prostriedky, pri ktorých je nutné obetovať záujem na ochrane garantovaných práv v prospech záujmu štátu na ochrane celej koncepcie ľudských práv, pilierov právneho a demokratického štátu. Prirodzene, že vždy by malo ísť

o také zásahy, ktoré prejdú na tieto účely testom proporcionality, lebo konkrétna miera zásahu do garantovaných práv, konkrétny rozsah obetovaných práv a právom chránených záujmov jednotlivcov (do práv ktorých sa zasahuje), je len ťažko možno vymedziť.

Ak aj právne úpravy obsahujú takéto a im podobné inštitúty tzv. tajného dohľadu nad jednotlivcami a ich činnosťou, je nutné, aby súčasne obsahovali vhodné, primerané, dostačujúce záruky ich ochrany, nezneužívania, využívania len v odôvodnených prípadoch. Ich systém je obsiahnutý aj v slovenskej procesnej a neprocesnej úprave, hoci zákonodarca v tomto smere nie je u nás celkom jednotný a exaktný. Na jednej strane povoľuje využitie informačno-technických prostriedkov v rámci takmer celého trestného konania, čomu prispôsobuje povoľovací mechanizmus (subjekt rozhodujúci o povolení použitia formou vydania príkazu). Na strane druhej požaduje v predsúdnom konaní návrh smerujúci k sudcovi pre prípravné konanie na vydanie príkazu, hoci jeho náležitosti v procesnej rovine takmer vôbec neformuluje. Zavedenie povinnej judiciarity je síce pozitívnym aspektom, teda rozhodovanie o použití informačno-technických prostriedkov neostáva výhradne na úrovni orgánov činných v trestnom konaní (ale požaduje sa príkaz vydaný sudcom), no na strane druhej viaceré aspekty tohto postupu nie sú v procesnej rovine dôsledne upravené. Popri absencii formálnych a obsahových náležitostí návrhu, neformuluje zákonodarca ani následný postup vo vzťahu k podanému návrhu, teda postup v prípade jeho neúplnosti. Práve takýto systém záruk vydania príkazu resp. súhlasu s použitím informačno-technických prostriedkov (na podklade žiadosti) je možné vidieť v neprocesnej línii úpravy informačno-technických prostriedkov v Zákone o ochrane súkromia pred odpočúvaním. Okrem toho, že možno upozorniť na tento nesúlad, možno jednoznačne odporúčať inšpiráciu procesnej roviny úpravy práve touto neprocesnou úpravou. Jej spresnenie je prostriedkom na podporu a posilnenie zodpovednosti prokurátorov za podávané návrhy na vydanie príkazu na použitie informačno-technických prostriedkov v trestnom konaní a súčasne jednou zo záruky ochrany garantovaných práv.

Samostatnou otázkou je príkaz ako forma rozhodnutia v trestnom konaní. Síce v rovine procesnej zákonodarca stanovuje, že príkaz musí byť písomný a odôvodnený (v rozsahu špecificky podľa informačno-technického prostriedku), problematickou ostáva možnosť dosiahnutia jeho preskúmania. Žiadny zrejmý zásah do garantovaných práv (osobitne do práva na súkromie) nemôže byť vyňatý z pod súdnej preskúmateľnosti. Prirodzene, v postupe ochrany základných ľudských práv je vždy možné obrátiť sa s požiadavkou na Ústavný súd. V rámci trestného konania však absentujú takmer úplne postupy, ktoré by umožnili preskúmať vydaný príkaz. Novelizáciou sa síce umožnilo v osobitnom konaní pred Najvyšším súdom SR dosiahnuť preskúmanie príkazu, ale len vo vzťahu k použitiu inštitútov podľa § 115 TP a § 116 TP. Z možnosti preskúmania je vyňatý resp. takáto možnosť ani nebola zavedená, inštitút podľa § 114 TP a súčasne aj rad prostriedkov operatívno-pátracej činnosti, kde možno predpokladať podstatne intenzívnejší zásah do garantovaných práv ako v prípade postupov podľa § 116 TP. Aj to je smerom do budúcna jedna z dôležitých úloh a súčasne úvaha smerom do budúcna, akým spôsobom v týchto otázkach podporiť garancie práv a právom chránených záujmov dotknutých osôb.

Literatúra

Čentéš, J. a kol.: Trestný poriadok. Veľký komentár, III. aktualizované vydanie. Bratislava: Eurokódex, 2017.

Ivor, J., Polák, P., Záhora, J.: Trestné právo procesné. II. časť. Bratislava: Wolters Kluwer, 2017.

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 Justičná revue č. 5/2013.

Perhács, Z.: O lehota na podanie sťažnosti vo veciach tajného sledovania osôb orgánmi verejnej moci. In Bulletin slovenskej advokácie, č. 10/2013.

Šimovček, I.: Revízia rozhodnutí v prípravnom konaní trestnom. In Záhora a kol.: Aktuálne problémy prípravného konania trestného. Leges: Praha, 2003.

Tittlová, M.: Zákon o ochrane súkromia pred odpočúvaním. Komentár. Bratislava: Wolters Kluwer, 2017.

Tittlová, M.: Kritické zhodnotenie trestnoprávnej úpravy odpočúvania a záznamu telekomunikačnej prevádzky. In Justičná revue č. 6–7/2016.

Tittlová, M.: Korupcia. Vybrané kriminologické a trestnoprávne aspekty. Bratislava: Wolters Kluwer, 2015.

Záhora, J. a kol.: Obrazové a zvukové záznamy v trestnom konaní. Bratislava: Wolters Kluwer, 2018.

Záhora, J.: Príkaz v trestnom konaní a možnosti jeho revízie. In Rozhodnutia súdov v trestnom konaní. Zborník príspevkov vydaný v rámci grantového projektu „Revízia rozhodnutí v trestnom konaní". Trnavská univerzita v Trnave, 2014.

Záhora, J.: Príkaz v trestnom konaní. In Justičná revue, roč. 56, č. 5/2004.

Európsky Dohovor o ochrane základných ľudských práv a slobôd.

Rozhodnutie ESĽP Case of Boyle and Rice vs. Spojené Kráľovstvo, 1988.

Rozhodnutie ESĽP Case of Camenzind vs. Švajčiarsko, 1997.

I. ÚS 290/2015.

Trestný poriadok, zákon č. 301/2005 Z. z. v znení neskorších predpisov.

Zákon č. 166/2003 Z. z. o ochrane súkromia pred odpočúvaním v znení neskorších právnych predpisov.

Trestnoprávne prostriedky boja proti kybernetickým hrozbám[1]

Criminal Means against Cyber Threats

Jozef Medelský[2]

***Abstrakt**: Štúdia je zameraná na definíciu bezpečnosti s poukázaním na nevojenské hrozby. Jadrom štúdie je analýza informačných hrozieb, konkrétne autor poukazuje na 3D kreslenú detskú pornografiu, vybrané sociálne siete a darkweb. Predstavené hrozby sú analyzované v kontexte protiprávnej činnosti, na ktoré sú využívané. Záverom autor poukazuje na trestnoprocesné inštitúty, ktoré sú vhodným nástrojom v boji proti týmto informačným hrozbám.*

***Abstract**: Presented study is aimed at defining security with reference to non-military threats. The core of the study is the analysis of information threats, namely the author points to 3d cartoon child pornography, selected social networks and darkweb. The threats presented are analyzed in the context of the illegal activity for which they are used. In conclusion, the author points to criminal-procedural institutes, which are a suitable tool in the fight against these information threats.*

***Kľúčové slová**: bezpečnosť, vojenské hrozby, nevojenské hrozby, informačné hrozby, darkweb, sociálne siete, informačno-technické prostriedky, prostriedky operatívno-patracej činnosti, analýza, zhodnotenie, závery.*

***Keywords**: security, military threats, non-military threats, information threats, darkweb, social networks, information technology, means of operative-action, analysis, evaluation, conclusions.*

1. Bezpečnosť a bezpečnostné hrozby

Bezpečnosť je jedným zo základných pojmov, ktoré rezonujú tak na národnej, ako aj medzinárodnej úrovni. Tak ako sa vyvíjajú mnohé právne inštitúty, vyvíja sa aj pojem bezpečnosť, predovšetkým sa objavujú nové bezpečnostné hrozby, na ktoré je potrebné efektívne odpovedať. Bezpečnosť je podstatným elementom fungovania štátov, ako aj medzinárodného spoločenstva. Prvoradým záujmom každého štátu je zaručiť bezpečnosť svojho obyvateľstva pred hrozbami vnútornými, ako aj vonkajšími a zároveň pred hrozbami vojenskými a nevojenskými. Pojem bezpečnosť je možné chápať ako istotu, ochranu, zabezpečenie. Prídavné meno bezpečný sa vysvetľuje v troch významoch. V prvom prípade ako poskytujúci ochranu pred nebezpečenstvom, po druhé ako nepociťovanie ohrozenia a po tretie ako nepochybný, určitý, istý.[3] Bezpečnosť sa vo všeobecnosti, v slovníkoch a encyklopédiách, spája najmä so stabilitou, určitosťou, poriadkom, spoľahlivosťou, rovnovážnosťou, existenciou subjektu bez hrozieb, stavom a pocitom istoty.[4]

Dôležitým pojmom pre potreby štúdie je pojem bezpečnostná hrozba. Bezpečnostné hrozby: „Sú to udalosti, javy a procesy spravidla súhrnného (viacstranného charakteru), ktoré pôsobia relatívne dlhodobo a môžu negatívne vplývať na sociálne subjekty, najmä na ich moc a bohatstvo, destabilizovať ich, spôsobiť im škody a pod. Dotýkajú sa najmä fungovania štátu a jeho inštitúcií a organizácií, predovšetkým v politickej a hospodárskej oblasti, života a činnosti veľkých

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

[2] Doc. PhDr. JUDr. Mgr. Jozef Medelský, PhD., Akadémia Policajného zboru v Bratislave, Katedra verejnoprávnych vied, Sklabinská 1, 835 17 Bratislava, e-mail: Jozef.Medelsky@minv.sk.

[3] ĎORULA, J. a kol. 2003. *Krátky slovník slovenského jazyka*. Bratislava: Veda, 2003, s. 64.

[4] ŠKVRNDA, F., PAWERA, R., WEISS, P. 2008. *Medzinárodná bezpečnosť*. Bratislava: Ekonóm, 2008. s. 18.

skupín obyvateľstva (najmä etnických a náboženských), ale aj života, zdravia a majetku jeho občanov. V súvislosti s rozširujúcim sa pohľadom na bezpečnosť sa rozširuje počet a podoby bezpečnostných hrozieb, ale aj rozsah ich pôsobenia predovšetkým v sociálnej a kultúrnej oblasti životného prostredia."[5] Významné delenie je prioritne na hrozby vojenské a nevojenské. V prípade vojenských hrozieb je pravdepodobné, že tieto hrozby sa zmenia na ozbrojený konfliktu. Škvrnda zaraďuje k vojenským hrozbám:

a) regionálne konflikty,
b) proliferácia zbraní hromadného ničenia.

Existencia regionálnych konfliktov je prioritne v skutočnosti, že tieto môžu prerásť do konfliktov celosvetových. Súčasné záväzky v rámci bezpečnostných organizácií umožňujú realizáciu kolektívnej sebaobrany. To v konečnom dôsledku znamená, že ohrozenie jedného z aktérov regionálneho konfliktu môže v konečnom dôsledku viesť k ohrozeniu členských štátov bezpečnostno-vojenskej organizácie.

Šírenie zbraní hromadného ničenia je v zmysle medzinárodného práva verejného zakázané. Napriek tejto skutočnosti sa objavujú subjekty (štáty), ktoré tento druh zbraní vyrábajú, ako aj rozširujú a ponúkajú na vývoz. Otázne je v konečnom dôsledku: Keď dochádza k takémuto konaniu, ktoré je v rozpore s medzinárodným právom, prečo nie sú prijaté adekvátne opatrenia zo strany existujúcich a právne podložených inštitútov, ako napríklad Bezpečnostná rada OSN a jej kapitola VII, ktorá predstavuje mechanizmus kolektívnej bezpečnosti. Iba ak sa na výrobe a rozširovaní podieľali priamo subjekty, ktoré majú priamy vplyv v tomto kolektívnom orgáne.

Nevojenské hrozby. V tomto prípade Škvrnda rozlišuje štyri základné oblasti:

a) sociálno-ekonomické problémy,
b) sociálno-demografické problémy,
c) zlé vládnutie,
d) environmentálne problémy.

V prvom prípade ide o negatívne procesy v štáte, ktoré smerujú k úpadku. Priamy vplyv majú chudoba, hlad, nezamestnanosť a podobne.

V druhom prípade sú to demografické zmeny. V rámci tohto fenoménu dominujú negatívne procesy ako:

a) narušenie demografického vývoja v dôsledku nízkeho prírastku obyvateľstva,
b) negatívny zdravotný stav obyvateľstva – existencia civilizačných chorôb, epidémií a podobne,
c) neprimeraná migrácia, pričom dochádza k nárastu ekonomických migrantov.

V treťom prípade zlé vládnutie predstavuje neschopnosť štátu garantovať vnútornú bezpečnosť. Impulzom je predovšetkým vysoká miera korupcie a klientelizmu. Nefunkčnosť bezpečnostného systému, ktorý nie je schopný zaručiť vnútornú bezpečnosť. Napokon to je neporiadok a chaos, ktoré sa prejavujú v narastajúcej kriminalite a násilí.

Vo štvrtom prípade to je oblasť životného prostredia, pričom narastá tendencia poškodzovania životného prostredia človekom, čo sa v konečnom dôsledku prejavuje v narastajúcich živelných pohromách a katastrofách.

Bez pochýb v súčasnosti je jednou z najzávažnejších bezpečnostných hrozieb kybernetická, resp. informačná hrozba, ktorá by bola v zmysle predstavenej teórie zahrnutá k nevojenským hrozbám. Informácia je v súčasností dominantným elementom vnútroštátnych ale aj medzinárodných vzťahov. V poslednej dekáde sa objavujú vnútroštátne ale aj medzinárodné dokumenty, ktoré hľadajú efektívne nástroje v boji proti kybernetickým útokom, či iným negatívnym využí-

[5] ŠKVRNDA, F., PAWERA, R., WEISS, P. 2008. *Medzinárodná bezpečnosť.* Bratislava: Ekonóm, 2008. s. 29 – 30.

vaním informačný prostriedkov s cieľom poškodiť fyzické, právnické osoby, či štáty ako celky. Informačné hrozby môžu mať rôzne podoby. Ich využívanie má fatálne následky pre jednotlivcov, zoskupenia, či štáty, ktoré sú dominantný subjektom Medzinárodného práva verejného.

2. Informačná bezpečnosť

Ako už bolo načrtnuté, informačné hrozby môžu mať rôzne podoby. Ich cieľom je zasiahnuť konkrétny subjekt a spôsobiť mu ujmu. Informačné hrozby by bolo možné rozdeliť do viacerých skupín. Konkrétne:

a) Detská kreslená pornografia, resp. 3D detská kreslená pornografia,
b) Whatsapp ako bezpečnostná hrozba,
c) Darkweb.

Bez pochýb v súčasnom digitálnom svete sa objavuje väčšie množstvo kybernetických hrozieb, ktoré maj negatívny vplyv na subjekty. Vybrané boli tri oblasti, proti ktorým je nevyhnutné bojovať efektívnymi nástrojmi a najmä efektívnou spoluprácou bezpečnostných orgánov na vnútroštátnej ale aj medzinárodnej úrovni.

Detská kreslená pornografia, resp. 3D detská kreslená pornografia – detská pornografia ako taká je negatívnym fenoménom, ktorý je prísne sankcionovaný v mnohých krajinách sveta. Jednotlivé štáty, ako aj medzinárodné organizácie sa usilujú o odhaľovanie detskej pornografie, bojujú proti jej šíreniu cez internet. Známe sú aj prípady agentúry Európskej únie – Europolu, kde sa jej podarilo rozbiť mnohé skupiny, ktoré sa zaoberali výrobou a distribúciou detskej pornografie. Známou bola operácia Europolu s názvom RESCUE. Predmetnou oblasťou trestnej činnosti bolo odhalenie celosvetovej siete páchateľov sexuálnych trestných činov na deťoch. Operácia bola vykonávaná na územiach: Austrálie, Belgicka, Grécka, Holandska, Islandu, Kanady, Nemecka, Nového Zélandu, Talianska, Poľska, Rumunska, Spojeného kráľovstva, Španielska a Spojených štátov.

Pokiaľ ide o skutkový stav, tak operácia trvala tri roky s podporou a koordináciou vyšetrovaní zo strany Europolu v poslednom 1,5 roku. Orgány presadzovania práva zo 14 krajín sa spojili s cieľom sledovať páchateľov v skutočne globálnom meradle. V niektorých ďalších krajinách, aj keď nie sú uvedené, ešte stále prebiehajú vyšetrovania, v rámci ktorých boli odhalené podozrivé osoby. Podozriví páchatelia sexuálnych trestných činov na deťoch boli členmi online fóra – boylover.net, ktoré propagovalo sexuálne vzťahy medzi dospelými a mladými chlapcami. Webová stránka prevádzkovaná zo servera so sídlom v Holandsku sa na svojom vrchole chválila až 70 000 členmi po celom svete. Webová stránka je zrušená. Pokúšala sa pôsobiť ako fórum „len na diskusie", kde si ľudia mohli vymieňať informácie o svojom sexuálnom záujme o mladých chlapcov bez toho, aby sa dopustili konkrétneho trestného činu, a tak pôsobila „mimo radaru" pozornosti polície. Po registrácii na stránku sa niektorí členovia mohli dostať na súkromnejšie kanály, ako sú[napr. e-maily, na účely zdieľania a prezerania nelegálnych obrázkov a filmov so zneužívanými deťmi. Počítače, zabavené zatknutým osobám, obsahovali zbierky obrovského množstva obrázkov a videonahrávok s obsahom zneužívania detí. Na začiatku vyšetrovania internetové tímy polície Spojeného kráľovstva a austrálskej polície identifikovali členov stránky boylover.net, ktorý predstavoval podľa hodnotenia najväčšie riziko pre deti. Sledovali tiež presun páchateľov na iné stránky, kde pokračovali ďalšie vyšetrovania a posudzovania rizík. Europol sa podieľal na identifikácii členov siete zameranej na sexuálne zneužívanie detí. Významná bola práca analytikov Europolu, ktorí prelomili prvky zabezpečenia hlavného počítačového servera v centre siete, čím sa odkryla identita a aktivita podozrivých páchateľov sexuálnych

trestných činov na deťoch. Europol následne vypracoval viac než 4 000 spravodajských správ pre policajné orgány vo viac než 30 krajinách v Európe a inde, čo viedlo k zatknutiu podozrivých osôb a ochrane detí. Výsledkom tejto operácie bolo: 779 podozrivých je už identifikovaných po celom svete; 250 zatknutí; 252 deťom bola poskytnutá ochrana. Počet obetí, ktorým bola poskytnutá ochrana, je vôbec najvyšší, aký sa dosiahol na základe tohto typu vyšetrovania, pričom vyšetrovania stále pokračujú.[6] Europol je významnou inštitúciou v boji proti detskej pornografii, čo dokazuje aj samotná analýza prípadu Rescue.

V súčasnosti sa však na internete objavujú aj nové formy tejto protiprávnej činnosti. Konkrétne to je kreslené, resp. 3D kreslené zobrazenie detskej pornografie. Jedná sa o obrázky, ktoré sú dostupné na internete, pričom odhaliť zhotoviteľa takejto kresby, ktorá zobrazuje súlož medzi deťmi, resp. súlož dospelých s deťmi, je takmer nemožné. V prípade slovenskej legislatívy je otázne či takéto kreslené zhotovenie napodobňujúce súlož je možné považovať za naplnenie skutkovej podstaty trestného činu výroby detskej pornografie v zmysle § 368 Trestného zákona. Komentár k TZ k výrobe dodáva: „Výrobou sa rozumie nie len priemyselná alebo remeselná výroba, ale aj akékoľvek zhotovovanie detskej pornografie v podobe filmov, fotografií, tlače, atď. Fotografovanie alebo filmovanie nahého detského tela pri kúpaní, na reklamné účely, ako umelecké dielo, nie je pornografiou. Pri obrazovej pornografii ide o zobrazenie dieťaťa pri skutočnej alebo simulovanej sexuálnej činnosti alebo vystavovanie pohlavných orgánov pre sexuálne ukájanie užívateľov. Zvuková pornografia využíva skutočný alebo simulovaný detský hlas za účelom sexuálneho uspokojenia užívateľa."[7] Pre naplnenie skutkovej podstaty trestného činu výroby detskej pornografie sa v zmysel úvodného ustanovenia § 368 ods. 1 vyžaduje: využitie, získanie, ponúknutie alebo iné zneužitie dieťaťa na výrobu detskej pornografie alebo detského pornografického predstavenia.[8] Z definície skutkovej podstaty je možné vyvodiť záver, že výroba 3D kresby, kde nie je dieťa prítomné, nie je možné považovať za výrobu detskej pornografie. Bez pochýb však bude naplnená skutková podstata trestného činu Rozširovania detskej pornografie (§ 369) a Prechovávania detskej pornografie (§ 370), ak dôjde k distribúcii takýchto 3D kresieb, resp. ich prechovávaniu na nosičoch. 3D detská pornografia predstavuje súlož detí, pričom často sú zobrazované populárne detské postavy z animovaných filmov a seriálov. Tieto zobrazenia sú pomerne novodobým fenoménom, ktorý je prítomný na internete. Je nevyhnutné, aby kompetentné orgány efektívne bojovali proti takejto výrobe, ako aj distribúcii detskej pornografie.

Whatsapp ako bezpečnostná hrozba. Whatsapp je v súčasnosti už bežným komunikačným prostriedkom, ktorý spája milióny ľudí po celom svete. Tento komunikačný prostriedok je však využívaný aj k páchaniu závažnej trestnej činnosti. V prvom prípade je potrebné spomenúť rôzne protesty po celom svete, kde sa ľudia mobilizujú prostredníctvom komunikácie na Whatsappe. Ako príklad je možné spomenúť hnutie „Žltých viest", ktoré začalo svoje pôsobenie na území Francúzska. Prostredníctvom Whatsappu sa dokázali zmobilizovať tisíce ľudí, ktorí zadefinovali konkrétne požiadavky a ktorí sa zišli na obrovských protestoch, ktoré nemali vždy pokojný charakter. Práve naopak. Zaznamenané sú mnohé protiprávne konania, kde musela polícia tvrdo zasahovať. Je taktiež potrebné zdôrazniť, že ľudia sa vedia cez Whatsapp veľmi rýchlo zmobilizovať, na čo nedokáže polícia adekvátne odpovedať, ani po personálnej, ani po technickej stránke. V tomto prípade je nevyhnutné prijať efektívne opatrenia, aby bezpečnostné zložky dokázali efektívne, relevantne a v krátkom čase reagovať na takúto mobilizáciu nespokojných demonštrantov.

[6] Pozri bližšie: https://www.europol.europa.eu/activities-services/europol-in-action/operations/operation-rescue.

[7] BURDA, E., ČENTÉŠ, J., KOLESÁR, J., ZÁHORA, J. a kolektív. 2011. *Trestný zákon. Osobitná časť. Komentár. II. diel.* 1. vydanie. Praha: C. H. Beck, 2011. s. 1260.

[8] Pozri bližšie: § 368 ods. 1 TZ.

Ešte závažnejším je však prípad, kde sa obyvatelia určitých komunít prostredníctvom Whatsappu mobilizujú k protiprávnej činnosti. Ako príklad je možné uviesť prípady zaznamenané v Indii. Whatsapp bol nútený vytvoriť vnútorný odbor proti „hoaxom", ktoré sa šíria prostredníctvom tejto siete. Zaznamenaných je niekoľko desiatok násilných úmrtí v dôsledku „hoaxov", ktoré sa šírili cez Whatsapp. Tieto prípady začínajú zverejnením správy v určitej komunite (mesto, obec), kde je v skupine niekoľko stoviek, tisícov používateľov. V dôsledku násilnosti prioritne voči deťom, ktoré sú zaznamenané v Indii, postačuje, že jedna osoba napíše správu, že videla auto s niekoľkými osobami, ktoré je podozrivé, a ktoré sa pravdepodobne usiluje o únos detí. Bez overenia akýchkoľvek informácií, bez kontaktovania bezpečnostných zložiek je pri danom vozidle do pár minút niekoľko desiatok, až stoviek ľudí, ktoré auto zdemolujú a osoby vo vozidle násilne usmrtia. Takýchto prípadov je zaznamenaných okolo 30 (len za rok 2017), kedy došlo k násilnému usmrteniu nevinných ľudí na základe jednej správy na Whatsappe. Otázne teda je ako postupovať v takýchto prípadoch? Je možné takýmto konaniam predchádzať a ochrániť tak ľudský život pred davom ľudí, ktorí konajú na základe domnienky, podozrenia. Aj v tomto prípade je potrebné vytvoriť efektívny systém, ktorý umožní zabrániť podobným tragédiám. Nevyhnutná je spolupráca súkromnej a verejnej sféry.

V súčasnosti je asi najväčšou informačno-bezpečnostnou hrozbou darkweb (darknet). Tento pojem sa len postupne dostáva do popredia štátnych orgánov, ktoré priznali potrebu bojovať proti tomuto fenoménu. Na základe štúdií je možné konštatovať, že obsah internetu, ktorý môžeme bežne vidieť a používať je tvorený len 4 %. Zvyšných 96 % je dostupných na základe prihlásenia sa, čo sa označuje ak používanie deepwebu. Darkweb je na konci reťazca. Niekedy považovaný za súčasť deepwebu. Rozdiel je však v tom, že na darkweb sa nie je možné prihlásiť cez bežný internetový prehliadač. Darkweb funguje cez TOR (The Onion Router), ktorý bol vytvorený a používaný americkou armádou. TOR umožňoval zdieľanie citlivých informácii v absolútnej anonymite. TOR mení každých pár minút IP adresy, ktoré náhodne generuje a tým sa teda subjekt používajúci darkweb stáva prakticky nevystopovateľným. Najčastejšie používanou, vyhľadávanou stránkou je Hidden wiki. Ponuka darkwebu je široká. Nelegálny čierny trh sa prispôsobil novým možnostiam. V darkmarkete sa obchoduje so mnohými komoditami, ako napríklad:

a) s drogami,
b) so zbraňami
c) objednávka vraždy,
d) s falošnými dokladmi, pasmi a vodičskými preukazmi,
e) s ukradnutými platobnými kartami aj s PIN kódmi,
f) s liekmi na predpis aj s rôznymi experimentálnymi liekmi, ku ktorým nemajú šancu dostať sa pacienti v smrteľnom štádiu choroby.

Ako konkrétne príklady by sme mohli uviesť Silk Road, kde si vie užívateľ zaobstarať drogy rôzneho typu y v rôznej kvalite. Kokaín, heroín, syntetické drogy sú bežnou komoditou na Silk Road.

Ďalším príkladom je získavanie cestovných pasov. Tak napríklad Lotyšský pas stojí 1 350,- eur. Holandský pas stojí 1 500,- eur. Dánsky pas stojí 1 500,- eur. Pas Veľkej Británie stojí 1 800,- eur. Kanadský pas stojí 1 250,- eur. Pás Spojených štátov amerických stojí 2 200,- eur.

Na inom mieste je možné nájsť darkmarket so zbraňami. Tak napríklad:

a) GLOCK 19 GEN 3 je možné zadovážiť si za 470,- $,
b) CZ P-07 DUTY 9mm za 475,- $,
c) HI POINT – 40 S&W CARBINE W/3 MAGS za 250,- $,
d) MOSSBERG 500 HOME SECURITY 410 za 320,- $.

Ďalšou súčasťou darkwebu je hackovanie. V rámci darkwebu je možné nájsť veľa ponúk na hackovanie. V rámci bežnej ponuky od 250,- eur vyššie za hodinu je možné získať tieto služby:

a) Jednoduché hackovanie bežne dostupných technológii,
b) Spôsobovanie technických problémov na webstránkach,
c) Ekonomickú špionáž,
d) Získavanie súkromných informácii o niekom,
e) Zničenie obchodovania, života súkromných osôb, vrátane ich finančného zničenia alebo aby boli zadržané bezpečnostnými zložkami,
f) Nahratie detskej pornografie do počítačov iných osôb a podobne.

Na darkwebe je možné nájsť aj inzerciu týkajúcu sa objednávky nájomného vraha. Napríklad Slayers hitmen. Slayers predstavuje skupinku ľudí po celom svete, ktorý na objednávku zrealizujú nájomnú vraždu. Ponúknutý je extrémne profesionálny prístup a anonymita. Organizácia združuje 48 nájomných vrahov ktorý sú dostupný podľa lokalít. Skupina uvádza aj cenovú ponuku. Napríklad:

Usmrtenie zbraňou – 15 000 $,
a) Usmrtenie nožom – 22 000 $,
b) Usmrtenie jedom – 40 000 $,
c) Smrteľné mučenie – 50 000 $,
d) Chemický útok na osobu – 4 000 $,
e) Zjazvenie tváre – 3 000 $,
f) Kastrácia osoby – 30 000 $,
g) Zmrzačenie osoby – 10 000 $,
h) Spôsobenie slepoty – 11 000 $,
i) Mučenie – 20 000 $,
j) Znásilnenie – 2 000 $,
k) Zbitie osoby – 2 000 $,
l) Vystrašenie – 1 000 $.

Podobným aktivitám sa venuje aj spoločenstvo s názvom Dark Mamba. Je to skupina bývalých vojakov, ktorí poskytujú svoje služby s prihliadnutím na maximálnu anonymitu a profesionálny prístup. Ponúkajú napríklad vraždu bežného človeka, vraždu dôležitej osoby, vraždu veľmi dôležitej osoby, likvidáciu šéfa, únosy ľudí a podobne. Ceny sú rôzne v závislosti od dopytu a konkrétnych požiadaviek.

Ďalším príkladom protiprávnej činnosti na darkwebe je tzv. Red Room (červená miestnosť). V tomto prípade je do malej miestnosti umiestnená osoba, ktorá je mučená pričom ponúkaný je live prenos. Účastníci fóra sa po prihlásení zúčastňujú takéhoto online mučenia s tým, že ponúknu konkrétnu finančnú čiastku a navrhnú, aby tej osobe spôsobili bolesť, či útrapu. Ako príklad je možné uviesť zaplatenie určitej sumy užívateľom s požiadavkou odrezania niekoľkých prstov na končatine a podobne. Zjednodušene je možné povedať, že to funguje ako hra na úkor osoby, ktorá je mučená.

Za všetky služby na darkwebe je potrebné zaplatiť. Platba sa uskutočňuje virtuálnou menou. Vzhľadom na anonymitu tejto siete a fakt, že v anonymnom prostredí je ťažké komukoľvek veriť, tak kryptopeniaze sa neposielajú priamo predajcovi. Dostane ich najskôr sprostredkovateľ, obvykle prevádzkovateľ anonymného obchodu, kryptomarketu, ktorý po realizácii služby uvoľní kryptopeniaze vykonávateľovi. Je potrebné uviesť, že riziká pre obchodníkov sú pritom relatívne malé. Oveľa menšie ako pre zákazníkov, ktorí si svoj tovar musia niekde fyzicky zobrať.

Americkej FBI sa napriek tomu podarilo odhaliť niektoré stránky darknetu, zadržať milióny dolárov a zatvoriť ich majiteľov. Takýmto spôsobom už skončil existenciu napríklad najväč-

ší anonymný kybertrh Silk Road a podobne zavreli Utopiu, ktorú odhalili holandskí a nemeckí agenti. V konečnom dôsledku to však vôbec nepomohlo. Prakticky hneď sa totiž objavili nové miesta, kde biznis beztrestne ďalej fungoval, a kde sa objavili identické ponuky na nelegálny tovar a služby.

Predstavených bolo len niekoľko príkladov kybernetických hrozieb, ktoré sú súčasťou dnešnej éry. Z uvedeného je možné prijať jednoznačný záver, že je priam nevyhnutné nájsť efektívne nástroje v boji proti týmto nevojenským bezpečnostným hrozbám.

3. Prostriedky boja proti informačným hrozbám

Nevojenské hrozby sú čoraz väčšou realitou, než tie vojenské. Je potrebné im venovať čoraz väčšiu pozornosť a hľadať efektívne nástroje aspoň k čiastočnej eliminácii týchto hrozieb. Otázkou je: Je možné efektívne bojovať proti vyššie predstaveným kybernetickým hrozbám? Je možné bojovať proti darknetu, je možné ho redukovať, eliminovať? V určitom aspekte to možné je. Tu musia zohrávať najdôležitejšiu úlohu bezpečnostné zložky štátu ako aj vybrané trestnoprávne inštitúty, ktoré musia byť efektívne využívané za účelom odhaľovania tak závažnej trestnej činnosti, ktorú sme vyššie predstavili. Bez pochyb k takýmto inštitútom je možné zaradiť využívanie informačno-technických prostriedkov, ako aj prostriedkov operatívno-pátracej činnosti. Ich legálne využívanie môže, podľa môjho názoru, prispieť k odhaľovaniu tak závažnej trestnej činnosti.

Pod **informačno-technickými prostriedkami** je potrebné rozumieť: „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." (§ 10 ods. 21 TP)

V zmysle TP je teda možné za informačno-technické prostriedky považovať:

a) odpočúvanie a záznam telekomunikačnej prevádzky (§ 115),
b) oznámenie údajov o telekomunikačnej prevádzke (§ 116 TP),
c) vyhotovovanie obrazových, zvukových a obrazovo-zvukových záznamov (§ 114 TP) a
d) vyhľadávanie, otváranie a skúmanie zásielok (§ 108 a § 109 TP).

Používanie ITP je možné len za naplnenia zákonných podmienok. „Informačno-technické prostriedky možno použiť iba vtedy, ak je to v demokratickej spoločnosti nevyhnutné na zaistenie bezpečnosti štátu, predchádzanie a objasňovanie trestnej činnosti alebo na ochranu práv a slobôd iných."[9] Základným predpokladom použitia uvedených prostriedkov je legálny dôvod, ktorým je potrebné dosiahnuť zákonom vymedzený cieľ. Podmienkou je nutnosť ich použitia len v takom rozsahu a na tak dlho, ako to umožňuje zákon. Ďalšou podmienkou je sústavnosť skúmania dôvodov používania jednotlivých prostriedkov. Za týchto, ako aj ďalších zákonných podmienok, ktoré budeme ďalej definovať, je možné spomenuté prostriedky plnohodnotne využívať. Ak dôjde k porušeniu niektorej z podmienok, získaný záznam nie je možné použiť ako dôkaz pre potreby ďalšieho konania. Zároveň je potrebné zdôrazniť, že ak sa nepodarilo po-

[9] ČENTÉŠ, J. a kolektív. 2016. *Trestné právo procesné, Všeobecná časť*. Šamorín: Heuréka. 2016. s. 293–294.

užitím informačno-technických prostriedkov získať skutočnosti, resp. informácie, pre ktoré bolo používanie týchto prostriedkov umožnené, takéto záznamy je potrebné bezodkladne zničiť.[10]

Orgánom oprávneným využívať jednotlivé informačno-technické prostriedky je v zmysle 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):

a) Policajný zbor,
b) Slovenská informačná služba,
c) Vojenské spravodajstvo, Zbor väzenskej a justičnej stráže,
d) Colná správa.

Prostriedky operatívno-patrácej činnosti sú rovnako zadefinované v TP. Konkrétne v § 10 ods. 22 TP. V zmysle tohto ustanovenia k prostriedkom operatívno-pátracej činnosti je možné zaradiť:

a) Kontrolovanú dodávku (§ 111 TP),
b) Zámenu obsahu zásielok (§ 110 TP),
c) Agenta (§ 117 TP),
d) Predstieraný prevod (§ 112 TP),
e) Sledovanie osôb a vecí (§ 113 TP).

Operatívno-pátracej činnosti sa venuje napríklad aj zákon č. 171/1993 Z. z. o Policajnom zbore v § 38a. v Zmysle predstaveného ustanovenia sa operatívno-pátracou činnosťou rozumie: „systém spravidla utajených, spravodajských opatrení vykonávaných Policajným zborom na účely predchádzania, zamedzovania, odhaľovania a dokumentovania trestnej činnosti a zisťovania jej páchateľov, 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."

Ako uvádza Tittlová vo všeobecnosti možno uviesť, že aplikáciou operatívno-pátracej činnosť, s ohľadom na jej povahu a charakter, ktoré plynú z právnej, personálnej, ako aj ekonomickej, technickej, taktickej požiadavky, a celého radu požiadaviek ďalších, sú poznávané objekty kriminality, ktoré môžu byť inými, menej zložitými postupmi, len ťažko poznateľné. Tieto objekty sú poznávané operatívnymi pracovníkmi, resp. inými subjektmi, ktoré sú cieľavedome zapojené do tejto činnosti, v konkrétnom čase, na určitom mieste, za určitej situácie. Cieľom tohto poznávania *je **účelové*** získavanie a vyhodnocovanie konkrétnych informácií o poznávanom kriminálnom objekte. V danom prípade je možné konštatovať, že ide o poznávanie informácií, ktoré sú vnímané poznávaným subjektom bezprostredne, a to buď v čase pred ich vznikom, v čase ich vzniku, prípadne retrospektívne v čase ich existencie prostredníctvom informácií, ktoré súvisia so vznikom a existenciou poznávaného kriminálneho objektu, alebo kombináciou týchto postupov.

Operatívna činnosť predstavuje *základ odhaľovania latentných druhov kriminality.* Ide o systém *utajených opatrení, ktoré majú spravodajský charakter*, a ktoré vykonávajú príslušné služby Policajného zboru. Operatívnu a operatívno-pátraciu činnosť je v tomto kontexte potrebné vnímať ako základ odhaľovania latentnej kriminality spoločne so zisťovaním a následne usvedčovaním jej páchateľov. Priamo zákon formuluje túto činnosť ako činnosť vykonávanú *spravodajským spôsobom*, teda *utajene,* čo je predpoklad jej efektívneho a účinného využívania. Ak by sa tieto prostriedky nevyužívali spravodajským spôsobom, a teda osoby, ktorých sa výkon týchto

[10] IVOR, J., TÓTHOVÁ, M. 2013. *Použitie informačno-technických a operatívno-pátracích prostriedkov*. In: Dokazovanie v trestnom konaní. Praha: Leges, 2013, s. 251 – 276.

prostriedkov dotýka, by v reálnom čase a na určitom mieste vedeli o ich použití, je zrejmé, že osoby by svoje konanie zámerne upravili a pozmenili tak, aby sa ich použitím nezistili žiadne relevantné informácie ani veci.[11] Prostriedky operatívno-pátracej činnosti sú bez pochýb významným nástrojom v boji proti vyššie spomenutým bezpečnostných hrozbám.

Záver

Informačno-technické prostriedky, ako aj prostriedky operatívno-patrácej činnosti sú bez pochýb významným prostriedkom v boji proti vnútorným, či vonkajším bezpečnostným hrozbám, vrátane vyššie predstavených informačných hrozieb. Ide o unikátne procesnoprávne inštitúty, ktorých realizácia spôsobuje zásahy do osobnostnej sféry dotknutých osôb. Zasiahnuté sú konkrétne práva a slobody dotknutých osôb. Preto je nevyhnutné dbať na striktné dodržiavanie zákonných podmienok. V súčasnosti je takmer nevyhnutné bojovať proti aktuálnym bezpečnostným hrozbám, tak vnútroštátnym, ako aj medzinárodným. Právny základ spolupráce v boji proti aktuálnym hrozbám existuje. Je však nevyhnutné apelovať na striktnú realizáciu jednotlivých nástrojov. Oba z predstavených prostriedkov dokážu efektívnym spôsobom bojovať proti vyššie predstaveným hrozbám. Ich využívanie však musí byť účelné, aby bola následne garantovaná efektivita. Bojovať proti analyzovaným hrozbám nie je vôbec jednoduché. Avšak aplikáciou predstavených inštitútov, vrátane cezhraničnej spolupráce prostredníctvom Europolu, Interpolu, či inej medzinárodnej organizácie, je možné takéto hrozby postupne redukovať či dokonca eliminovať.

Literatúra

BURDA, E., ČENTÉŠ, J., KOLESÁR, J., ZÁHORA, J. a kolektív. 2011. *Trestný zákon. Osobitná časť. Komentár. II. diel*. 1. vydanie. Praha: C. H. Beck, 2011. s. 1608, ISBN 978-80-7400-394-3.

ČENTÉŠ, J. a kolektív. 2016. *Trestné právo procesné, Všeobecná časť*. Šamorín: Heuréka. 2016. s. 440. ISBN 978-80-8173-02-07.

ĎORULA, J. a kol. 2003. *Krátky slovník slovenského jazyka*. Bratislava: Veda, 2003. s. 985. ISBN 80-224-0750-X.

IVOR, J., TÓTHOVÁ, M. 2013. *Použitie informačno-technických a operatívno-pátracích prostriedkov*. In: Dokazovanie v trestnom konaní. Praha: Leges, 2013, s. 251-276, ISBN 9788087576762.

ŠKVRNDA, F., PAWERA, R., WEISS, P. 2008. *Medzinárodná bezpečnosť*. Bratislava: Ekonóm, 2008. s. 184, ISBN 978-80-225-2527-5.

TITTLOVÁ, M., MEDELSKÝ, J. 2017. *Zákon o Policajnom zbore, Komentár*. Bratislava: Wolters Kluwer. 2017. s. 394, ISBN 978-80-8168-577-4.

Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov.

Zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov.

https://www.europol.europa.eu/activities-services/europol-in-action/operations/operation-rescue.

[11] Pozri bližšie: TITTLOVÁ, M., MEDELSKÝ, J. 2017. *Zákon o Policajnom zbore, Komentár*. Bratislava: Wolters Kluwer. 2017. s. 209.

Obrazový, zvukový alebo obrazovo-zvukový záznam ako informačno-technický prostriedok v trestnom konaní

Video, Audio or Video-sound Recording as Information and Technology in Criminal Proceedings

Dominik Vanek[1]

Abstrakt: *V modernej spoločnosti predstavujú informačno-technické prostriedky, pomocou ktorých je možné bojovať proti organizovanej kriminalite v takej miere, aby sa dosiahla maximálna miera efektivity. V mnohých prípadoch nám prax jednoznačne ukázala, že informačno-technické prostriedky sú unikátnou možnosťou boja napríklad proti rôznym druhom kriminality. Je teda možné povedať, že práve pomocou nami vybraného informačno-technického prostriedku je možné zvýšiť efektivitu boja s kriminalitou a túto aj odhaľovať. Obrazový, zvukový alebo obrazovo-zvukový záznam predstavuje jeden z najpoužívanejších a najefektívnejších informačno-technických prostriedkov.*

Abstract: *In modern society, information technology means that it is possible to combat organized crime to the extent that maximum efficiency is achieved. In many cases, the practice has clearly shown that information technology is a unique opportunity to fight, for example, against various types of crime. Thus, it is possible to say that it is by means of the information and technical means chosen by us that it is possible to increase the effectiveness of the fight against crime and to detect it. Video, audio or video-audio is one of the most widely used and effective information technologies.*

Kľúčové slová: *Informačno-technické prostriedky, Organizovaná kriminalita, Ústava, Ľudské práva, Spoločnosť, Aplikačné problémy.*

Keywords: *Information technology, Organized crime, Constitution, Human rights, Society, Application problems.*

1. Úvod

Vplyvom vývoja modernej spoločnosti, predovšetkým potreby zvýšenia efektivity vymoženia práva a spravodlivosti, sa zvyšoval tlak aj na zákonodarcu aby prijal právne normy v takom rozsahu, aby sa zvýšila efektivita vymožiteľnosti práva a spravodlivosti. Rovnaký vplyv malo postupné a relatívne pomalé snahy o rekodifikáciu právneho poriadku. Podstatný vplyv na nami predostieranú tému mala aj snaha o upevnenie rešpektovania ľudských práv, ako podstatných zložiek právnych poriadkov každého vyspelého demokratického štátneho zriadenia. Predovšetkým snaha o vyššiu efektivitu dokazovania a tým aj celého trestného konania mala vplyv na to, že sa do právneho poriadku začali implementovať prvky, ktoré dosiaľ neexistovali. Rovnako podstatnou zmenou bola snaha o zabránenie neprirodzeného a neprimeraného zásahu do osobných práv jednotlivca zo strany štátu a štátnej moci. Spoločnosť a jej demokratické zriadenie vystavané na demokratických princípoch, ktoré okrem iných zahŕňali aj princípy ako odhaľovanie a trestanie trestnej činnosti a ochrana právom chránených záujmov jednotlivcov a celej spoločnosti mala snahu o zvýšenie vplyvu pri odhaľovaní trestnej činnosti. Hlavne v období *mečiarizmu*[2] sa začal naplno prejavovať masívny problém s organizovanou trestnou činnosťou, ktorá mala na svedomí rovnako násilnú trestnú činnosť prepojenú s ekonomickou kriminalitou. Tieto

[1] JUDr. Dominik Vanek, Paneurópska vysoká škola, Fakulta práva, e-mail: Dominik.Vanek1@gmail.com.

[2] Obdobie vlády HZDS a premiéra V. Mečiara (90-roky 20. storočia).

pomerne organizované skupiny vykonávali svoju trestnú činnosť pomerne sofistikovaným spôsobom, preto bežné metódy vyšetrovania často neviedli k úspešným výsledkom.

Spoločnosť preto oprávnene žiadala vládnucu elitu o zefektívnenie boja proti týmto kriminálnym živlom. Je pomerne zarážajúce to, že do roku 1990 neexistovala zmienka v právnom poriadku o tom, akým spôsobom je možné zasahovať do ľudských práv a či vôbec, za zámerom objasnenia kriminálnej činnosti jednotlivca za pomoci techniky, ktorá je určená na vykonávanie takejto činnosti. Spomenutá technika bola využívaná na získanie predovšetkým obrazových a zvukových materiálov, ktoré sa v drvivej väčšine prípadov získavali utajeným (spravodajským) spôsobom. Prvým a prelomovým momentom bolo začlenenie inštitútu odpočúvania a získavania obrazovo-zvukových záznamov vo veľkej väčšine spravodajským spôsobom konania. Spolu s týmto inštitútom bola prijatá právna norma označená ako zákon č. 422/2002 Z. z., ktorá do vtedajšej právnej úpravy začlenila aj možnosť vyhotoviť obrazový alebo zvukový záznam utajeným spôsobom. Aj v týchto momentoch je evidentný vplyv politického zoskupenia v krajine, pretože toto obdobie našej histórie je známe postupným odhaľovaním trestnej činnosti. Vyššie spomenutý inštitút sa v nezmenenej podobe preniesol aj do nového rekodifikovaného Trestného poriadku. Možno teda jednoznačne povedať, že inštitút ktorý nám priznáva právo v zákonom ustanovených prípadoch a v prípade splnenia podmienok, ktoré nám priznáva zákon zachytávať pohyb osôb, komunikáciu osôb, činnosť dotknutých osôb a všetky tieto informácie zaznamenávať takým spôsobom, aby následne informácie takto získané, mohli byť použité v trestnom konaní ako dôkaz.

Takto získané dôkazy a informácie a fakt, že boli získané utajeným spôsobom zvyšuje faktor ich dôveryhodnosti a objektívnosti. Jediným možným obmedzením, je ľudský faktor. Aj vďaka pokročilej technológii, všetky tieto spravodajské prístroje ovláda človek, preto jeho zmyslové vnímanie a odhad majú často priamy vplyv na kvalitu a rozsah získaných informácii. Aj tento fakt sa vplyvom stále narastajúcej kapacity zariadení mení skôr na raritné prípady, pretože v dnešnej dobe je možné zachytávať a uschovávať obrovské množstvo materiálu a moderné počítačové programy nám značne uľahčujú prácu s týmito informáciami.

2. Obrazový, zvukový alebo obrazovo-zvukový záznam ako informačno-technický prostriedok

V období od vzniku samostatnej Slovenskej republiky sa v oblasti kriminality začal objavovať veľmi nebezpečný jav. Začína existovať a prejavovať sa vo všetkých zložkách spoločnosti tzv. organizovaná kriminalita. Spolu s rastúcim vplyvom organizovanej kriminality a vzrastajúcej dynamike trestnej činnosti narastá aj potreba spoločnosti brániť sa voči takýmto vplyvom. Organizovaná kriminalita sa transformuje do rôznych kriminálnych zoskupení, ktoré sú tvorené organizovanou štruktúrou jednotlivcov, kde každý jednotlivec plní svoju úlohu vykazuje určité prvky odolnosti voči bežne využívaným praktikám orgánov činných v trestnom konaní. Tieto skupiny boli hierarchicky vystavané subjekty, ktoré mali vlastné interné pravidlá a rovnako aj významný zdroj príjmov, ktoré pochádzali prevažne z násilnej alebo ekonomickej kriminality. Práve ekonomická sila a vnútorný kapitál takýchto organizovaných skupín, ruka v ruke s prerastajúcou korupčnou činnosťou, využívaním brutálnej sily alebo demonštratívnych aktov sily, predstavoval pre štát a spoločnosť silného protivníka, ktorému musela mladá krajina čeliť. Práve tieto fakty vyvolali nielen na území tak mladého štátu akým Slovenská republika stále je potrebu zmeny tak trestných zákonov, ako aj rekodifikáciu trestných poriadkov. Tieto zmeny v sebe prinášali aj obmedzenia v oblasti ľudských práv, avšak záujem spoločnosti o vyšetrenie a po-

trestanie páchateľov takejto trestnej činnosti vysoko prevýšil záujem o ochranu ľudských práv jednotlivých subjektov. Tieto subjekty boli priamo zodpovedné za páchanie trestných činov, v prevažne organizovaných skupinách. Jednotlivé štáty teda posilnili svoje právomoci aby mohli efektívnejšie bojovať s podobným druhom trestnej činnosti. Ivor charakterizuje tieto prostriedky nasledovne:

- *Ide o veľmi intenzívny zásah do základných práv a slobôd, garantovaných medzinárodnými dokumentmi a ústavou, čo si vyžaduje veľmi precíznu a podrobnú zákonnú úpravu*
- *Ide o postupy, ktorých efektívnosť výsledku predpokladá ich utajenosť aplikácie. V tejto súvislosti sú niektoré kontrolné mechanizmy značne obmedzené ba úplne vylúčené*
- *Pre dôkazné využitie týchto prostriedkov za súčasného garantovania riadneho procesu (čl. 6 Európskeho dohovoru) sa predpokladá špeciálna legislatívna úprava a jej dôsledné dodržiavanie v aplikačnej praxi*[3]

Na základe uvedeného, je možné sa odvolať aj na Ústavu, ktorá v čl. 1 ustanovuje že, *Slovenská republika je zvrchovaný, demokratický a právny štát*.[4] Na základe ďalších ustanovení Ústavy jednoznačne vyplýva, že Slovenská republika je štát, ktorý je založený na princípoch, ktoré rešpektujú všetky práva a slobody jednotlivca. Tieto práva nám vyplývajú z množstva prijatých medzinárodných zmlúv, ktorými je Slovenská republika viazaná. Tieto zmluvy Slovenská republika prijala a ratifikovala spôsobom, ktorý jej ustanovuje príslušný zákon. Špeciálnu pozornosť si zaslúži právna ochrana ľudských práv a slobôd, presnejšie právo na súkromie, ochrana osobných údajov, ochrana osobnosti. Týchto oblastí sa veľmi citlivo dotýka aj čl. 8 Európskeho dohovoru o ľudských právach a základných slobodách. Spomenutý článok v skratke ustanovuje, že každý jednotlivec má právo na súkromie a štátna moc do tohto práva môže zasiahnuť iba v súlade so zákonom a v nevyhnutných prípadoch. Zásahy do súkromia výrazne obmedzuje aj naša Ústava, ktorá tak robí v čl. 13, kde ustanovuje, že zásah je možný len na základe zákona. Podobné ustanovenie obsahuje aj Občiansky zákonník[5] ktorý ustanovuje, *že privolenie nie je potrebné, ak sa vyhotovia alebo použijú písomnosti osobnej povahy, podobizne, obrazové snímky, zvukové alebo obrazové a zvukové záznamy na úradné účely na základe zákona*.[6]

Ako sme uviedli vyššie, do roku 1990 neexistovalo v právnom poriadku uznesenie právo štátu zasahovať do práv, ktoré boli garantované Ústavou alebo medzinárodnými zmluvami. Neexistovala ani právna úprava, ktorá by dovoľovala použitie techniky operatívnej povahy na zabezpečenie dôkazov, ktoré by mohli mať relevantný vplyv na trestné konanie. Je to však paradoxné, pretože je dnes priamo dokázané, že vtedajšie spravodajské služby využívali operatívne technológie a aj cvičený personál, na odpočúvanie komunikácie a vytváranie zvukovo-obrazových záznamov o politicky nepohodlných osobách. Tieto postupy priamo upravovali interné, medzirezortné dokumenty, ktoré boli často utajené. Informácie, ktoré sa podarilo týmto spôsobom zistiť, však boli často využívané na celkom iné účely, ako bolo preukazovanie a dokazovanie trestnej činnosti v trestnom konaní. Právny poriadok dokonca ani nepriznával oprávnenie subjektom činným v trestnom konaní takéto informácie v konaní použiť. Trestný poriadok platný v danom období, iba demonštratívnym výpočtom vymenovával dôkazné prostriedky, ktoré je možné využiť v trestnom konaní.

V roku 1990 bola prijatá právna norma pod označením zákon č. 178/1990 Zb., ktorým bol novelizovaný vtedajší Trestný poriadok (č. 141/1990 Zb.). Táto právna úprava prvý krát zaviedla

[3] IVOR, J. Obrazovo-zvukový záznam, In Zborník príspevkov z vedeckej konferencie na tému Teoretické a praktické problémy dokazovania, z roku 2008, s. 70.

[4] Ústava SR, čl. 1.

[5] Zákon č. 40/1964 Zb. Občiansky zákonník.

[6] § 12 Občianskeho zákonníka.

do Trestného poriadku ustanovenie pod § 88 *odpočúvanie telefónnych hovorov*. Tento paragraf sa dal využiť pre trestné činy, ktoré boli taxatívne uvedené. Novela Trestného poriadku (č. 366/200 Z. z.) priznala právo súdu nariadiť odpočúvanie a záznam telekomunikačnej prevádzke súdu. Iná novela Trestného poriadku označená ako zákon č. 422/2002 Z. z. a norma č. 458/2003 Z. z. výrazne obmedzila poskytovanie údajov pre telekomunikačnú činnosť, ktoré dovtedy tvorili súčasť telekomunikačného tajomstva, pretože sa na tieto údaje vzťahoval zákon o ochrane osobných údajov a vydanie týchto údajov bolo podmienené vydaním súhlasného stanoviska príslušného súdu.

Práve novela Trestného poriadku na základe zákona č. 422/2002 Z. z. zavádza do slovenského právneho poriadku nový, prostriedok mimoriadneho významu, ktorým je možné zabezpečiť informácie. Ide o ustanovenie § 88 písm. e. Dotknuté ustanovenie hovorí o vyhotovení obrazových, zvukových záznamov podľa § 88.

Aj v súčasnej dobe platnom Trestnom poriadku, označenom ako právna norma č. 301/2005 Z. z. sa považuje za významný inštitút zásahu do osobných práv jednotlivca ustanovenie § 114. Práve toto ustanovenie poskytlo zákonodarcovi priestor na zásadnú úpravu dovtedy platnej právnej úpravy. Prišlo k zmene demonštratívneho výpočtu vecí, pre ktoré sa dal spomenutý zabezpečovací inštitút použiť na taxatívny výpočet trestných činov, pre ktoré bolo využitie inštitútu oprávnené. Zákonodarca presne ustanovil kto a za akých podmienok je oprávnený začať a schváliť potrebný mechanizmus pri použití inštitútu vyhotovenia obrazového, zvukového alebo zvukovo-obrazového záznamu. Aby sa predišlo tomu, že stíhaní jednotlivci sa budú pri svojom trestnom stíhaní odvolávať na svoje ústavné právo o ochrane pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužitím osobných údajov, zákonodarca do ustanovenia § 114 ustanovil, že ak sa nezistia skutočnosti významné pre trestné konanie, príslušný orgán musí tieto informácie okamžite zničiť. Aby sa zaistilo zničenie týchto záznamov, zákonodarca stanovil príslušnému orgánu povinnosť, aby o tomto zničení vypracoval podrobnú zápisnicu a upovedomiť v lehote do 3 rokov všetky dotknuté osoby. Z taktických dôvodov sa realizuje povolenie využitie spomenutého inštitútu vo forme príkazu, ktorý sa však nedoručuje dotknutej osobe, je možné realizáciu tohto zabezpečovacieho inštitútu zaradiť medzi utajované skutočnosti. Keby v právnej úprave neexistovala táto povinnosť oznámiť dotknutým osobám tieto skutočnosti, bol by to významný problém v oblasti ochrany práva na súkromie. Keďže išlo o významný zásah do súkromia týchto osôb, mali by byť oprávnené domáhať sa dôvodnosti takého zásahu do súkromia súdnou cestou. Zákonodarca myslel aj na túto možnosť a dotknutá osoba sa môže obrátiť na Najvyšší súd SR so žiadosťou o preskúmanie zákonnosti spomenutého zásahu.

3. Využitie obrazovo-zvukového záznamu v zákonných podmienkach Slovenskej republiky

Aby nebol zmarený účel využitia informačno-technického prostriedku v trestnom konaní, je potrebné naplniť všetky, relatívne prísne zákonné podmienky kumulatívnou formou. *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.[7] Pri tak výraznom zásahu do osobných práv jednotlivca žijúceho v demokratickej krajine, je to oblasť hodná osobitného zreteľa. Zákonodarca zhrnul zákonné podmienky do Trestného poriadku, presnejšie do ustanovenia § 114. Spomenuté ustanovenie presne popisuje proces povoľovania využitia spomenutého zabezpečovacieho prostriedku, rovnako zákonné podmienky jeho využitia, druh a povahu rozhodnutia akým bude v budúcnosti povolené využiť tento prostriedok, rovnako ako aj lehotu, počas ktorej je možné zasahovať do osobných práv jednotlivca týmto prostriedkom. Najdôležitejšou podmienkou, je fakt, že spomenutý informačný prostriedok sa na základe § 114 TP využije v trestnom konaní. Na základe uvedeného je na mieste tvrdenie, že sa využíva v trestnoprocesnej rovine. V trestnom konaní existuje viacero fáz. Podľa faktov, ktoré sme uviedli vyššie, je možné uviesť, že informačno-technický prostriedok využívame v nasledujúcich fázach:

- v rámci prípravného konania v trestnej veci
- postupe pred začatím trestného stíhania konkrétnej osoby
- trestnom konaní, ktoré sa musí viesť pred súdom

V priamej súvislosti s tým, v akej fáze sa trestné konanie nachádza, je potrebné rozlíšiť aj subjekt, ktorému zákon priznáva možnosť vydať príkaz pre použitie spomenutého prostriedku. Okrem týchto podmienok jednu z najpodstatnejších podmienok tvorí aj to, či sa bude vyhotovovanie záznamu spájať so vstupom do bydliska osoby alebo naopak. Zákonodarca evidentne rozlišuje to, či vyhotovenie záznamu je priamo spojené aj so vstupom do obydlia iného. Ak by sa malo vstúpiť do obydlia iného, zákonodarca stanovil podstatne prísnejšie kritéria pre vydanie takého príkazu sudcom, resp. okruh prípadov, pre ktoré je možné vydať potrebný príkaz je značne menší. Zákon rovnako popisuje aj dômyselný povoľovací mechanizmus. Zákonodarca pre vydanie príkazu obligatórne vyžaduje písomnú formu. Subjekt, ktorý má oprávnenie vydávať príkaz sa odlišuje v závislosti na tom, v akom štádiu sa trestné konanie nachádza. V zásade platí nasledovné:

- V súdnom konaní je oprávnený subjekt predseda senátu
- V postupe pred začatím trestného stíhania je to vždy sudca pre prípravné konanie rovnako ako v prípravnom konaní

Z týchto všeobecných pravidiel platí výnimka. Ak by nastala v praxi situácia, že v prípravnom konaní resp. v postupe pred začatím trestného stíhania nebude možné takýto príkaz vydať klasickým spôsobom, zákonodarca oprávňuje pre vydanie takého príkazu aj prokurátora. Ide však o veľmi špecifické prípady, kedy je potrebné brať ohľad predovšetkým na operatívnosť resp. časovú tieseň, ktorá bráni vydaniu príkazu klasickou cestou. Zákonodarca stanovil viaceré podmienky, ktoré musia byť naplnené kumulatívnou formou:

- Splnenie podmienok, za ktorých by aj sudca pre prípravné konanie vydal príkaz, hoci posudzovanie podmienok je v tomto prípade na prokurátorovi
- Povaha prípadu musí dostatočne odôvodniť tento špecifický postup
- Nesmie sa vstúpiť do obydlia osoby
- Táto vec neznesie odklad
- Do 24 hodín od schválenia príkazu prokurátorom tento príkaz dodatočne musí schváliť sudca. Bez naplnenia tejto podmienky nie je možné pokračovať vo vyhotovovaní záznamu a všetky doteraz získané záznamy je potrebné zničiť zákonom predpísaným spôsobom.

Príkaz, ktorým sudca pre prípravné konanie štartuje proces vyhotovovania záznamu sa vydáva vždy na základe žiadosti prokurátora. Iba prokurátor má zo zákona oprávnenie iniciovať

[7] POLÁK, P., TALAPKA, M. Prípustnosť využitia dôkazov získaných použitím informačno-technických prostriedkov pre účely trestného konania, In Zborník príspevkov z medzinárodnej konferencie na tému Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní, FP PEVŠ 2017, s. 153.

tento prostriedok v konkrétnej časti trestného konania. V tomto príkaze prokurátorovi zákonodarca priznáva povinnosť odôvodniť vydanie príkazu priamymi podozreniami, ktoré musia byť podložené zisteným skutkovým stavom prípadu. Tento návrh obligatórne obsahuje aj osobné identifikačné údaje osôb resp. vecí ktoré majú byť predmetom vyhotovovania záznamu. Tieto skutočnosti následne sudca zahrnie do vydania príkazu. Je samozrejmé, že tieto skutočnosti sa uvádzajú tak prokurátorom alebo sudcom iba v prípade, že sú im tieto známe. Neznalosť týchto údajov nezakladá prekážku vydania takéhoto rozhodnutia. Zákonodarca však ustanovil, že ak sú známe dodatočné informácie o osobe podozrivej z trestnej činnosti voči ktorej budú nasadené spomenuté prostriedky, sudca resp. prokurátor je povinný tieto oznámiť a zaznamenať ich do príkazu, resp. jeho návrhu. V praxi sa často stáva, že sú uvádzané telesné odchýlky, ktoré výrazne zjednodušia prácu subjektom, ktoré budú následne do vykonávania procesu záznamu zapojené. Veľmi často ide o farbu vlasov, špecifickú úpravu zovňajšku osoby (tetovania, zranenia), špecifický typ chôdze, zlozvyky a podobne. Tieto informácie sa zaznamenávajú preto, aby v reálnom vykonávaní procesných úkonov nemohlo prísť k zámene podozrivej osoby za inú osobu a tým následne zmarenie operatívnej činnosti. Okrem týchto informácií, ktoré napomáhajú týmto subjektom k vyhotoveniu záznamov, sa do príkazu uvádza aj časové obdobie (lehota) počas ktorej je možné prostriedok využívať. Zákonodarca stanovil maximálnu možnú lehotu na obdobie 6 mesiacov. Túto lehotu je však možné predĺžiť a to aj opakovane vždy o dva mesiace. V týchto miestach v prichádza k značným rozporom v odborných diskusiách. Zákonodarca zrejme neúmyselne nedomyslel dané ustanovenie, pretože síce stanovil maximálnu možnú lehotu, stanovil aj výnimku avšak už presne neustanovil možný počet opakovaní využívania tejto výnimky. V praxi môže teda nastať prípad, kedy bude využitie tohto prostriedku trvať aj niekoľko rokov. Je na mieste otázka, či niekoľkoročný zásah do takých závažných práv jednotlivca je stále v slabšej pozícii ako záujem spoločnosti? Pokiaľ počas 6 mesiacov nebolo zistené, že dotyčná osoba pácha trestnú činnosť, nebolo by správne ukončiť tento zásah? Na druhej strane, počas celého trvania využívania tohto prostriedku, zákonodarca ustanovil povinnosť príslušníkom PZ SR povinnosť, aby neustále skúmali oprávnenosť využitia tohto prostriedku. Ak by zistili, že počas využívania spomenutého prostriedku pominuli dôvody, pre ktoré sú oprávnení prostriedok využívať, sú zo zákona povinní ukončiť takýto záznam a o tejto skutočnosti informovať subjekt, ktorý vydal takýto príkaz. V prípravnom konaní sa okrem subjektu ktorý vydal príkaz oznamuje táto skutočnosť aj prokurátorovi.

Z vyššie uvedených informácii vyplýva, že sú to príslušníci PZ SR, ktorí sú poverení vyhotovovaním predmetných záznamov. Poverení príslušníci z jednotlivých odborov PZ SR majú na starosti záznam zvuku, obrazu alebo vyhotovujú kombináciu týchto záznamov. Pri vyhotovovaní takýchto záznamov, musia dbať o to aby boli dodržané všetky zákonné náležitosti, poprípade aby neporušili žiadnu z mnohých výnimiek, ktorú podozrivým osobám priznáva TP. Jednou z podobných výnimiek je aj rozhovor medzi obvineným a jeho obhajcom. Podľa TP sa totiž nesmie zaznamenávať rozhovor medzi obvineným a jeho obhajcom. Ak by aj bol vykonaný tento záznam, nemôžu sa informácia z neho použiť v trestnom konaní. Táto výnimka iba rešpektuje právo obvineného na to, aby sa mohol slobodne radiť so svojim obhajcom bez prítomnosti inej osoby. Informácie, ktoré si počas takéhoto rozhovoru vymenia, majú povahu tajnej informácie. Obhajca v trestnom konaní je povinný zachovávať mlčanlivosť o týchto informáciách, ktoré sa dozvie počas výkonu povolania pri zastupovaní práv obvineného. Toto tajomstvo sa vzťahuje na všetko o čom sa dozvie, až na výnimku o plánovanom trestnom čine, o ktorom sa vďaka komunikácii s klientom dozvedel. Na základe uvedeného teda platí, že keď sa príslušníci zboru dozvedia o tom, že informácie ktoré získali pochádzajú z rozhovoru medzi klientom a obvineným, tieto informácie strácajú na procesnej hodnote a nesmú sa v procese použiť. Naopak, ak by sa

zistilo, že ide o komunikáciu s advokátom, ktorý obvineného v danej veci nezastupuje, tieto informácie sa dajú v prebiehajúcom trestnom konaní bez akýchkoľvek pochybností použiť. Rovnako ako predošlé, aj toto ustanovenie je miestami vágne. Odkiaľ sa dozvedia príslušníci PZ SR o tom takomto rozhovore medzi klientom a obhajcom? Jediná možnosť je, že budú nepriamy účastníci takéhoto rozhovoru v rámci vyhotovovania záznamu. To je prvý problém a druhým problémovým miestom právnej úpravy je aj určenie subjektu oprávneného na rozhodnutie o povahe takéhoto rozhovoru. Je to konkrétny príslušník PZ SR ktorí si rozhovor vypočul, alebo jeho nadriadený? Zákonodarca nám odpovede na tieto otázky vo svojich ustanoveniach zatiaľ neposkytuje. K predmetným informáciám sa teda dostanú aj iné osoby, čo je vo svojej podstate v priamom rozpore s vyššie spomenutým tajomstvom. Aj keď zákonodarca zakázal použitie týchto informácii v trestnom konaní, avšak orgán činný v trestnom konaní touto informáciu už disponuje. Nemôže s ňou však priamo pracovať, avšak je otázka, či tieto informácie nebudú nápomocné pri vyšetrovaní a ďalšom procesnom postupe. Síce povaha týchto informácii je nezákonná orgány s ňou môžu a pravdepodobne aj budú disponovať. Je teda na mieste otázka, či by sa vyšetrovanie trestného činu dostalo do oblastí, aj keby orgány činné v trestnom konaní nedisponovali informáciami, ktoré de facto získali nezákonnou cestou. Burda hovorí o nezákonne získanom dôkaze nasledovné a to že, *v praxi sa často môžu vyskytnúť prípady, i keď pripúšťam, že sa mi na Slovensku a ani v Čechách, ba ani v rozhodovacej praxi Európskeho súdu pre ľudské práva nepodarilo nájsť taký judikát v ktorých je dôkaz evidentne získaný nezákonne, avšak svedči v prospech obvineného, teda je tzv. ospravedlňujúcim dôkazom. Slovenská trestnoprávna teória sa v týchto prípadoch zväčša uspokojuje s jednoduchou konštaláciou, že aj nezákonne získaný dôkaz v prospech obvineného nie je neprípustný*.[8]

V praxi to vyzerá potom tak, že sa z celej získanej zaznamenanej komunikácie vyberie len tá časť, ktorá má svojím významom relevantný vzťah k trestnému konaniu. Z tejto komunikácie sa následne vyhotoví doslovný prepis. Okrem prepisovaných skutočností sa uvádzajú aj informácie vzťahujúce sa k zákonnosti vyhotovenia a použitia tohto záznamu. Uvedú sa aj informácie ktoré hovoria o čase a mieste, kde bol záznam vyhotovený, rovnako sa uvedú aj informácie o zodpovednom orgáne, ktorý záznam vykonal. Vplyvom modernej techniky je možné záznam následne uložiť na vhodný nosič a tento založiť a označiť túto skutočnosť v spise. Oprávnené osoby (prokurátor, obvinený prípadne jeho obhajca) majú zo zákona oprávnenie vyžiadať si kópiu takéhoto materiálu. Obhajcovi aj obvinenému zo zákona prislúcha možnosť nechať si vyhotoviť doslovnú prepis celého záznamu alebo len jeho časti, tieto úkony však spadajú pod ich vlastné náklady. Vierohodnosť a objektivita získaných informácii využitím vyššie spomenutého informačného prostriedku sa vždy musí posudzovať v kontexte zásady voľného hodnotenia dôkazov. Dôkazy súd musí hodnotiť vždy samostatne resp. vo vzájomných súvislostiach. Na základe uvedených skutočností je možné jednoznačne tvrdiť, že ani takto zaobstarané dôkazy nemajú vyššiu právnu silu v priamom porovnaní s inými inak získanými dôkazmi resp. dôkazovým materiálom. Jedine súd má právo hodnotiť dôkazy a vo svojom odôvodnení rozsudku je povinný sa k nim vyjadriť.

Je dôležité spomenúť, že už vyhotovený prepis komunikácie ktorý sa zakladá do spisu už nepodlieha utajeniu. Tu sa uplatňuje výnimka a to v miestach, ak by informácie zaznamenané v prepise komunikácie obsahovali štátom chránené tajomstvo. Tieto informácie musia zostať utajené v zmysle zákona. V určitých prípadoch je možné predložiť súdu záznam aj bez vyhotoveného, resp. existujúceho prepisu. Tieto prípady však musia byť dostatočne odôvodňujú. V prevažnej väčšine prípadov ide o prípady, kedy je dôvodom časová tieseň. Prepis vyhotoveného zá-

[8] BURDA, E. Nezákonne získaný dôkaz. In Zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou na tému Teoretické a praktické problémy dokazovania, FP PEVŠ, z roku 2008, s. 27.

znamu nie je potrebný ani v prípade, ak je záznam na toľko jednoznačný a zrozumiteľný, že by samotný prepis strácal na význame v prípade využitia v trestnom konaní. Aj keď nie je vyhotovený prepis záznamu, tak je potrebné k samotnému záznamu pripojiť identifikačné údaje dotknutých osôb. Je na mieste tvrdiť, že v súlade s intenzitou zásahu do osobných práv jednotlivca, má každá osoba právo na ochranu proti neoprávnenému zásahu do svojich práv. V tomto prípade je to samozrejmé, pretože už len samotná povaha vykonávaných opatrení predstavuje veľmi významný zásah do osobných práv. Táto ochrana vyplýva každému jednotlivcovi z Ústavy Slovenskej republiky, rovnako ako z množstva medzinárodne uznaných a ratifikovaných dokumentov, ktorými je Slovenská republika právne viazaná.

Vo vnútroštátnej právnej úprave existuje možnosť domáhať sa ochrany svojich práv súdnou cestou prostredníctvom príslušného súdu. Tým je v týchto prípadoch Najvyšší súd Slovenskej republiky. V súvislosti s ochranou tohto práva, je možné vnímať určité problémy. Osoba, voči ktorej bol použitý informačný prostriedok je o tomto použití informovaná z taktického hľadiska až po ukončení vykonávania záznamu. Zo zákona táto informačná povinnosť prislúcha konkrétnemu orgánu. Zákonodarca to týmto spôsobom ustanovil preto, aby bola každej osobe zaručená možnosť súdnou cestou žiadať ochranu svojich práv. Trestný poriadok vo svojom znení predpokladá, že v prípade, ak nebudú zistené také skutočnosti, ktoré majú vplyv na trestné konanie, tieto sa musia bezodkladne zničiť. Následne je potrebné informovať konkrétne osoby, že bol voči nim použitý konkrétny informačno-technický prostriedok. Táto informačná povinnosť spadá pod orgány činné v trestnom konaní. Informačná povinnosť existuje iba v prípade, že sa vyhotovením záznamu nezistia skutočnosti významné pre trestné konanie a zároveň týmto osobám neprináleží právo nahliadania do spisu resp. spisového materiálu. Touto podmienkou sa radikálne znižuje počet subjektov, ktoré majú toto právo. Akou cestou sa napríklad môže domáhať ochrany osoba, ktorá je v pravidelnom dennom styku s osobou voči ktorej je využívaný vyššie spomenutý informačný prostriedok ?

Takáto osoba nemá právo nahliadať do spisu, teda orgány činné v trestnom konaní nemajú povinnosť ju informovať. Pritom bolo zasiahnuté do jeho práv v určitom rozsahu a to bez potrebnej diskusie. Táto osoba nie je teda ani podozrivou osobou ani ňou nebude. Navyše, sa na základe získaných informácii zvolí konkrétny procesný postup, takže tieto informácie mali preukázaný význam pre trestné konanie. Akým spôsobom sa ona môže domáhať svojich práv? Rovnako vágne ustanovenie nachádzame v trestnom poriadku pod tým, čo zákonodarca označuje ako skutočnosti, ktoré nie sú pre trestné konanie dôležité. Zákonodarca nám nikde v Trestnom poriadku ani v iných normatívnych právnych aktoch nedáva odpoveď, čo sú to tie skutočnosti, ktoré nie sú pre trestné konanie dôležité. Možno diskutovať, či sú to informácie ktoré svedčia o jednoznačnej nevine osoby voči ktorej sú využívaní spomenuté informačno-technické prostriedky, alebo sú to informácie ktoré nevinu naznačujú? Alebo informácie, ktoré žiadnym spôsobom nemajú možnosť preukázať akúkoľvek protiprávnu aktivitu sledovanej osoby? Ani na tieto otázky nám zákonodarca nedáva vo svojich ustanoveniach tak v Trestnom poriadku alebo v iných právnych aktoch odpovede. Tieto ustanovenia by bolo vhodné v čo najkratšom čase zmeniť. Zmenu môžeme odôvodniť stavom, že aj keď orgány činné v trestnom konaní nezískajú prostredníctvom vykonaného záznamu informácie, ktoré sú relevantné pre trestné konanie a svedčia o vine páchateľa, zistia mnohé iné informácie, na základe ktorých je možné ďalej zvoliť procesný postup. Možno na základe nich napríklad odmietnuť trestné stíhanie, zastaviť už existujúce a podobne. V zmysle medzinárodnej judikatúry je potrebné zmeniť toto ustanovenie, lebo na základe vyššie uvedených skutočností, majú všetky osoby, voči ktorým sa takýto prostriedok použil právo na súdnu ochranu svojich práv.

Záver

Informačno-technické prostriedky v demokratickej spoločnosti predstavujú a aj budú predstavovať priestor pre diskusiu. Diskusiu na odbornej a rovnako aj laickej verejnosti. Práve povaha informačno-technických prostriedkov je dôvod, prečo pojem informačno-technických prostriedkov predstavuje zložitú oblasť v problematike Trestného práva. Verejnosť v demokratickej spoločnosti veľmi citlivo reaguje na zásahy do súkromia každého jednotlivca. Povaha informačno-technických prostriedkov v trestnom konaní zasahuje do vyššie spomínaných práv na súkromie obyvateľstva. Nebyť problematickej minulosti, ktorú si najmä starší obyvatelia stále pamätajú, možno by tomu bolo inak. Povaha informačno-technických prostriedkov, predurčuje informačno-technické prostriedky na využitie spravodajským spôsobom. To znamená, že jednotlivec nemá vedomosť o využívaní týchto prostriedkov a najmä, že mu štát zasahuje do jeho osobných práv. V praxi to teda znamená konflikt medzi záujmom jednotlivca, ktorý je považovaný za základnú bunku spoločnosti a na druhej strane záujmom spoločnosti na odhaľovaní trestnej činnosti v tých najzávažnejších formách. Práve odhaľovanie a trestane trestných činov sa všeobecne pokladá za jeden zo základných prvkov demokratického zriadenia štátu. Vyriešiť tento konflikt medzi záujmom spoločnosti a jednotlivcom sa snaží zákonodarca v citlivom znení konkrétnych ustanovení, ktoré sa venujú danej problematike. Na jednej strane tvrdíme, že trestné činy treba veľmi dôsledne odhaľovať a trestať, na druhú stranu treba zvážiť intenzitu zásahu do konkrétnych práv jednotlivca. Záujmom zákonodarcu je jednoznačne vytvoriť určitú právnu rovnováhu. Prispieva k tomu veľmi dôslednou zákonnou špecifikáciou tak trestných činov, pri ktorých je použitie jednotlivých informačno-technických prostriedkov možné, ako aj nastavením podmienok procesného postupu orgánov činných v trestnom konaní.

Práve vytvorenie prísnych podmienok má za následok, že informačno-technické prostriedky bývajú využívané v praxi účelne a vecne a vo veľkej miere prispievajú k odhaľovaniu najzávažnejších foriem trestnej činnosti. Práve stupeň organizovanosti a sofistikovanosti trestnej činnosti je javom, ktorý jednoznačne prispieva k tomu, že verejnosť pri odhaľovaní týchto foriem trestnej činnosti pristupuje kladne k využitiu informačno-technických prostriedkov.

Literatúra

1. IVOR, J.: *Obrazovo-zvukový záznam*, In Zborník príspevkov z vedeckej konferencie na tému *Teoretické a praktické problémy dokazovania*, z roku 2008
2. Zákon č. 460/1992 Z. z. Ústava Slovenskej republiky
3. Zákon č. 40/1964 Zb. Občiansky zákonník
4. POLÁK, P., TALAPKA, M.: Prípustnosť využitia dôkazov získaných použitím informačno-technických prostriedkov pre účely trestného konania, In Zborník príspevkov z medzinárodnej konferencie na tému *Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní.* Bratislava, FP PEVŠ, 2017
5. BURDA, E.: Nezákonne získaný dôkaz, In Zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou na tému *Teoretické a praktické problémy dokazovania.* Bratislava, FP PEVŠ, 2008.

Odpočúvanie a záznam telekomunikačnej prevádzky v trestnom konaní[1]

Listening and Recording of Telecommunications Traffic in Criminal Proceedings

Filip Korček[2]

Abstrakt: *Príspevok sa zaoberá témou v súčasnej dobe veľmi aktuálnou a síce právu na súkromie a odpočúvaniu a záznamu telekomunikačnej prevádzky. Autor najskôr rozoberá právo na súkromie z pohľadu vnútroštátneho, medzinárodného i práva Európskej únie. Ďalej je v práci rozobratá súčasná právna úprava odpočúvania a záznamu telekomunikačnej prevádzky v SR. V neposlednom rade sa príspevok zaoberá aplikačnou praxou vrátane veľmi zaujímavej problematiky použitia záznamov vytvorených mimo trestného konania súkromnými osobami v rámci trestného konania.*

Abstract: *The paper deals with the topic of the very current, namely the right to privacy and listening and recording of telecommunication traffic. The author first discusses the right to privacy from the perspective of national, international and European Union law. Furthermore, the thesis discusses the current legal regulation of interception and recording of telecommunications in the Slovak Republic. Last but not least, the paper deals with application practice, including the very interesting issue of using records created outside criminal proceedings by private individuals in criminal proceedings.*

Kľúčové slová: *súkromie, odpočúvanie, trestné konanie.*

Key words: *privacy, interception, criminal proceedings.*

Právo na súkromie

Ide o právo nemajetkovej povahy, ktoré prof. JUDr. Ján Svák, DrSc. vymedzuje ako zákaz zhromažďovania a úschovy osobných údajov, právo spojené s menšinovou sexuálnou orientáciou, právo na ochranu dobrého mena a cti, ochranu obydlia a domovej slobody, ochranu korešpondencie a tajomstva dopravovaných správ a právo na ochranu životného prostredia.[3]

Právo na súkromie a nerušený výkon tohto práva, rovnako ako jeho ochrana musí byť garantované štátom. Účelom Ústavou priznaného práva na súkromie je zabrániť štátnym orgánom i orgánom územnej samosprávy, aby zasahovali do správania jednotlivca nad nevyhnutnú mieru a príliš neprimerane riadili jeho súkromný život.[4]

V právnej literatúre je možné sa stretnúť s negatívne a pozitíve vymedzením záväzku štátu pri ochrane práva na súkromie.[5] Negatívny záväzok štátu spočíva v povinnosti obmedziť zásahy do práva na súkromie, zatiaľ čo pozitívny záväzok štátu spočíva v povinnosti vytvoriť také podmienky, ktoré by znemožňovali porušenia práva na súkromný život. Tieto dva záväzky mu-

---

[1] Príspevok vznikol v rámci Konferencie“ Informačno-technické prostriedky v trestnom konaní – možnosti a perspektívy“ organizovanou FP PEVŠ 4. 4. 2019.

[2] JUDr. Filip Korček, LL.M., Katedra trestného práva a kriminológie Právnickej fakulty Trnavskej univerzity v Trnave, e-mail: fkorcek@centrum.sk.

[3] Svák, J., Ochrana ľudských práv v troch zväzkoch. II. zväzok. Žilina: Eurokódex, 2011, s. 425.

[4] II. ÚS 94/95 C. 10/95 dostupné dňa 29. 12. 2013.

[5] Leander v. Švédsko a Gaskin v. Spojené kráľovstvo.

sia byť rešpektované pri prijímaní akejkoľvek právnej úpravy, resp. pri výkone zásahu do tohto práva.[6]

V článku 13 tohto ústavného zákona č. 23/1991 Zb. je zároveň ustanovené že „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." Toto ustanovenie úzko korešponduje s odpočúvaním a záznamom telekomunikačnej prevádzky ako výrazným zásahom do tohto Ústavným zákonom garantovaného práva. V súvislosti s čl. 13 Listiny sa napr. Ústavný súd Českej republiky vyslovil, že čl. 13 Dohovoru chráni nie len vlastný obsah telekomunikácie, ale tiež aj všetky súvisiace údaje, ako napríklad dátum a čas hovoru, údaje o volaných číslach, o dobe trvania, informácie o základných staniciach, ktoré zaisťujú hovor, alebo iné, ktoré je možné považovať za neoddeliteľnú súčasť tohto obsahu.

Nakoľko je Slovenská republika členom Európskej únie významnú ochranu práva na súkromie poskytuje jednak primárne právo Európskej únie, jednak rozhodnutia Súdneho dvora. Najvýznamnejším dokumentom upravujúcim ľudské práva a medzi nimi aj práva na súkromie v Európskej únii je Charta základných práv Európskej únie, ktorá v článku 8 uvádza že „Každý má právo na rešpektovanie svojho súkromného a rodinného života, obydlia a komunikácie."Charta sa zároveň stala primárnym prameňom práve Európskej Únie preto je na území Slovenskej republiky právne záväzná. Mimo Charty základných práv Európskej únie a Zmluvy o fungovaní Európskej únie (ďalej len „ZFEU") je potrebné v súvislosti s odpočúvaním a záznamom telekomunikačnej prevádzky potrebné spomenúť smernicu 95/46/EHS o ochrane fyzických osôb v súvislosti so spracovaním osobných údajov a o voľnom pohybe týchto údajov, ktorá významne prispela k ochrane osobných údajov v SR transpozíciou tejto smernice do právneho poriadku SR. Takisto v sekundárnom práve nachádzame množstvo odkazov a úpravu rôznych aspektov ktoré súvisia s úpravou odpočúvania a záznamu a telekomunikačnej prevádzky. Napríklad smernica Európskeho parlamentu a Rady 2011/92/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii. Subjektom zodpovedným za vyšetrovanie a trestné stíhanie trestných činov uvedených v tejto smernici by mali byť poskytnuté efektívne nástroje vyšetrovania. Tieto nástroje by mohli zahŕňať odpočúvanie, utajené sledovanie vrátane elektronického sledovania, monitorovania bankových účtov alebo iné finančné vyšetrovanie, pričom sa okrem iného zohľadní zásada proporcionality a povaha a závažnosť vyšetrovaných trestných činov.

Súčasná právna úprava odpočúvania a záznamu telekomunikačnej prevádzky

„Odpočúvanie je zámerné a utajované vnímanie obsahu komunikácie sprostredkované telekomunikačnými zariadeniami alebo sieťami prostredníctvom k tomu určenými zariadeniami."[7] Za odpočúvanie teda nie je možné považovať náhodné dopočutie konverzácie pri vedľajšom stole, alebo dvoch vo vedľajšej miestnosti komunikujúcich osôb za predpokladu, že k tomu neboli využité informačno-technické prostriedky.

Záznamom je súbežne zachytený obsah komunikácie na nosičoch záznamu umožňujúci ich uchovanie a reprodukciu. Definícia pojmu telekomunikačná prevádzka chýba napriek tomu,

[6] Čentéš, J. Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. Bratislava: C. H. Beck, 2013, s. 9 – 15.

[7] Musil, J., Kratochvíl, V., Šámal, P. Kurs trestního práva, Trestní právo procesní. Praha: C. H. Beck, 2003, s. 358.

že sa tento pojem aj v zákonoch často používa. Preto je potrebné si pri výklade tohto pojmu pomôcť právnou literatúrou resp. komentárom k Trestnému poriadku Telekomunikačnou prevádzkou je spojenie zabezpečované prostredníctvom telefónu, telefaxu, mobilných telefónov, vysielačiek a iných telekomunikačných zariadení využívajúcich napríklad modem (zasielanie správ elektronickou poštou).

Definícia telekomunikačnej prevádzky je nasledujúca: Činnosť telekomunikačných zariadení (napr. telefónov, rádiostaníc, počítačových sietí atď.), ktorá spočíva v preprave alebo smerovaniu ako obsahu komunikácie (napr. hovorov alebo písomných správ), tak i súvisiacich prevádzkových údajov (napr. sprievodných dát identifikujúcich určité účastnícke stanice, dátum, čas zahájení, dobu trvania, poprípade čas ukončenia súvisiacich činnosti účastnícke adresy, prístupový bod siete, výpis aktívneho a pasívneho volania.

Hlavným prameňom úpravy odpočúvania a záznamu telekomunikačnej prevádzky v trestnom konaní na Slovensku je zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov. Tento inštitút vymedzuje v § 115 a § 116. pod názvom „Odpočúvanie a záznam telekomunikačnej prevádzky." Kým v § 115 je upravený postup a realizácia odpočúvania ktoré sa uskutoční v budúcnosti, § 116 upravuje možnosť vydať príkaz na zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke.

Zákonnými podmienkami pre aplikáciu inštitútu odpočúvania a záznamu telekomunikačnej prevádzky tak ako je uvedená v Trestnom poriadku sú: **existencia trestného konania**, **existencia trestného činu** taxatívne vymedzeného v § 115 ods. 1. Trestného poriadku a **dôvodný predpoklad** zistenia skutočností významných pre trestné konanie.

Trestné konanie je vymedzené podľa § 10 ods. 15 Trestného Poriadku ako konania podľa tohto zákona, trestné stíhanie ako konanie od začatia trestného stíhania až do právoplatnosti rozsudku. Trestné konanie je základnou zákonnou podmienkou pre možnosť použitia inštitútu odpočúvania podľa Trestného poriadku. Jedná sa o podmienku, ktorej nenaplnenie vylučuje možnosť využitia tohto inštitútu. Trestné konanie začína spravidla podaním oznámenia o skutočnostiach, že bol spáchaný trestný čin. Je teda možné zvažovať využite odpočúvania aj vo fáze postupu pred začatím trestného stíhania, ako aj vo fáze trestného stíhania. Vo fázach pred trestným stíhaním sa využije najmä pri odhaľovaní obzvlášť závažnej trestnej činnosti. V praxi ide o inštitút, ktorý je často využívaný.

Existencia taxatívne vymedzeného trestného činu ja ďalšou podmienkou, ktorá musí byť naplnená, súčasne s vyššie uvedenými. Trestný poriadok okrem taxatívne vymedzených trestných činov, ktorými sú korupcia, trestný čin zneužívania právomoci verejného činiteľa, trestný čin legalizácie príjmu z trestnej činnosti ďalej odkazuje na trestné činy, o ktorých na konanie zaväzuje medzinárodná zmluva. Takéto vymedzenie trestných činov je koncipované značne široko a k jeho správnemu posúdeniu je potrebné pracovať s veľkým množstvom medzinárodných zmlúv a dohovorov ktorých je Slovenská republika signatárom. Zároveň takéto vymedzenie nie je uzatvorené a môžu pribúdať nové trestné činy, na ktoré je možné aplikovať inštitút odpočúvania. Na skúmanie platných medzinárodných zmlúv ku dňu začatia odpočúvania, preto nemožno zabudnúť pri preskúmavaní zistiť, či odpočúvanie prebehlo na základe podmienok stanovených zákonom.

Ďalším zákonným predpokladom na vydanie príkazu na odpočúvanie a záznam telekomunikačnej prevádzky je dôvodný predpoklad, že budú zistené skutočnosti významné pre trestné konanie. Pri vydaní príkazu na odpočúvanie súd nemôže mať istotu, že skutočnosti významné pre trestné konanie budú aj naozaj zistené. Vyplýva to zo samotného charakteru odpočúvania, ako i zo správania a obozretnosti odpočúvaných osôb. Dôvodnosť takéhoto predpokladu je možné vyvodiť napr. z trestnej činnosti, ktorá vyžaduje koordinovanú spoluprácu páchateľov alebo zo

samotného charakteru trestnej činnosti. To či takýto dôvodný predpoklad existuje, skúma súd pred vydaním príkazu na odpočúvanie, nakoľko jeho neexistencia by použitie inštitútu odpočúvania vylučovala.

Nesplnenie týchto základných podmienok má za následok nezákonnosť takto vykonaného odpočúvania a prípadnej nemožnosti použiť takto získané údaje ako dôkaz v trestnom konaní. „Dotknutá osoba, ktorej rozhovor bol takto odpočúvaný, môže v trestnom konaní pred súdom namietať nezákonnosť odpočúvania a z toho vyplývajúcu nepoužiteľnosť odpočúvaného rozhovoru ako dôkazu. Môže však tak urobiť len pri súčasnom splnení dvoch podmienok: trestná vec musí dospieť do štádia súdneho konania a dotknutá osoba musí byť stranou v trestnom konaní či už ako obžalovaná, alebo ako poškodená[8]

Aplikačná prax

V trestnom konaní vykonáva odpočúvanie a záznam telekomunikačnej prevádzky príslušný orgán policajného zboru. V súčasnosti je takýmto orgánom Úrad zvláštnych policajných činností Prezídia policajného zboru.

Pri takomto použití zvukového záznamu zaobstaraných súkromnou osobou je potrebné zvážiť najmä kolíziu chránených práv.

Vzhľadom k skutočnosti, že jediným procesným predpisom, ktorý upravuje možnosti použitia odpočúvania v trestnom konaní je Trestný poriadok, je na mieste otázka, do akej miery je prípustné použiť odpočúvanie vykonané inou osobou ako Policajným orgánom. Napr. súkromnou osobou, ktorá si predmetný rozhovor nahrala.

Nahrávanie hovoru volajúcim je dnes už technicky ľahko dostupné a v praxi sa čoraz častejšie vyskytujú takéto prípady. Podľa § 12 zákona č. 40/1964 Zb. Občiansky zákonník sa

„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.“ Je preto potrebné pre vyhotovenie a použitie vyžiadať si súhlasy dotknutej osoby, ku každému takémuto úkonu, resp. zo súhlasu tejto osoby musí byť zrejmé, že sa takýto jej súhlas viaže k obom týmto úkonom. V prípade, že osoba takýto súhlas nevydá prichádza do úvahy zodpovednosť práve podľa občianskeho zákonníka.

Zaujímavá situácia nastáva v prípade, že má byť takýto záznam vyhotovený súkromnou osobou použitý ako dôkaz v trestnom konaní. V prípade, že bol takýto záznam vyhotovený súkromnou osobou so súhlasom druhej osoby, mám za to že použitie takéhoto dôkazu v trestnom konaní by prostredníctvom § 119 ods. 2. zákona č. 301/2005 Z. z. Trestný poriadok bolo bezproblémové,(viď nižšie). Čo ale v prípade, že takýto súhlas druhej osoby nebol udelený. Uznesenie NS České republiky sp. zn. 5 Tdo 459/2007 zo dňa 30. 5. 2007, hovorí, že nie je možné vylúčiť možnosť, aby bol ako dôkaz použitý zvukový záznam, ktorý bol vyhotovený súkromnou osobou bez súhlasu osôb, ktorých hlas je takto zaznamenaný. Takto definované využitie odpočúvania je ale koncipované značne široko, a preto je potrebné ku každému takémuto prípadu pristúpiť s veľkou obozretnosťou. Táto skutočnosť sa v praxi vyskytuje čoraz častejšie, na koľko prístroje a mobilné zariadenia, ktoré sú v súčasnosti bežne dostupné, umožňujú nahrávať si svoje hovory s inými osobami.

Akékoľvek odpočúvanie a záznam telekomunikačnej prevádzky mimo trestného konania vykonaný podľa zákona je možné použiť ako dôkaz v trestnom konaní, na koľko § 119 ods. 2. zákona č. 301/2005 Z. z.. Trestný poriadok umožňuje použitie ako dôkazu všetkého čo môže pris-

[8] IV. ÚS 216/2013.

pieť k objasneniu veci. Musí ale ísť o záznam, ktorý bol získaný podľa špeciálneho zákona a musí byť splnený predpoklad, že tieto špeciálne zákony budú ústavne komfortné vo vzťahu k podmienkam za ktorých bude toto odpočúvanie realizované. Existuje dva rôzne prístupy pri výklade toho, čo sa rozumie „z dôkazných prostriedkov podľa tohto zákona, alebo podľa osobitného zákona." Užším výkladom sa dostaneme k formulácii, že pôjde len o taký zákon, ktorý na možnosť použitia ako dôkazu v trestnej veci priamo odkazuje. Napríklad ako zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov v § 7 ods. 2.. Aplikáciou širšieho výkladu naopak prídeme k výkladu, že v § 119 ods. 2 zákona č. 301/2005 Trestný poriadok sa myslí akýkoľvek zákon, ktorý upravuje odpočúvanie a záznam telekomunikačnej prevádzky bez ohľadu na to či na použitie záznamu takejto komunikácie ako dôkazu v trestnej veci priamo odkazuje. Ťažko dedukovať úmysel zákonodarcu, či k spojeniu „podľa osobitného zákona" pristúpil zámerne a myslel tým účelovo pojem odlišný od pojmu „iného zákona". Takéto vysvetlenie neposkytuje ani dôvodová správa k tomuto zákonu. V tomto prípade sa prikláňam k jazykovo-gramatickému užšiemu výkladu, nakoľko k slovu osobitný sa viaže nejaký zvláštny, špeciálny význam, čo by v tomto prípade mohlo odkazovať na zákony, ktoré na použite záznamu ako dôkazu priamo odkazujú. Pre tento výklad svedčí aj argument, že zákonodarca mohol použiť pojem „iný zákon" napriek tomu zvolil formuláciu osobitný

Právo na súkromie má úzky súvis s judikatúrou Európskeho súdu pre ľudské práva (ďalej len „ESĽP") Vo svojej judikatúre ESĽP postupne upúšťal od veľmi prísneho a striktného výkladu, že štátne orgány nesmú do práva na súkromie zasahovať a postupne sa prikláňal k legálnosti zásahov do tohto práva za splnenia podmienky, že právne úpravy stanovia podrobné a presné rámce, ako aj limity týchto zásahov.

Zlomovým sa v tejto oblasti javí rozsudok Klass a iní vs. Nemecko, v ktorom sťažovatelia uviedli, že tajné sledovanie v trestnej veci orgánmi je zásahom do ich práve. Súd vyslovil názor ad. 1: že telefonický rozhovor je súčasťou pojmu „korešpondencia" a „súkromný život." a ad. 2: vyhlásil, že nemecké predpisy, ktoré upravujú dohľad, sú dostatočne presné, a postupy, ktoré majú zabezpečiť, aby všetky opatrenia pri sledovaní boli v súlade s podmienkami zákona, sú dostatočne striktné a teda v súlade s požiadavkou zákonnosti v článku 8 ods. 2. Súd takisto vyhlásil, že potreba štátu chrániť spoločnosť pred „bezprostredným nebezpečenstvom" ohrozujúcim „slobodný demokratický ústavný poriadok", je legitímnym cieľom štátu zodpovedajúcim ustanoveniam „nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti (a) predchádzania nepokojom a zločinnosti". Súd napokon konštatoval, že uvedené postupy boli adekvátne z hľadiska záruk, že každý postup štátu bude primeraný týmto legitímnym cieľom

Súd tento svoj názor potvrdil a ďalej rozviedol aj v prípade Malone vs. Spojené kráľovstvo, kde konštatuje, že zákon by bol v rozpore s ideou právneho štátu, ak by oprávnenie postupovať podľa voľnej úvahy, ktoré sa poskytuje výkonnej moci, nemalo svoje medze. Práve preto zákon musí definovať rozsah takejto úvahy príslušných orgánov, ako aj spôsob výkonu tohto oprávnenia dostatočne jasne, s prihliadnutím na legitímny ciel príslušného opatrenia a tak, aby poskytol jednotlivcovi náležitú ochranu pred svojvoľnými zásahmi.

V prípade Kopp vs. Švajčiarsko dospel ESĽP k názoru, že ustanovenia vnútroštátnych predpisov, ktoré poskytujú možnosť zásahu do základných práv, musia byť jasné, presné z hľadiska rámca, limitov a tiež musia obsahovať primerané garancie ochrany[9]

Taktiež treba spomenúť judikáty ESĽP Leander v. Švédsko a Gaskin vs. Spojené kráľovstvo v ktorých bolo vymedzený negatívny a pozitívny záväzok štátu v rámci zásahu do práva na súkromie.

[9] Prípad Kopp vs. Švajčiarsko.

Ako prvý by som chcel uviesť judikát I. ÚS 274/05 v ktorom Ústavný súd konštatoval, že odpočúvania a záznam telekomunikačnej prevádzky je závažným zásahom do práva na súkromie a to nie len osoby, ktorá je odpočúvaná ale i do práv osôb, ktoré s touto osobou komunikujú.

Ďalej spomeniem judikáty Uznesenie Najvyššieho súdu SR sp. zn. 3 To 2/2011 zo dňa 21. 9. 2011 a Rozsudok Najvyššieho súdu SR sp. zn. 2 To 5/2011 zo dňa 7. 2. 2012 v ktorých sa NS SR vyjadril v dvoch rovnakých veciach úplne rozdielne, čím vytvoril nežiaduci právny stav, ktorý sa snažilo vyriešiť trestnoprávne kolégium NS SR v roku 2012, no k rozdielnym výkladom slova „súčasne" nezaujal stanovisko.

Významným sa javí aj rozhodnutie NS Českej republiky sp. zn. 5 Tdo 459/2007 zo dňa 30. 5. 2007, ktoré hovorí, že nie je možné vylúčiť možnosť, aby bol ako dôkaz použitý zvukový záznam, ktorý bol vyhotovený súkromnou osobou bez súhlasu osôb, ktorých hlas je takto zaznamenaný. Táto skutočnosť je významná najmä pre dokazovanie v trestnom konaní a tiež súvisí s § 119 ods. 2 zákona č. 301/2005 Z. z. Trestný poriadok.

Pre účely dokazovania v trestnom konaní sa javí aj nález Ústavného súdu ČR sp. zn. IV. ÚS 1235/09 zo dňa 14. 7. 2010 určil, že pokiaľ dôkaz, resp. informácia ktorú obsahuje, nebol získaný čo do jednotlivých fáz procesu dokazovania prípustným spôsobom, musí byť súdom vylúčený z predmetu úvah smerujúcich k zisteniu skutkového základu vecí.

Literatúra

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

Musil, J., Kratochvíl, V., Šámal, P. Kurs trestního práva, Trestní právo procesní. Praha: C. H. Beck, 2003

Svák, J. Ochrana ľudských práv v troch zväzkoch. II. zväzok. Žilina: Eurokódex, 2011

Leander v. Švédsko

Gaskin v. Spojené kráľovstvo

Kopp vs. Švajčiarsko

II. ÚS 94/95 C. 10/95 dostupné dňa 29. 12. 2013

IV. ÚS 216/2013

Oznámenie o odpočúvaní a zničenie záznamu telekomunikačnej prevádzky[1]

Notice of Interception and Destruction of Telecommunication Service Records

Monika Šebestová - Širilová[2]

Abstrakt: *Tento príspevok sa venuje problematike oznámenia a následného zničenia záznamu telekomunikačnej prevádzky, ktoré možno zaradiť medzi „spôsoby" slúžiace na kontrolu uplatňovania informačno-technických prostriedkov vyžadovanú Dohovorom o ochrane ľudských práv a základných slobôd. Uvádzané spôsoby možno označiť za jedny z najnevyhnutejších elementov, ktoré sú uplatňované pri používaní informačno-technických prostriedkov, nakoľko práve oni majú za účel zabrániť zneužitiu informačno-technickým prostriedkov a dávajú možnosť príslušnému subjektu brániť sa súdnou cestou proti zásahu vykonanému v rozpore s príslušnými ustanoveniami Trestného poriadku ako aj Dohovoru o ochrane ľudských práv a základných slobôd.*

Abstract: *This article concentrates on issue of the notice of interception and following destruction of telecommunication service records, which shall be subsumed among "methods" used for control of application of the information-technical means required by the Convention for the Protection of Human Rights and Fundamental Freedoms. Stated methods may be labelled to be one of the most necessary elements applied during the process of using of the information-technical means, however they shall prevent the abusion of the information-technical means and give to the respective subject the option to defend himself by the legal action before interference in contrary with the relevant provisions of the Criminal procedure and as well as Convention for the Protection on Human Rights and Fundamental Freedoms.*

Kľúčové slová: *informačno-technické prostriedky, Dohovor o ochrane ľudských práv a základných slobôd, Trestný poriadok, zničenie záznamu telekomunikačnej prevádzky, oznámenie o odpočúvaní.*

Key words: *information-technical means, Convention for the Protection on Human Rights and Fundamental Freedoms, Criminal procedure, destruction of telecommunication service records, notice of interception.*

Úvod

Z hľadiska členenia zákona č. 301/2005 Z. z. Trestného poriadku (ďalej len „TP") je trestno-procesný inštitút „*Odpočúvanie a záznam telekomunikačnej prevádzky*", upravený v § 115 piatej hlavy TP, ktorá má názov zabezpečovanie informácií.

Je absolútne nepochybné, že spomínaný trestno-procesný inštitút upravený v § 115 TP patrí v súčasnosti jednoznačne medzi nenahraditeľné a najúčinnejšie nástroje používané zo strany orgánov činných v trestnom konaní a súdov v boji proti sofistikovaným páchateľom terorizmu, korupcii, ako aj organizovaným a zločineckým skupinám. Protispoločenská a trestná činnosť na území Slovenskej republiky je prepojená s finančnými a politickými subjektmi ako na organizačnej, tak aj na personálnej báze. Je nepochybné, že prienik do takýchto štruktúr je zložitý a odhaľovaniu tejto činnosti vo veľmi značnej miere pomáhajú práve informačno-technické prostriedky. Využitie informačno-technických prostriedkov pri odhaľovaní trestnej činnosti býva častokrát predmetom rôznych diskusií, či už na politickej, technickej alebo dokonca laickej

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

[2] Mgr. Monika Šebestová-Širilová, MLA, Fakulta práva Paneurópskej vysokej školy, Tomášikova 20, Bratislava, monika.sirilova@centrum.sk.

úrovni. Nakoľko použitie informačno-technického prostriedku je veľmi špecifické, nesie v sebe riziko jeho zneužitia na iné účely, ako tie, ktoré sú povolené platnými právnymi predpismi. Na to aby nedochádzalo ku ich zneužívaniu nám slúžia rôzne kontrolné mechanizmy, ako aj personálne zabezpečenie, ktoré je v kompetencii oprávnených subjektov.[3]

Použitím tohto trestno-procesného inštitútu zvereného útvarom Policajného zboru, ktorý disponuje osobitnými, na to skonštruovanými, zariadeniami, ktoré umožňujú odpočúvanie a zaznamenávanie telekomunikačnej prevádzky sa získavajú priame, usvedčujúce dôkazy o skutkových okolnostiach dôležitých pre trestné konanie. Samozrejme je nevyhnutné neopomenúť, že týmito prostriedkami disponujú a používajú ich aj zložky štátu ako orgány Finančnej správy, Zbor väzenskej a justičnej stráže alebo Slovenská informačná služba s tým, že ich použitie zabezpečuje Policajný zbor. V zmysle § 2 ods. 2 zákona č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov informačno-technické prostriedky môže používať Policajný zbor, Slovenská informačná služba, Vojenské spravodajstvo, Zbor väzenskej a justičnej stráže a Colná správa. Pritom v zmysle § 2 ods. 3 a 4 zákona č. 166/2003 Z. z. odpočúvanie a záznam telekomunikačnej prevádzky technicky zabezpečuje Policajný zbor aj pre Colnú správu, Vojenské spravodajsto a Zbor väzenskej a justičnej stráže. Zo samotnej povahy hore uvádzaných informácii vyplýva, že pri použití inštitútu upraveného v § 115 TP dochádza k výraznému stretu so základnými ľudskými právami. Pri nasadzovaní a použití skrytých odpočúvacích zariadení sa výrazne značným spôsobom zasahuje do práva na súkromný život. Ochrana súkromia je upravená vo viacerých článkoch Ústavy Slovenskej republiky[4] (ďalej len „Ústava") a Listiny základných práv a slobôd (ďalej len „Listina"). Dohovor o ochrane ľudských práv a základných slobôd (ďalej len „Dohovor") sústreďuje úpravu ochrany práva na súkromie do článku 8. Je nevyhnutné podotknúť, že Ústavný súd Slovenskej republiky už v minulosti viackrát judikoval, že základné práva, ktoré sú obsiahnuté v Ústave, vykladá v súlade s Dohovorom, ako aj judikatúrou Európskeho súdu pre ľudské práva v Štrasburgu.[5]

Osoba v konaní pred Ústavným súdom, môže namietať porušenie článku 22 Ústavy a článku 13 Listiny a článok 8 ods. 1 a ods. 2 Dohovoru v súvislosti s tým, že súdy použili nelegálne získaný záznam ako dôkaz v trestnom konaní, čím došlo k neoprávnenému zásahu do práva na súkromie. V uvádzanom prípade by takéto použitie záznamu bolo absolútne bezdôvodné a v rozpore s platnými a všeobecne záväznými právnymi predpismi, upravujúcimi použitie informačnom-technických prostriedkov. Treba si predovšetkým uvedomiť, že použitím informačno-technického prostriedku v mnohých prípadoch, ako napríklad vykonaním použitia telefonického záznamu, sa nevykoná zásah len do práva na súkromie jednej osoby, ktorou je držiteľ telefónnej linky,[6] ale aj osôb, ktoré na túto linku telefonujú resp. túto linku na telefonovanie použili.[7]

---

[3] ZACHAR, A.: Informačno-technické prostriedky a možnosti ich používania na území Slovenskej republiky, Trestní právo, 09, 2008, s. 42.

[4] Ústavný zákon č. 460/1992 Zb. Ústava Slovenskej republiky, v znení č. 244/1998 Z. z., 9/1999 Z. z., 90/2001 Z. z., 90/2001 Z. z., 140/2004 Z. z., 323/2004 Z. z., 323/2004 Z. z., 463/2005 Z. z., 92/2006 Z. z., 210/2006 Z. z., 100/2010 Z. z., 356/2011 Z. z., 232/2012 Z. z., 161/2014 Z. z., 306/2014 Z. z., 427/2015 Z. z., 44/2017 Z. z., 71/2017 Z. z., 137/2017 Z. z.

[5] Nález Ústavného súdu Slovenskej republiky zo dňa 14. júna 2006 pod. sp. zn. I. ÚS 274/05.

[6] Ochrana tajomstva správ podávaných telefónom je súčasťou širšej kategórie, ktorou je ochrana súkromia. V zmysle judikatúry Súdu pre ľudské práva v Štrasburgu sa zásahy do práva na súkromie vykladajú v určitej logickej nadväznosti resp. postupnosti. V takýchto prípadoch sa predovšetkým skúma, či možno takýto skutkový stav „ratio materiae" považovať za súčasť práva na súkromie. Po kladnej odpovedi prichádza na rad skúmanie, či bol takýto zásah legálny. V ďalšom kroku sa skúma, či bol takýto vykonaný zásah legitímny, a napokon či bol proporcionálny. Negatívna odpoveď na niektorú z uvádzaných otázok znamená, že sa v skúmaní ďalej nebude pokračovať.

[7] Huvig a Kruslin v. Francúzsko z 24. apríla 1990.

Európsky súd pre ľudské práva opodstatňuje vykonanie zásahu do práva na súkromie dvoma okolnosťami: prvou je technický pokrok zaznamenaný vo vývoji špionážnych prostriedkov a aj v prostriedkoch kontrašpionážneho dohľadu, druhou okolnosťou je rozmach terorizmu v Európe. Práve rozvoj špionážnych prostriedkov a rozmach terorizmu spôsobuje, že sa demokratické zriadenia jednotlivýc štátov ocitajú v ohrození. Je absolútne racionálne odôvodniteľné, že pokiaľ majú štáty dostatočne, včasne a účinne predchádzať páchaniu takejto trestnej činnosti, musia mať zákonnú možnosť podrobiť uplatnením tajného dohľadu podozrivé živly pôsobiace vo sfére ich jurisdikcie. Samozrejme netreba zabudnúť, že v súlade s Dohovorom je výlučne len taký systém dohľadu, v ktorom existujú primerané a účinné záruky proti ich zneužitiu. Jednoducho povedané, použitím takýchto prostriedkov, nesmie byť vytvorená príležitosť pre podkopanie, alebo dokonca až zničenie demokratickej spoločnosti so zámienkou boja proti terorizmu či špionáži.[8]

Nakoľko sa má tento článok venovať problematike zničenia záznamu telekomunikačnej prevádzky a informovaniu subjektu o skutočnosti, že bola odpočúvaná, považujem za potrebné len okrajovo na záver tohto úvodu uviesť, že použitie informačno-technického prostriedku, je možné len vo vzťahu k určitému podozreniu, ktoré musí byť vymedzené-ohraničené skutkovými okolnosťami a odôvodnené tak, aby čo najviac znížilo riziko zneužitia. Zásahy vykonané do súkromia osôb zo strany štátnych orgánov bez súhlasu subjektu, ktorého sa takýto zásah týka, sú viazané na splnenie zákonmi špecifikovaných podmienok. Trestno-procesný inštitút upravený v § 115 TP, možno vykonať len na základe príkazu sudcu pre prípravné konanie, ktoré je rozhodnutím sui generis. Vo výnimočných prípadoch, ktoré neznesú odklad, môže byť takýto príkaz pred začatím trestného stíhania alebo v prípravnom konaní vydaný dozorujúcim prokurátorom s tým, že takýto príkaz musí byť do 24 hodín potvrdený zo strany sudcu pre prípravné konanie.[9] Netreba opomenúť, že zásah do práva na súkromie možno vykonať aj na základe zákona č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov (ďalej len „zákon o ochrane pre odpočúvaním"), pričom v takomto prípade sa takýto zásah do práva na súkromie deje na základe predchádzajúceho súhlasu zákonného sudcu, kde ide o tzv. rozhodnutie sudcu „sui generis".[10] Pripomínam, že ani voči jednému z rozhodnutí, ktorým sa vykonáva zásah do práva na súkromie, nie je prípustný opravný prostriedok.

K zničeniu záznamu získaného prostredníctvom informačno-technických prostriedkov

Po ukončení dôvodov, ktoré mali za následok použitie zariadení potrebných na zabezpečovanie informácií, zabezpečí spravidla orgán činný v trestnom konaní (policajt) prostredníctvom príslušného útvaru Policajného zboru odtajnenie a doslovný prepis z vyhovených záznamov. Laicky povedané, policajt požiada príslušný útvar Policajného zboru o ich „sprocesnenie". Uvedený postup vyplýva priamo zo znenia ustanovenia § 115 ods. 6 TP.[11] „V tejto súvislosti však treba

[8] Ústavný a zákonný rámec použitia informačno-technických prostriedkov štátnymi orgánmi. Justičná revue, 53, 2001, č. 10, s. 1019.

[9] Pozn. uvedene sa vzťahu na príkaz vydaný podľa TP.

[10] ZÁHORA, J.: Príkaz v trestnom konaní; Justičná revue, 56, 2004, č. 5.

[11] § 115 ods. 6. TP: „Ak sa má záznam telekomunikačnej prevádzky použiť ako dôkaz, treba k nemu pripojiť, ak to vyhotovený záznam umožňuje, doslovný prepis 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. 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

zdôrazniť, že ukončenie odpočúvania sa neviaže na posledný deň platnosti príkazu, resp. sa na tento deň viazať nemusí. Jediným a rozhodujúcim momentom z hľadiska ukončenia odpočúvania je skutočnosť, či jeho dôvody trvajú alebo nie, čo znamená, že ak napríklad policajt pred uplynutím doby, na ktorú bol vydaný príkaz sudcu pre prípravné konanie zistí, že dôvody ktoré viedli k jeho vydaniu pominuli, musí spracovať a na príslušný útvar Policajného zboru zaslať žiadosť o predčasné ukončenie použitia informačno-technických prostriedkov. V prípade ak bolo použitie informačno-technických prostriedkov predčasne ukončené, policajt bezodkladne túto skutočnosť písomne oznámi sudcovi pre prípravné konanie a v prípravnom konaní taktiež dozorujúcemu prokurátorovi."[12]

V ustanovení § 115 ods. 8 TP sa uvádza, že pokiaľ 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. Zápisnica o zničení záznamu sa založí do spisu. V takomto prípade osobu uvedenú v § 115 ods. 3 TP, ktorá nemá možnosť nazerať do spisu podľa tohto zákona, 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.

Odsek 8 § 115 TP stanovuje postup orgánov v prípade, ak sa nezistili skutočnosti významné pre trestné konanie. Zmysle uvedeného ustanovenia je predovšetkým v tom, že upravuje podmienky, ktoré v prípade, ak nastanú, majú za následok, že takéto záznamy musia byť predpísaným spôsobom zničené. Originál aj rovnopis vyšetrovacieho spisu musia obsahovať zápisnicu o zničení záznamu a subjekt, ktorý nemá možnosť nazerania do príslušného vyšetrovacie spisu sa musí oboznámiť, že jej telefonické rozhovory boli odpočúvané, prípadne, že bol vykonaný priestorový odposluch (§ 114 TP), alebo oboje.

Trestný poriadok rieši zničenie záznamu telekomunikačnej prevádzky v troch odlišných prípadoch:

a) pri vykonávaní odpočúvania sa zistí, že obvinený komunikuje so svojim obhajcom a informácie sa týkajú trestnej veci, v ktorej ho obhajca zastupuje;[13] alebo
b) príkaz na odpočúvanie vydaný zo strany dozorujúceho prokurátora nebol najneskôr do 24 hodín potvrdený sudcom pre prípravné konanie;[14] alebo
c) počas vykonávania odpočúvania, neboli zistené skutočnosti významné pre trestné konanie.[15]

---

môžu na svoje náklady vyhotoviť prepis záznamu telekomunikačnej prevádzky v rozsahu, v akom to uznajú za vhodné. Povinnosti uvedené v prvej vete sa na nich vzťahujú primerane. 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. Do spisu sa zakladá prepis záznamu telekomunikačnej prevádzky, ktorý sa neutajuje, podpísaný príslušníkom Policajného zboru, ktorý ho vyhotovil; ak doslovný prepis záznamu obsahuje utajovanú skutočnosť, utajuje sa podľa predpisov o ochrane utajovaných skutočností. Záznam telekomunikačnej prevádzky sa môže použiť ako dôkaz až po skončení odpočúvania a záznamu telekomunikačnej prevádzky. V prípravnom konaní, ak to odôvodňujú okolnosti prípadu, možno predložiť záznam telekomunikačnej prevádzky súdu aj bez prepisu tohto záznamu, ak zo sprievodnej správy vyplývajú údaje o mieste, čase, orgáne, ktorý záznam vyhotovil, a zákonnosti vykonávania odpočúvania, ako aj o osobách, ktorých sa záznam telekomunikačnej prevádzky týka, a záznam telekomunikačnej prevádzky je zrozumiteľný."

[12] PERHÁCS, Z.: O zničení záznamov získaných použitím informačno-technických prostriedkov. Justičná revue, 59, 2007, č. 5, s. 644 – 645.

[13] § 115 ods. 1 druhá veta TP.

[14] § 115 ods. 2 druhá veta TP.

[15] § 115 ods. 8 TP.

Pri všetkých troch uvádzaných prípadoch sa uplatňuje pravidlo, že takto vyhotovené záznamy sa musia predpísaným spôsobom „bezodkladne" zničiť. Takáto úprava v zmysle rozhodovacej praxe Európskeho súdu pre ľudské práva vytvára minimálne záruky, ktoré musia byť obsiahnuté vo vnútroštátnom práve, aby sa predišlo zneužitiu právomoci zo strany orgánov, ktoré využitie informačno-technických prostriedkov vykonávajú.

Posledný, vyššie uvádzaný, prípad sa týka situácie, kedy rozhovor (záznam), ktorý nemá žiadnu súvislosť s predmetom trestného konania (bez ohľadu na skutočnosť, či je to rodinný, súkromný alebo iný rozhovor) sa nesmie zaznamenávať. V prípade zachytenia takéhoto záznamu vzniká povinnosť jeho bezodkladného zničenia. Je potrebné, aby o takejto skutočnosti bola vyhotovená zápisnica, ktorú je následne potrebné založiť do originálu ako aj rovnopisu vyšetrovacieho spisu. Jedná sa o situácie, ktoré boli čisto súkromného charakteru a záznamy zachytili iba takéto detaily, nehovoriac o záznamoch ktoré by obsahovali detaily z rodinného života. Takýto záznam je nielenže zákaz „sprocesniť" alebo nemôže sa vykonať ani jeho žiadna archivácia, ktorá by akýmkoľvek spôsobom umožňovala jeho reprodukciu v systéme policajného útvaru. Inak povedané, výsledok z použitia informačno-technického prostriedku sa pred zničením nesmie kopírovať ani prepisovať do písomnej alebo akejkoľvek inej podoby. Uvedený zákaz sa vzťahuje aj na zákaz vyhotovenia záznamu z operatívnej informácie „ZOI", ktorý by inak bol pod príslušným stupňom utajenia.[16]

Zápisnica o zničení záznamu obsahuje okrem všeobecných náležitostí taktiež spôsob akým bol vyhovený záznam zničený. Zničenie vykonaných záznamov sa uskutočňuje spravidla zmazaním alebo spálením. Pre doplnenie, zničenie záznamov sa pritom týka vlastných záznamov (kazety, pásky, počítačové diskety, CD nosiče..), ako aj ich prepisov.[17] Podrobnejší je v tomto ohľade § 7 ods. 5 prvá veta zákona o ochrane pred odpočúvaním v zmysle ktorého: „*O zničení záznamu alebo iného výsledku sa vyhotoví písomná zápisnica, v ktorej sa uvedie dôvod zničenia záznamu alebo výsledku, osobné údaje osoby, ktorá nariadila alebo schválila použitie informačno-technického prostriedku, v rozsahu titul, meno, priezvisko a jej funkcia, osobné údaje osoby, ktorá nariadila alebo schválila zničenie záznamu alebo iného výsledku, v rozsahu titul, meno, priezvisko a jej funkcia a osobné údaje zákonného sudcu, ktorý bol prítomný pri jeho zničení, v rozsahu titul, meno, priezvisko, funkcia, identifikácia príslušného súdu.*" V nadväznosti na zákon o ochrane pred odpočúvaním dodávam, že súčasná úprava TP z pohľadu ochrany základných práv dotknutých osôb neobsahuje povinnosť zničenia záznamu o odpočúvaní v prípade, ak tento bol získaný v rozpore so zákonom, rovnako ako tomu je v § 7 ods. 3 zákona o ochrane pred odpočúvaním.

V prípade ak sa zaznamenaním rozhovoru zistia skutočnosti dôležité resp. významné pre trestné konanie, predpokladáme, že v takomto prípade bude takáto situácia dostatočná na postup podľa § 206 TP. Čo sa týka skutočností dôležitých pre trestné konanie, tak za tie možno považovať také, ktoré čo i len sčasti potvrdzujú protiprávne konanie zakladajúce trestno-procesnú zodpovednosť, alebo majú súvislosť s predmetom trestného konania. Takéto informácie sa následne „odtajnia a sprocesnia" a v ďalšom kroku sa stávajú trestno-procesnými dôkazmi a podozrivého páchateľa usvedčujú z trestného činu.

Bežná prax ukazuje najmä v spojitosti s korupčnými trestnými činmi, pri procesnom vypočúvaní osôb, vypočúvaných v procesnom postavení svedka, ktoré boli prítomné pri korupčnom konaní iných osôb, že tieto tvrdia, že prítomné neboli, alebo keď aj boli, tak nič nevedeli a nič nepočuli. Takéto osoby mnohokrát nemajú vedomosť, že orgány činné v trestnom konaní disponujú prepismi záznamov, ktoré o hovoria o opaku. Treba prekvapivo dodať, že výpovede

[16] PERHÁCS, Z.: O zničení záznamov získaných použitím informačno-technických prostriedkov. Justičná revue, 59, 2007, č. 5, s. 647 – 648.

[17] Nález Ústavného súdu ČR z 27. septembra 2007, sp. zn. II. ÚS 789/06.

sa častokrát zásadne nezmenia ani po ich oboznámení sa s obsahom vykonaného záznamu na technickom zariadení. Reakcie takýchto osôb sú rôzne. Svedkovia majú snahu upravovať svoju výpoveď tak, aby bola racionálne odôvodniteľná v kontexte záznamu. Spravidla však tak nedôjde k potvrdeniu najdôležitejších momentov, ktoré sú dôležité pre trestné konanie. Takéto prípady jednoznačným spôsobom potvrdzujú nevyhnutnosť existencie a vytvorenia možnosti použitia informačno-technických prostriedkov, nakoľko bez ich existencie by v mnohých prípadoch orgány činné v trestnom konaní nemohli zabezpečiť takmer žiadne priame dôkazy.[18]

V danom prípade však netreba opomenúť spomenúť situáciu, kedy použitím vykonania odposluchu dôjde k zisteniam informácií, ktoré podozrenie z páchania z trestného činu vyvracajú. Takéto informácie sa považujú za skutočnosti významné pre trestné konanie. Získané informácie po „odtajnení a sprocesnení", slúžia v prospech podozrivého, nakoľko podozrenie spochybňujú alebo priam vyvracajú. Záznamy spolu s ich doslovnými prepismi sa založia do vyšetrovacieho spisu a spolu s ďalšími ospravedlňujúcimi dôkazmi slúžia ako podklad na zastavenie trestného stíhania podľa § 215 ods. 1 písm. a) TP. Hovorím o prípade, kedy sa ešte pred vznesením obvinenia získavajú dôkazy preukazujúce, že skutok, pre ktorý bolo začaté trestné stíhanie sa nestal. Dotknutá osoba na základe získaných dôkazov už nie osobou podozrivou zo spáchania trestného činu a nemusí byť upovedomená, že voči nej boli použité zaznamenávacie informačno-technické prostriedky. V takomto prípade sa osoba o použití informačno-technických prostriedkov nedozvie a vykonané záznamy sa nezničenia alebo „sprocesnia" a spolu s nosičmi informácii sa stanú súčasťou vyšetrovacieho spisu.

Ak sa vykonaním použitia informačno-technického prostriedku zistia skutočnosti dôležité pre trestné konanie, možno logickým výkladom „argumentum a contrario" konštatovať, že orgán činný v trestnom konaní ani príslušný útvar Policajného zboru, vyhotovené záznamy nezničí. Bez pochyby tak treba uviesť, že za skutočnosti dôležité pre trestné konanie treba považovať skutočnosti, ktoré nie len usvedčujú podozrivého páchateľa resp. páchateľov, ale aj také, ktoré vyvracajú spáchanie trestného činu z ich strany.

V danom prípade treba zdôrazniť, že samotné posudzovanie otázky či použitím informačno-technického prostriedku boli zistené skutočnosti dôležité pre trestné konanie zo strany orgánov činných v trestnom konaní alebo príslušného útvaru Policajného zboru, sa môže javiť ako problém. Spomínané orgány totižto nemusia za každých okolností správne vyhodnotiť, ktoré informácie sú resp. ktoré nie sú, dôležité pre trestné konanie. Stotožňujem sa s názorom pána profesora Jozefa Záhoru, podľa ktorého sa v takomto prípade môže jednať o porušenie práva na obhajobu, ak vyhotovený záznam alebo jeho prepis, nie sú súdu predložené kompletne. Jednoducho povedané neboli predložené v celom rozsahu. Krátenie práva obžalovaného na spravodlivé súdne konanie je možné len z dôvodov ochrany základných ľudských práv iného jednotlivca alebo z dôvodu verejného záujmu.

„Treba poukázať na ustálené rozhodovanie ESĽP, ako aj súdov SR, že pokaľ obžaloba posudzuje význam informácií zatajených obhajobe, nemôže vyhovieť požiadavkám čl. 6 ods. 1 Dohovoru. Existencia dôvodov zatajenia dôkazov obhajobe musí vychádzať iba z uznaných dôvodov, pričom tieto musia podliehať kontrole súdu, ktorému by takýto dôkaz mal byť v celistvosti oznámený, a až následne súd môže rozhodnúť o kolízii práva na obhajobu a spravodlivé súdne konanie s daným dôvodom zatajenia dôkazu v prospech jednej z procesných strán. Vyhotovené obrazové a zvukové záznamy, resp. prepisy, takéhoto záznamu zásadne musia byť súdu predložené ako kompaktný celok, bez ohľadu na obsah, pokiaľ si taký dôkaz nárokuje na označenie

[18] PERHÁCS, Z.: O zničení záznamov získaných použitím informačno-technických prostriedkov. Justičná revue, 59, 2007, č. 5, s. 643.

‚legálny'. Len súd môže potom takýto dôkaz hodnotiť, základným predpokladom však je jeho celistvosť."[19] V takýchto prípadoch by len súd mohol v prípade existencie celého zvukové prepisu tzn. kompletného dôkazu posúdiť, ktoré časti sa týkajú žalovanej trestnej činnosti, resp. nie sú relevantné. Ak by nastal prípad nemožnosti uvádzaného postupu, nebude možné sa takýmto zaoberať a posudzovať ho ako dôkaz svedčiaci v prospech obžaloby.[20]

Čas použitia informačno-technického prostriedku

Podľa § 4 ods. 1 zákona o ochrane pred odpočúvaním možno informačno-technické prostriedky použiť len na základe predchádzajúceho súhlasu zákonného sudcu a len na nevyhnutný čas, najdlhšie však na obdobie šesť mesiacov. Lehota na uskutočnenie odpočúvania podľa zákona o ochrane pred odpočúvaním začína plynúť dňom udelenia súhlasu. TP upravuje čas používania informačno-technického prostriedku „Odpočúvanie a záznam telekomunikačnej prevádzky" v ust. § 115 ods. 3 TP, v zmysle ktorého možno čas odpočúvania a záznamu vykonať počas obdobia najviac šesť mesiacov.

Ak by v rozhodnutí o použití informačno-technického prostriedku absentovala lehota, počas ktorej možno informačno-technický prostriedok použiť, poprípade by bola takáto lehota spochybnená a nepodložená, v takomto prípade by išlo o porušenie princípu proporcionality zásahu. Takáto skutočnosť by automaticky a bez ďalšieho, mala za následok nezákonnosť použitia informačno-technického prostriedku.

Európska komisia pre ľudské práva pri preskúmavaní súladu španielskej úpravy s článkom 8 Dohovoru dňa 11. apríla 1997 vo veci Cosme Valenzuela Contreras proti Španielsku[21] za hodnotiace kritériu označila otázku, či príslušné ustanovenia poskytujú dostatočnú záruku proti svojvoľným zásahom verejnej moci, a na jej základe zistila, že španielske právo nevymedzilo s náležitou jasnosťou a presnosťou rozsah a spôsob výkonu odpočúvania. Španielska úprava totižto nedefinovala kategórie prípadov, v ktorých možno povoliť odpočúvanie a neurčovala časový limit trvania odpočúvania, povinnosť zničiť zvukové záznamy v prípade zastavenia konania alebo zbavenia obvinenia atď.

Predĺženie doby použitia informačno-technického prostriedku

Ďalšie rozhodnutie sudcu (po predchádzajúcom rozhodnutí o použití informačno-technického prostriedku), ktorým má dôjsť k predĺženiu použitia informačno-technického prostriedku, musí obsahovať konkrétne a dodatočne preskúmateľne dôvody, ktorými sa odôvodňuje predĺženie doby použitia informačno-technických prostriedkov. Predĺženie použitia informačno-technických prostriedkov prichádza do úvahy, ak ich doterajším použitím boli zaznamenané skutočnosti, ktoré sa priamo vzťahujú na dôvody jeho vydania. Podľa zákona o ochrane pred odpočúvaním, konkrétne ust. § 4 ods. 2 môže zákonný sudca, ktorý dal súhlas na použitie informačno-technických prostriedkov, na základe novej žiadosti dobu ich použitia predĺžiť, zakaždým však najviac o ďalších šesť mesiacov, ktoré začínajú plynúť dňom udelenia súhlasu. Pokiaľ sa vydáva ďalší súhlas, je potrebné, aby ten bol vydaný v posledný deň lehoty podľa odseku 1. Pokiaľ by takýto súhlas v lehote podľa predchádzajúcej vety nebol vydaný, použitie informačno-technického prostriedku musí skončiť v posledný deň lehoty určenej v súhlase. Čo sa týka

[19] ZÁHORA, J. et. al.: Obrazové a zvukové záznamy v trestnom konaní. Bratislava: Wolters Kluwer. 2018. s. 232.
[20] Uznesenie Najvyššieho súdu SR, sp. zn. 3 To 6/2009.
[21] Pozn. sťažnosť č. 27671/95.

predĺženia použitia informačno-technického prostriedku, konkrétne „Odpočúvania a záznamu telekomunikačnej prevádzky", podľa § 115 ods. 3 štvrtej vety TP, čas odpočúvania a záznamu telekomunikačnej prevádzky môže v prípravnom konaní na návrh prokurátora predĺžiť sudca pre prípravné konanie vždy najviac o dva mesiace, a to aj opakovane.[22]

Bez ohľadu na skutočnosť, či sa jedná o predĺženie súhlasu podľa zákona o ochrane pred odpočúvaním alebo príkazu na vyhotovenie odpočúvania alebo záznamu telekomunikačnej prevádzky podľa § 115 TP, vydané rozhodnutie musí obsahovať konkrétne dôvody, pre ktoré sa použitie informačno-technického prostriedku predlžuje. V prípade ak by vydané rozhodnutie o predĺžení doby použitia informačno-technického prostriedku neobsahovalo konkrétne a dostatočne preskúmateľne dôvody odôvodňujúce predĺženie doby vydaného príkazu, ktoré by zároveň taktiež predstavovali ospravedlňujúci zásah do práva na súkromie, takéto rozhodnutie by bolo možné považovať za nepreskúmateľné a svojvoľné. Treba dodať, že predĺženie doby použitia informačno-technického prostriedku možno realizovať len základe vydaného nového rozhodnutia o použití, pričom takéto ďalšie rozhodnutie musí byť vydané taktiež písomne, a to najneskôr v posledný deň lehoty určenej v rozhodnutí. V prípade ak vydaniu rozhodnutiu podľa predchádzajúcej vety nedôjde, použitie informačno-technického prostriedku musí byť ukončené v posledný deň lehoty. V praxi uvedená skutočnosť neznamená len „vypnutie" informačno-technického prostriedku, ktorým bolo vykonávané odpočúvanie a záznam telekomunikačnej prevádzky, ale uplynutím posledného dňa uvedeného v príkaze musí byť predovšetkým vykonaná fyzická demontáž operatívneho zariadenia.

Oznámenie o odpočúvaní

V predchádzajúcej časti som sa venovala najmä zničeniu záznamu z odpočúvania a záznamu telekomunikačnej prevádzky v zmysle § 115 ods. 8 TP v prípade, ak sa v priebehu odpočúvania a záznamu telekomunikačnej prevádzky nezistili skutočnosti významné pre trestné konanie.

V tejto časti sa venujem inštitútu oznamovania o odpočúvaní dotknutým osobám v prípade zničenia záznamu v zmysle § 115 ods. 8 TP.

Právo byť informovaný o odpočúvaní z pohľadu Európskeho súdu pre ľudské práva

„Ako vyplýva z medzinárodných dohovorov, ale najmä z judikatúry Európskeho súdu pre ľudské práva, vždy keď je to možné 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 namietať nezákonnosť alebo bezdôvodnosť odpočúvania."[23]

Európsky súd pre ľudské práva predstavuje inštitúciu, ktorá tradične chráni práva jednotlivcov pred neoprávnenými zásahmi jednotlivých štátov, pričom rovnaká zásada sa vzťahuje aj na zásahy do práva na súkromie jednotlivcov prostredníctvom odpočúvania. Európsky súd pre ľudské práva vo svojej judikatúre ustanovil základné kritériá, ktoré obmedzujú právo štátu na zásah do práva chráneného článkom 8 Dohovoru. Európsky súd pre ľudské práva v priebehu trvania svojej existencie vydal celý rad rozhodnutí, v ktorých upresnil zásady, ktoré je nevyhnutné rešpektovať pri uplatňovaní právnych noriem týkajúcich sa inštitútu odpočúvania, pričom

[22] PERHÁCS, Z.: O nevyhnutných atribútoch rozhodnutia sudcu na použitie informačno-technických prostriedkov. Bulletin Slovenskej advokácie, 2013, č. 12, s. 16 – 18.

[23] IVOR, J. a kol.: Trestné právo procesné. Bratislava: IuraEdition, 2010, s. 406.

Európsky súd pre ľudské práva sa v týchto rozhodnutiach zameral najmä ochranu jednotlivcov pred zneužitím inštitútu odpočúvania.

Aktuálnou je najmä otázka, či majú štátne orgány povinnosť „a posteriori" informovať odpočúvanú osobu o uskutočnenom odpočúvaní. Európsky súd pre ľudské práva sa k predmetnej otázke vyjadruje tak, že v právnych poriadkoch je nevyhnutné zakotviť mechanizmy, ktoré zabezpečujú efektívnu kontrolu odpočúvania po jeho ukončení a zároveň poskytnú odpočúvanej osobe možnosť preskúmať zákonnosť odpočúvania. Medzi predmetné inštitúty kontroly zaraďujeme aj aposteriórnu informačnú povinnosť. V priebehu svojej existencie Európsky súd pre ľudské práva vytvoril pomerne komplexný systém ochrany odpočúvaných osôb a zároveň ustanovil podmienky, pri ktorých splnení je možné predmetnú ochranu porušiť.[24]

Na základe vyššie uvedeného považujem za vhodné spomenúť niekoľko príkladov z rozhodovacej praxe Európskeho súdu pre ľudské práva.

Prípad Klass a ostatní proti Nemecku

Jedným z prvých krokov v súvislosti s interpretáciou práv jednotlivcov byť ex post informovaní o vykonanom odpočúvaní v súlade s článkom 8 Dohovoru, bolo rozhodnutie vo veci Klass proti Nemecku. Napriek skutočnosti, že sa jedná o takmer štyridsať rokov staré rozhodnutie, jeho závery sú rovnako aplikovateľné aj v súčasnosti.[25]

V prípade Klass proti Nemecku sa nemecká vláda odvolávala na ochranu národnej bezpečnosti a predchádzanie trestnej činnosti s cieľom ospravedlniť svoju kontroverznú legislatívu (pozn. autora: Zákon o obmedzení listového, poštového a telekomunikačného tajomstva, tiež známy ako zákon „G-10", ktorý bol prijatý v nadväznosti na teroristické hrozby v 70. rokoch 20. storočia) v oblasti sledovacích prostriedkov, ktorú sťažovatelia napadli. Nemecko zastávalo názor, že štátne orgány môžu na základe zákona sledovať korešpondenciu ako aj telefonickú komunikáciu osôb, a to bez toho, aby o tom následne museli dotknuté osoby informovať.[26]

Pri rozhodovaní o tom, či predmetná napadnutá legislatíva predstavuje porušenie článku 8 Dohovoru, sa súd opieral o dve skutočnosti. Za prvé poukázal na technologický pokrok dosiahnutý v oblasti „špionážnej techniky" a následne poukázal na nebezpečenstvo hrozby terorizmu. Súd priamo uviedol, že demokratické spoločnosti musia čeliť veľmi sofistikovaným formám špionáže a terorizmu. Štát teda musí disponovať možnosťou sledovať tieto živly, ktoré operujú na jeho území. V dôsledku toho súd musí akceptovať existenciu právnych predpisov, ktoré oprávňujú štátne orgány k tajnému monitorovaniu korešpondencie a telekomunikácie. Takéto monitorovanie je teda v súlade s článkom 8 Dohovoru, nakoľko je to v demokratickej spoločnosti nevyhnutné v záujme národnej bezpečnosti a predchádzaniu trestnej činnosti.[27]

Členské štáty vtedy disponovali pomerne širokou voľnosťou v oblasti opatrení proti terorizmu a iným závažným trestným činom. Európsky súd pre ľudské práva však mal na zreteli potenciálne nebezpečenstvo, ktoré predstavovali práve právne predpisy umožňujúce odpočúvanie osôb, v dôsledku čoho konštatoval, že štáty nesmú v rámci boja proti trestnej činnosti prijímať ľubovoľné opatrenia, ktoré by považovali za vhodné. V predmetnej súvislosti sú potrebné primerané a najmä účinné záruky proti zneužitiu predmetných inštitútov.[28]

---

[24] DE HERT, BOEHM. The rights of notification after surveillance is over: Ready for Recognition?. In: BUS, J. et al., Digital Enlightenment Yearbook 2012. IOS Press BV, 2012, s. 23.

[25] Tamtiež.

[26] DE HERT, BOEHM. The rights of notification after surveillance is over: Ready for Recognition?. In: BUS, J. et al., Digital Enlightenment Yearbook 2012. IOS Press BV, 2012, s. 24.

[27] Rozhodnutie Európskeho súdu pre ľudské práva zo dňa 6. 9. 1978, č. 5029/71, § 48. Vec: Klass proti Nemecku.

[28] Tamtiež. § 49.

Jednu z predmetných záruk predstavuje možnosť osoby, ktorá bola odpočúvaná, domáhať sa svojich práv v prípade, ak bola odpočúvaná nezákonne. Aby to bolo možné, musí byť dotknutá osoba v prvom rade informovaná, že vôbec bola odpočúvaná. V predmetnej súvislosti Európsky súd pre ľudské práva v § 57 spojil aposteriórnu kontrolu odpočúvania s informačnou povinnosťou štátnych orgánov.[29] Súd v predmetnom ustanovení priamo konštatuje, že je potrebné určiť, či má jednotlivec možnosť na aposteriórne preskúmanie legality odpočúvania súdom. Daný problém je neoddeliteľne spojený s otázkou ex post informovania, a to najmä preto, že existuje len veľmi malý priestor pre to, aby občan spochybnil zákonnosť odpočúvania, pokiaľ nebol oboznámený s príkazom na jeho vykonanie, ako aj so samotným vykonaním.

V prípade Klass sa nakoniec Európsky súd pre ľudské práva stotožnil so záverom nemeckého ústavného súdu, ktorého rozhodnutie bolo rovnako napadnuté. Nemecký súd sa dopracoval k záveru, že dotknutá osoba musí byť informovaná o vykonaní odpočúvania po jeho skončení, a to ihneď, ako je to možné bez toho, aby došlo k ohrozeniu účelu samotného odpočúvania.[30] Podľa názoru Európskeho súdu pre ľudské práva je tiež potrebné vyhodnotiť, či je aposteriórna notifikácia nevyhnutná vo všetkých prípadoch, pričom konštatoval, že notifikovanie každej odpočúvanej osoby môže ohroziť dlhodobý cieľ odpočúvania. Podľa Európskeho súdu pre ľudské práva, skutočnosť, že osoba nebola dodatočne informovaná o vykonanom odpočúvaní, nemôže sama osebe predstavovať porušenie článku 8 Dohovoru, nakoľko práve predmetná skutočnosť zabezpečuje efektivitu zásahu do práva na súkromie.[31]

Súd dospel v predmetnom prípade k záveru, že nemecká legislatíva je v zásade v súlade s článkom 8 Dohovoru, nakoľko stanovuje prísne podmienky pre vykonávanie odpočúvania a spracovávanie takto získaných informácií. Predmetné rozhodnutie bolo v danej oblasti prelomové, nakoľko sa v ňom Európsky súd pre ľudské práva prvý krát zaoberal konfliktom medzi záujmom štátu na odhaľovaní trestnej činnosti a právom jednotlivca byť ex post informovaný o zásahu do jeho súkromia. Aposteriórna notifikácia však v danom prípade nebolo uznaná ako nevyhnutná podmienka vykonávania odpočúvania. Súd vo svojom rozhodnutí zdôraznil, že napriek tomu, že sa jedná o nástroj, ktorý zaručuje účinnú kontrolu odpočúvania, nie je nevyhnutný, ani jediný.[32]

Prípad Weber a Saravia proti Nemecku

V roku 2006, takmer tridsať rokov od vydania rozhodnutia vo veci Klass, sa stal nemecký zákon G-10, konkrétne jeho novelizácia, opätovne predmetom konania pred Európskym súdom pre ľudské práva. Sťažovatelia napadli štyri zmeny zákona, ktoré rozšírili právomoci v oblasti strategického monitoringu telekomunikácií. Európsky súd pre ľudské práva skúmal, či bola vtedajšia právna úprava v súlade s čl. 8 Dohovoru, predovšetkým či boli dodržané minimálne požiadavky stanovené predchádzajúcou judikatúrou.

Súd vo svojom rozhodnutí skonštatoval, že právna úprava musí predovšetkým obsahovať konkrétne záruky proti zneužitiu odpočúvania, ako napríklad obmedzené monitorovanie len na krátku dobu, okamžité skončenie odpočúvania v prípade, že už nie sú splnené podmienky pre

[29] DE HERT, BOEHM. The rights of notification after surveillance is over: Ready for Recognition?. In: BUS, J. et al., Digital Enlightenment Yearbook 2012. IOS Press BV, 2012, s. 25.

[30] Tamtiež.

[31] KMEC, J. Právo být informován a posteriori o provedených odposleších aneb „pokoutní" posun v judikatuře ESLP. Soudní rozhledy, 2008, č. 8, s. 312.

[32] DE HERT, BOEHM. The rights of notification after surveillance is over: Ready for Recognition?. In: BUS, J. et al., Digital Enlightenment Yearbook 2012. IOS Press BV, 2012, s. 25.

jeho vykonávanie a následné zničenie získaných informácií. Súd taktiež konštatoval, že rovnako je nutná aj nezávislá aposteriórna kontrola odposluchu, vrátane informačnej povinnosti.[33]

V súvislosti s aposteriórnou informačnou povinnosťou súd odkázal na závery vyplývajúce z rozhodnutia Klass proti Nemecku, pričom poukázal na to, že informačná povinnosť je veľmi úzko spojená s možnosťou jednotlivca obrátiť sa na súd, pričom predstavuje jednu zo záruk, že nebude dochádzať k zneužívaniu inštitútu odpočúvania zo strany štátu. Následne však súd zdôraznil, že skutočnosť, že odpočúvaná osoba nebola následne informovaná, sama osebe nevedie k záveru, že došlo k porušeniu čl. 8 Dohovoru, nakoľko práve nevedomosť dotknutej osoby môže predstavovať účinnosť zásahu do práva chráneného Dohovorom. S poukazom na riziká spojené s informačnou povinnosťou súd dodal, že akonáhle môže byť dotknutá osoba informovaná o odpočúvaní bez toho, aby ohrozila jeho účel, tak by mala byť informovaná.[34] Súd pritom odkazoval na svoje predchádzajúce rozhodnutie vo veci Klass proti Nemecku a tiež na rozhodnutie vo veci Leander porti Švédsku. Podľa názorov niektorých právnych odborníkov bol však odkaz na predmetné rozhodnutia prekvapivý, nakoľko v rozhodnutí Klass proti Nemecku sa Európsky súd pre ľudské práva len zmienil o tom, že dotknutá osoba musí byť aposteriórne informovaná o vykonanom odpočúvaní jedine v prípade, ak predmetné informovanie neohrozí účel odpočúvania. Predmetná skutočnosť však nezohrávala rozhodujúcu úlohu v argumentácii súdu ani v prípade Leander. Európsky súd pre ľudské práva tak významným spôsobom posunul svoju judikatúru bez toho, aby použil relevantnú argumentáciu. Európsky súd pre ľudské práva len poukázal na rozhodnutia vo veciach Klass a Leander, čím vzbudil nesprávny dojem, že najnovšie formulovaný princíp povinnosti dodatočne informovať dotknutú osobu o tom, že bola odpočúvaná, je už dávno súčasťou jeho judikatúry.[35]

Európsky súd pre ľudské práva konštatoval, že požiadavky obsiahnuté v čl. 8 Dohovoru boli splnené a nemecká právna úprava je vyhovujúca. Spolkový ústavný súd navyše posilnil ochranné opatrenia proti zneužitiu odpočúvania formou vyhýbania sa informačnej povinnosti. Okrem toho je v Nemecku zriadená nezávislá komisia, ktorá dohliada na dodržiavanie dotknutého zákona a má právo rozhodnúť, či aposteriórna notifikácia bola v konkrétnych prípadoch nevyhnutná. Predmetné opatrenia viedli Európsky súd pre ľudské práva k záveru, že zákon G-10 dostatočne zaručuje, že aposteriórna informačná povinnosť bude splnená alebo minimálne bude jej absencia riadne podložená. V predmetnom rozhodnutí súd potvrdil závery zistené vo veci Klass proti Nemecku.[36]

Nakoľko z hľadiska rozsahu tohoto príspevku nie je možné venovať sa judikatúre Európskeho súdu v danej oblasti detailnejšie, považujem za potrebné zdôrazniť, že aposteriórna informačná povinnosť predstavuje jeden z kľúčových prvkov ochrany pred zneužitím odpočúvania. Zavedením potreby aposteriórnej informačnej povinnosti Európsky súd pre ľudské práva reagoval na technologický pokrok a nové metódy získavania informácií v Trestnom konaní. Jedine v prípade, ak sú jednotlivci informovaní o vykonanom odpočúvaní, môžu využiť ochranu, ktorú im poskytujú čl . 8 a 13 Dohovoru, a samotné štáty si tak zároveň plnia povinnosť, ktorá im z predmetných článkov vyplýva.

---

[33] Rozhodnutie Európskeho súdu pre ľudské práva zo dňa 29. 6. 2006, č. 54934/00, § 114 – 116. Vec: Weber a Saravia proti Nemecku.

[34] Tamtiež. § 135.

[35] KMEC, J. Právo být informován a posteriori o provedených odposleších aneb „pokoutní" posun v judikatuře ESLP. Soudní rozhledy, 2008, č. 8, s. 314.

[36] DE HERT, BOEHM. The rights of notification after surveillance is over: Ready for Recognition?. In: BUS, J. et al., Digital Enlightenment Yearbook 2012. IOS Press BV, 2012, s. 29.

Informovanie o odpočúvaní v zmysle Trestného poriadku

V súvislosti s predmetnou právnou úpravou v rámci právneho poriadku Slovenskej republiky k predmetnej veci uvádzam, že

§ 115 ods. 9 TP ustanovuje, že o zničení záznamu informuje osobu uvedenú v odseku 3 (pozn. autora: osoba, ktorej sa odpočúvanie a záznam telekomunikačnej prevádzky týka), 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.

Na druhej strane § 115 ods. 10 TP ustanovuje, že informáciu podľa odseku 9 predseda senátu, policajt alebo prokurátor nepodá, 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 jednej z nich nebolo trestné stíhanie právoplatne skončené, alebo ak by poskytnutím takej informácie mohol byť zmarený účel trestného konania.

Práve predmetné ustanovenia zabezpečujú primeranú a účinnú záruku proti zneužitiu inštitútu odpočúvania a záznamu telekomunikačnej prevádzky, a to tým spôsobom, že stanovujú povinnosť upovedomiť osobu, ktorá nemá možnosť nazerať do vyšetrovacieho spisu, o použití predmetného informačno-technického prostriedku.

Z vyššie uvedeného vyplýva, že v predsúdnom konaní je informáciu povinný podať policajt alebo prokurátor, ktorého rozhodnutím bola predmetná trestná vec právoplatne ukončená. V konaní pred súdom zasa táto povinnosť pripadá na predsedu senátu. V súvislosti s právoplatným ukončením konania pred súdom rovnako uvádzam do pozornosti skutočnosť, že k informovaniu dotknutej osoby dochádza bezodkladne po právoplatnom skončení veci pričom predseda senátu nečaká, ako dopadne prípadné konanie o mimoriadnom opravnom prostriedku.

Z ustanovení § 115 ods. 9 TP, okrem iného, vyplýva, že informácia zaslaná dotknutej osobe obsahuje označenie súdu, ktorý vydal alebo potvrdil príkaz na odpočúvanie a záznam telekomunikačnej prevádzky, dĺžku odpočúvania a dátum jeho ukončenia.

V predmetnej súvislosti považujem za potrebné uviesť do pozornosti skutočnosť, že napriek tomu, že sa samotné odpočúvanie vykonáva na základe príkazu príslušného súdu, vydaniu samotného príkazu predchádza vydanie podnetu na odpočúvanie policajtom a následným vydaním návrhu na odpočúvanie prokurátorom. Keďže podstatou samotného odpočúvania je získavanie informácií dôležitých pre trestné konanie utajovaným spôsobom, rovnako uvedené písomnosti, teda podnet, návrh aj príkaz podliehajú režimu utajenia, a to spravidla režimu „vyhradené" v zmysle zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností v znení neskorších predpisov, ktorý v zmysle § 1 ods. 1 upravuje podmienky na ochranu utajovaných skutočností, práva a povinnosti právnických osôb a fyzických osôb pri tejto ochrane, pôsobnosť Národného bezpečnostného úradu a pôsobnosť ďalších štátnych orgánov vo vzťahu k utajovaným skutočnostiam a zodpovednosť za porušenie povinností ustanovených týmto zákonom a ktorý v § 3 ods. 6 definuje stupeň utajenia „vyhradené" ako takú utajovanú skutočnosť, ak by neoprávnená manipulácia s ňou mohla zapríčiniť poškodenie právom chránených záujmov právnickej osoby alebo fyzickej osoby, ktoré by mohlo byť nevýhodné pre záujmy Slovenskej republiky.

V súvislosti s informovaním dotknutej osoby o tom, že bola odpočúvaná poukazujem na logický výklad ustanovení TP ako aj zákona o ochrane utajovaných skutočností v zmysle ktorého je nepochybné, že k samotnému informovaniu nemôže dôjsť skôr, než dôjde k zrušeniu stupňa utajenia príkazu na odpočúvanie.

Tu uvádzam do pozornosti ustanovenie § 7 ods. 1 zákona č. 215/2004 Z. z., v zmysle ktorého „ak pominula potreba ochrany informácie alebo veci obsahujúcej utajované skutočnosti v určenom stupni utajenia, pôvodca utajovanej skutočnosti rozhodne o zmene stupňa utajenia alebo zrušení utajenia." Zároveň predmetný zákon definuje pôvodcu utajovanej skutočnosti v § 2 písm. e) právnickú osoba alebo fyzickú osobu, ktorá je oprávnená rozhodnúť, že určitá informácia je utajovanou skutočnosťou, určiť stupeň utajenia a rozhodnúť o zmene alebo zrušení stupňa jej utajenia.

Z uvedeného nepochybne vyplýva, že na zrušenie stupňa utajenia príkazu na odpočúvanie je oprávnený len súd, ktorý predmetný príkaz vydal.

S poukazom na vyššie uvedené považujem za vhodné zamyslieť sa nad samotným inštitútom informovania odpočúvanej osoby o vykonávanom odpočúvaní v prípade, ak došlo k právoplatnému skončeniu veci policajtom alebo prokurátorom. Na to, aby policajt resp. prokurátor mohol splniť informačnú povinnosť v zmysle § 115 ods. 9 TP, musí požiadať príslušný súd o odtajnenie príkazu na odpočúvanie, avšak súd nie je povinný predmetnej žiadosti vyhovieť, čím by mohlo dôjsť k zmareniu účelu inštitútu informovania dotknutej osoby a rovnako k porušeniu čl. 8 Dohovoru. V Slovenskej republike v súčasnosti nie sú k dispozícii štatistiky vo vzťahu k počtu vykonaných odpočúvaní a teda ani k počtom prípadov, kedy skutočne došlo k informovaniu dotknutej osoby o odpočúvaní resp. kedy príslušný súd odmietol zrušiť stupeň utajenia príkazu na odpočúvanie a k nemohlo dôjsť k samotnému informovaniu.

V rámci úvah de lege ferenda by som navrhovala spracovať predmetné štatistiky a rovnako by som navrhovala zriadenie určitej kontrolnej komisie, ktorej úlohou by bolo validovať, či odmietnutie zrušenia stupňa utajenia príslušným súdom je skutočne odôvodnené. Som toho názoru, že predmetné kontrolné mechanizmy by si nepochybne našli svoje miesto v spoločnosti, nakoľko ich implementácia by zvyšovala prevenciu najmä vo vzťahu k porušovaniu ustanovení TP a čl. 8 Dohovoru.

V samotnom závere môjho príspevku by som rada opätovne zdôraznila nevyhnutnosť nájdenia rovnováhy medzi potrebou štátnych orgánov zasahovať do práva na súkromie v súvislosti s odhaľovaním trestnej činnosti a samotným právom jednotlivca na súkromie. Ako som to už uviedla vyššie v mojom príspevku, v mnohých prípadoch predstavuje použitie inštitútu odpočúvania a záznamu telekomunikačnej prevádzky jediný spôsob zabezpečenia dôkazov v trestnom konaní, a teda samotná nevyhnutnosť a dôležitosť tohto inštitútu je nespochybniteľná. Rovnako si dovoľujem tvrdiť, že slovenská právna úprava odpočúvania je na vysokej úrovni a spĺňa požiadavky obsiahnuté v rozličných dokumentoch venujúcich sa ochrane ľudských práv a základných slobôd, a zároveň zamedzuje svojvôli štátnych orgánov v súvislosti so zneužívaním tohto inštitútu. Avšak zároveň mi nedá nespomenúť poslednú vetu § 115 ods. 10 TP, v zmysle ktorej dotknutá osoba nemusí byť upovedomená o tom, že bola odpočúvaná, ak by poskytnutím takej informácie mohol byť zmarený účel trestného konania. V predmetnej súvislosti sa predsa len zamýšľam nad tým, čo konkrétne mal zákonodarca na mysli týmto ustanovením, a to najmä s poukazom na to, že už došlo k právoplatnému skončeniu trestnej veci. Nevytvára to nakoniec určitý priestor na určitú manipuláciu v súvislosti odôvodnením, prečo neinformovať dotknutú osobu?

Literatúra

Knihy

IVOR, J. a kol.: Trestné právo procesné. Bratislava: Iura Edition, 2010. ISNB: 9788080783082

ZÁHORA, J et. al.: Obrazové a zvukové záznamy v trestnom konaní. Bratislava: Wolters Kluwer. 2018. ISBN 9788081689574

Časopisy

DE HERT, BOEHM. The rights of notification after surveillance is over: Ready for Recognition?. In: BUS, J. et al., Digital Enlightenment Yearbook 2012. IOS Press BV, 2012. ISSN 1070-9622

DRGONEC, J.: Ústavný a zákonný rámec použitia informačno-technických prostriedkov štátnymi orgánmi. Justičná revue, 53, 2001, č. 10. ISSN 1335-6461

KMEC, J.: Právo být informován a posteriori o provedených odposleších aneb „pokoutní" posun v judikatuře ESLP. Soudní rozhledy, 2008, č. 8, s. 312

PERHÁCS, Z.: O nevyhnutných atribútoch rozhodnutia sudcu na použitie informačno-technických prostriedkov. Bulletin Slovenskej advokácie, 2013, č. 12. s. 13 – 23. ISSN 1335-1079

PERHÁCS, Z.: O zničení záznamov získaných použitím informačno-technických prostriedkov. Justičná revue, 59, 2007, č. 5.

ZACHAR, A.: Informačno-technické prostriedky a možnosti ich používania na území Slovenskej republiky, Trestní právo, 09, 2008.

ZÁHORA, J.: Príkaz v trestnom konaní. Justičná revue 56, 2004, č. 5.

Zákony

Zákon č. 460/1992 Z. z. Ústava SR

Zákon č. 301/2005 Z. z. Trestný poriadok

Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností

Judikatúra

Nález Ústavného súdu ČR z 27. septembra 2007, sp. zn. II. ÚS 789/06

Nález Ústavného súdu Slovenskej republiky zo dňa 14. júna 2006 pod. sp. zn. I. ÚS 274/05

Rozhodnutie Európskeho súdu pre ľudské práva zo dňa 24. 4. 1990. Vec: Huvig a Kruslin v. Francúzsko

Rozhodnutie Európskeho súdu pre ľudské práva zo dňa 29. 6. 2006. Vec: Weber a Saravia proti Nemecku

Rozhodnutie Európskeho súdu pre ľudské práva zo dňa 6. 9. 1978. Vec: Klass proti Nemecku

Uznesenie Najvyššieho súdu SR, sp. zn. 3 To 6/2009

Preskúmanie zákonnosti vydaného príkazu na odpočúvanie a záznam telekomunikačnej prevádzky[1]

The Reviewing the Legality of the Interception and Recording of the Telecommunications Order

Barbora Tallová[2]

Abstrakt: *Odpočúvanie a záznam telekomunikačnej prevádzky predstavuje dôležitý inštitút trestného práva procesného. Jeho prostredníctvom sa výrazne zasahuje do garantovaných práv a slobôd dotknutých osôb, preto podmienky jeho využitia podliehajú striktnej zákonnej limitácii. Dotknuté osoby preto musia disponovať aj účinnou možnosťou (za predpokladu že získali vedomosť o realizácii odpočúvania) žiadať o jeho dodatočné preskúmanie. Príspevok bude venovaný zákonnej regulácii príkazu na odpočúvanie a následne preskúmateľnosti jeho zákonnosti na Najvyššom súde Slovenskej republiky.*

Abstract: *The interception and recording of telecommunications is an important institute of procedural criminal law. It significantly interferes with the guaranteed rights and freedoms of the persons concerned, so the conditions for its use must have strict legal limitations. Therefore, the persons concerned must also have an effective option (provided they have acquired knowledge of the execution of the interception) to request an additional review. This article will be devoted to the legal regulation of the interception order and subsequently to the verifiability of its lawfulness at the Supreme Court of the Slovak Republic.*

Kľúčové slová: *odpočúvanie a záznam telekomunikačnej prevádzky, príkaz, zákonnosť, zásah do práva na súkromie*

Keywords: *Interception and Recording of Telecommunications, Order, Legality, Interference with the Right to Privacy*

Úvod

Odpočúvanie a záznam telekomunikačnej prevádzky predstavuje dôležitý inštitút trestného práva využívaný pri odhaľovaní a dokazovaní závažnejšej trestnej činnosti. Do základných ľudských práv prostredníctvom odpočúvania je možné zasahovať iba v prípadoch, ak sú splnené zákonné požiadavky na jeho využitie. Súčasne sa požaduje, aby existoval dostatočný a efektívny systém garancií ochrany práv pred zásahmi, ktoré sú nezákonné, neprimerané a neodôvodnené. Prostriedky získavania informácií dôležitých pre trestné konanie prostredníctvom využitia informačno-technických prostriedkov, predstavujú závažný zásah do sféry súkromia, pričom dotknuté osoby nemajú možnosť podať proti nariadeniu takéhoto opatrenia opravný prostriedok a o jeho realizácii sa môžu potenciálne dozvedieť až dodatočne, keď už zásah do práva na súkromie bol realizovaný. Po použití týchto prostriedkov by mali byť dotknuté osoby informované o tom, že sa voči nim využili a došlo k zásahu do ich práv. Všetky osoby v dôsledku porušenia svojich práv majú garantované právo na súdnu ochranu nielen na národnej, ale i európskej a medzinárodnej úrovni. Garanciu ochrany práv by mala zabezpečovať tá právna úprava, kto-

[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] JUDr. Barbora Tallová, Ústav verejného práva, Fakulta práva, Paneurópska vysoká škola, Bratislava, e-mail: barboratallova@gmail.com.

rá použitie takýchto zásahov umožňuje. Na tieto účely je zameraná celková úprava podmienok, za ktorých sa konkrétny inštitút môže využiť, stanovuje sa okruh trestných činov, pri ktorých je ich možné nariadiť, fázy konania, v ktorých je možné inštitút vykonávať, stanovený je subjekt oprávnený rozhodnúť o ich použití, písomná forma príkazu, jeho odôvodnenie, možnosti využitia zistených informácií, úprava spôsobu kontroly dodržiavania zákonnosti pri ich využívaní a v neposlednom rade sú upravené možnosti informovania dotknutých osôb, v súvislosti s inštitútom odpočúvania a záznamu telekomunikačnej prevádzky ide aj o poskytnutie informácie o možnosti preskúmania vydaného príkazu.

Právny rámec odpočúvania v Slovenskej republike tvorí najmä zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov (ďalej iba „TP") 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 príspevku bude pozornosť zameraná na vykonávanie odpočúvania a záznamu telekomunikačnej prevádzky v trestnom konaní podľa § 115 TP.

Verejnosť vníma odpočúvanie veľmi negatívne, vzhľadom na jeho invazívny charakter a ťažkú zistiteľnosť takéhoto zásahu. Dotknuté osoby preto musia disponovať aj účinnou možnosťou (za predpokladu že získali vedomosť o realizácii odpočúvania) žiadať o jeho dodatočné preskúmanie.

Preskúmateľnosť dôvodnosti vydania súhlasu na použitie informačno-technického prostriedku 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 konkrétne skutočnosti je daný súhlas spravidla nepreskúmateľný. Z uvedeného dôvodu, je nutné v odôvodnení príkazu uviesť konkrétne skutočnosti odôvodňujúce vydanie súhlasu.[3] Vzhľadom k princípom právneho štátu je nutné, aby dotknutá osoba bola informovaná o využití takýchto invazívnych zásahov do jej súkromia prostredníctvom informačno-technických prostriedkov a mala možnosť v prípade neoprávnenosti ich využitia sa proti nim brániť súdnou cestou.

V súvislosti s využitím odpočúvania a záznamu telekomunikačnej prevádzky v trestnom konaní sa novelou zákona č. 397/2015 Z. z. s účinnosťou od 1. 1. 2016 do Trestného poriadku, okrem iného, doplnila právna úprava, ktorá umožňuje osobe, ktorá bola príslušným orgánom informovaná o zničení záznamu, podať návrh na preskúmanie zákonnosti príkazu na odpočúvanie a záznam telekomunikačnej prevádzky na Najvyšší súd SR. Predmetné ustanovenie poskytuje určitému okruhu osôb širšiu ochranu zo strany orgánov verejnej moci. Uvedené konanie je možné iba na návrh osoby, ktorej bola doručená informácia o zničení záznamu z vykonaného odpočúvania. K porušeniu zákona v súvislosti s príkazom na odpočúvanie môže dôjsť pri vydaní predmetného príkazu, pri jeho realizácii alebo súčasne pri jeho vydaní a následne aj pri jeho realizácii.

[3] Nález Ústavného súdu SR III. ÚS 490/2015-367.

Inštitút odpočúvania a záznamu telekomunikačnej prevádzky a potreba limitov jeho uplatňovania

Odpočúvanie telekomunikačnej prevádzky predstavuje závažný zásah do ústavne zaručených práv a slobôd jednotlivca, napriek tomu patrí k jednému z najpoužívanejších dôkazných prostriedkov v trestnom konaní pri stíhaní niektorých foriem trestnej činnosti. Zohrávajú nezastupiteľnú úlohu pri získavaní informácií v boji proti trestnej činnosti, avšak predstavujú výrazný zásah do súkromia osoby, proti ktorej sú použité. Dôležitá je precízna právna úprava podmienok ich použitia a nakladania s takto získanými informáciami. Pri dokazovaní rozsiahlej organizovanej kriminality bývajú zachytené informácie z odpočúvania dokonca dôkazom kľúčovým a nezastupiteľným. Pri vykonávaní odpočúvania sa postupuje utajeným spôsobom, čo je jeden z obligatórnych znakov charakterizujúcich využitie informačno-technických prostriedkov v trestnom konaní. Spravidla sa odpočúvanie realizuje po určitý čas, nejde o jednorazovú záležitosť. Pri jeho realizácii sa zachytávajú, zisťujú a dokumentujú komunikácie realizované prostredníctvom elektronických komunikačných sietí niekoľko týždňov, alebo mesiacov a v priebehu jeho vykonávania dochádza k intenzívnemu zásahu do základných ľudských práv a slobôd dotknutej osoby. Ide najmä o telefonické rozhovory, textové správy, elektronickú poštu, telefonovanie cez internet. „O použitie informačno-technického prostriedku ide predovšetkým pri odpočúvaní a zaznamenávaní telekomunikačnej prevádzky uskutočnenej prostredníctvom zabezpečených telekomunikačných sietí. Pri odpočúvaní a zaznamenávaní telekomunikačnej prevádzky realizovanej prostredníctvom nezabezpečených sietí, najmä formou rádio-komunikácie, nie je potrebný súhlas, resp. príkaz sudcu, a preto nejde o použitie informačno-technických prostriedkov v pravom zmysle. Rovnako nie je potrebný súhlas sudcu na odpočúvanie a záznam telekomunikačnej prevádzky, ktorú záujmová osoba realizuje prostredníctvom verejne dostupných komunikačných platforiem, napríklad diskusných fór na internete."[4] Využitie inštitútov TP použitím informačno-technických prostriedkov utajeným spôsobom je konštruované zámerne, čo smeruje k tomu, aby sa ich použitím získali informácie dôležité a významné pre trestné konanie a bola zachovaná ich objektivita. Ak by osoby mali vedomosť, že sa voči nim takéto prostriedky využívajú, ich konanie a správanie by spravidla bolo ovplyvnené tak, aby orgány činné v trestnom konaní a súdy dostali informácie, ktoré by boli skreslené a upravené podľa vôle dotknutej osoby, aby sa vyvrátilo podozrenie o protiprávnej činnosti a zistené informácie by už stratili svoju relevanciu a dôležitosť. Z uvedených dôvodov, teda osoby o ich použití nesmú mať žiadnu vedomosť a počas ich vykonávania je takáto osoba zbavená akejkoľvek možnosti brániť sa proti zásahu do jej práv. Na zachovanie ochrany ich práv pred neoprávnenými, nezákonnými či neodôvodnenými zásahmi sa stanovuje požiadavka, aby o použití týchto prostriedkov boli dodatočne príslušnými orgánmi informované. Možnosť dodatočnej obrany je garantovaná iba osobe, ktorá bola *a posteriori* upovedomená o uskutočnenom zásahu.

Dodatočné informovanie dotknutej osoby o uskutočnenom zásahu do jej práv predstavuje dôležitú súčasť primeraných a účinných záruk proti zneužitiu. Práve informovanosť dotknutej osoby o vykonanom zásahu je nevyhnutným predpokladom, aby bolo možné požiadať o preskúmanie jeho zákonnosti a príp. tiež získať odškodnenie v prípade zistenia jeho neoprávnenosti.[5]

„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 spo-

[4] ALÁČ, M., 2015. Získavanie informácií na spravodajské účely a na účely trestného konania. Bratislava: C. H. Beck. 2015. s. 72 – 73.

[5] KYJAC, Z., 2015. Použitie informačno-technických prostriedkov v trestnom konaní. Odpočúvanie a záznam telekomunikačnej prevádzky. Bratislava: Wolters Kluwer. 2015. s. 223.

ločnosti, 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."[6]

Z existujúcej judikatúry Európskeho súdu pre ľudské práva (ďalej len „ESĽP") je nesporné, že odpočúvaním sa zasahuje do práva na súkromie. 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 na ochranu jeho súkromia na 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.

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. Významným prameňom ochrany ľudských práv je Európsky dohovor o ochrane ľudských práv a základných slobôd (ďalej len Dohovor). Podľa čl. 8 Dohovoru, každý má právo na rešpektovanie svojho súkromného a rodinného života, obydlia 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 ESĽP 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.

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.[7] Na účely ochrany práva na súkromný život ESĽP zdôraznil, že právna úprava každého štátu musí vymedziť jasné a podrobné pravidlá upravujúce rozsah a použitie opatrení zasahujúcich do práva na súkromie. ESĽP 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,

[6] ČENTÉŠ, J., 2013. Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. Bratislava: C. H. Beck. 2013. s. 36.
[7] Rozsudok ESĽP vo veci Huvig vs. Francúzskoz 24. apríla 1990, č. 11105/84.

za ktorých môžu, ale nemusia byť nahrávky vymazané alebo pásky zničené, najmä vtedy, ak bol obvinený zbavený obžaloby vyšetrujúcim sudcom alebo súdom."[8]

Z hľadiska zásahov do práva na súkromie je veľmi dôležitá rozhodovacia činnosť ESĽP 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. Aby nedochádzalo k neoprávnenému, nezákonnému a neodôvodnenému zásahu do práv dotknutej osoby, vydaný súhlas na vykonanie tajného dohľadu nad osobou a s tým spojený zásah do jej súkromia prostredníctvom informačno-technického prostriedku v zmysle ustálenej rozhodovacej činnosti ESĽP, resp. Ústavného súdu SR musí spĺňať tieto tri základné podmienky:

- podmienku legality, ktorá znamená, že štát môže do práva na súkromie zasiahnuť iba na základe zákona a v súlade so zákonom. Preto v rámci legality zásahu sa skúma, či k nemu došlo v súlade s platnými právnymi predpismi. Pričom sa prihliada aj na to, či právny predpis bol verejne publikovaný, a teda dostupný, presný, dostatočne jasný dotknutým osobám a či jeho následky boli predvídateľné, aby osoba vedela predvídať za akých okolností a za akých podmienok sú orgány verejnej moci oprávnené použiť takýto zásah.[9] 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."[10]
- podmienku legitimity. Jej 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 iba v podobe nevyhnutnosti záujmu štátu z dôvodov ochrany národnej bezpečnosti, verejnej bezpečnosti, predchádzania nepokojov a zločinnosti, v záujme spoločnosti z dôvodu ochrany zdravia a morálky, zabezpečenia hospodárskeho blahobytu krajiny a v záujme jednotlivcov z dôvodu ochrany ich práv a slobôd.
- podmienku proporcionality, ktorej splnenie vyžaduje, že k zásahu možno pristúpiť len vtedy, keď je to nevyhnutné (sledovaný cieľ nemožno dosiahnuť miernejšími prostriedkami). Ide o dodržiavanie rovnováhy vo vzťahu medzi právom jednotlivca na súkromie a výberom prostriedkov, ktorými orgán verejnej moci disponuje pri plnení legitímneho cieľa.[11]

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.

S ohľadom na závažnosť zásahu do práv a slobôd jednotlivca prostredníctvom odpočúvania bol vytvorený rámec záruk chrániacich pred jeho zneužitím v trestnom konaní. Za takéto záruky možno považovať:

a) definovanie trestných činov pri ktorých môže byť využité odpočúvanie,
b) stanovenie osôb oprávnených na vydanie príkazu na odpočúvanie,

[8] STRÁŽNICKÁ, V., a kol., 2013. Medzinárodná a európska ochrana ľudských práv. Bratislava: Eurokódex. 2013. s. 400.

[9] ČENTÉŠ, 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. s. 17.

[10] Nález Ústavného súdu SR, II. ÚS 280/09.

[11] ZÁHORA, J., 2018. Uplatňovanie zásady primeranosti a zdržanlivosti pri využívaní informačno-technických prostriedkov v trestnom konaní v Slovenskej republike. In: Časopis pro právní vědu a praxi, XXVI, 1/2018. s. 35, 36.

c) stanovenie náležitostí príkazu na odpočúvanie vrátane pravidiel k vykonávaniu odpočúvania,
d) stanovenie doby trvania odpočúvania,
e) stanovenie pravidiel nakladania so záznamom vrátane podmienok, za ktorých sa záznamy zničia,
f) stanovenie okruhu osôb, ktorým bude poskytnutá informácia o zničení záznamu o vykonanom odpočúvaní,
g) možnosť kontroly zákonnosti vydaného príkazu na odpočúvanie.

Treba podotknúť, že príkaz na použitie tohto inštitútu je utajovanou skutočnosťou a utajuje sa počas celej doby archivácie. Ide o formu rozhodnutia voči ktorému nie je možné podať žiadny opravný prostriedok. Celý procesný postup, od podania návrhu na schválenie príkazu na odpočúvanie, jeho akceptácia oprávneným subjektom až po jeho samotné vykonávanie sa realizuje bez vedomia dotknutých osôb. Hoci ide o závažný zásah do základného práva, dotknuté osoby nemajú možnosť podať opravný prostriedok a o vydaní príkazu sa dozvedia spravidla až dodatočne, keď zásah do práva na súkromie bol realizovaný. Majú preto možnosť žiadať o preskúmanie opodstatnenosti vydania príkazu až dodatočne. Práve následná ochrana dotknutej osoby, ktorej bolo vykonaným odpočúvaním zasiahnuté do práva na súkromie sa zdá, za súčasného platného a účinného stavu v podmienkach Slovenskej republiky problematická.

Kritéria posudzovania zákonnosti vydaného príkazu na odpočúvanie

Právna úprava odpočúvania v trestnom konaní v Slovenskej republike je obsiahnutá v ustanovení § 115 TP. Vydaný príkaz na odpočúvanie a záznam telekomunikačnej prevádzky, musí striktne spĺňať všetky zákonné podmienky, ktorými 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.

Drvivá väčšina odpočúvaní, vzhľadom aj na jeho charakter prebieha v predsúdnej časti konania, v postupe pred začatím trestného stíhania a v prípravnom konaní. Pri využití odpočúvania pred začatím trestného stíhania, bude pri následnom preskúmavaní zákonnosti príkazu na odpočúvanie dôležité preukázanie existencie dôvodného podozrenia o spáchaní jedného z uvedených trestných činov. „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 ods. 1 TP.“[12] 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

[12] ČENTÉŠ, J., 2013. Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. Bratislava: C. H. Beck. 2013. s. 99.

v trestnom konaní vydá ihneď uznesenie o začatí trestného stíhania s uvedením úkonu, ktorým sa trestné stíhanie začalo.

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 v zmysle ustanovenia § 115 ods. 2 TP 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 obydlia. 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.

V konaní pred súdom príkaz vydáva predseda senátu, ktorý má právomoc ho vydať z úradnej povinnosti, bez návrhu prokurátora.

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. 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.“[13] Označenie osoby, ktorá má byť odpočúvaná pritom predpokladá uvedenie jej mena, priezviska, adresy bydliska, prípadne zamestnania a ďalších potrebných identifikačných údajov.[14]
c) určenie času vykonávania odpočúvania. V zmysle ustanovenia § 115 ods. 3 TP odpočúvanie a záznamu telekomunikačnej prevádzky môže trvať najviac šesť mesiacov. Tento čas môže v prípravnom konaní na návrh prokurátora sudca pre prípravné konanie predĺžiť vždy o ďalšie dva mesiace, a to aj opakovane.
d) odôvodnenie, a to aj skutkovými okolnosťami. 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. Pre každú odpočúvanú stanicu musí existovať konkrétny dôvod na použitie tohto inštitútu.

V súvislosti s nutnosťou riadneho odôvodnenia príkazu na odpočúvanie je vhodné spomenúť rozhodovaciu činnosť Ústavného súdu SR, 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 č. 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.“[15]

[13] KYJAC, Z., 2015. Použitie informačno-technických prostriedkov v trestnom konaní. Odpočúvanie a záznam telekomunikačnej prevádzky. Bratislava: Wolters Kluwer. 2015. s. 150.
[14] Nález Ústavného súdu ČR z 23. mája 2007, sp. zn. II. ÚS 615/06.
[15] Nález Ústavného súdu SR zo 4. februára 2009, sp. zn. I. ÚS 117/07.

Realizácia odpočúvania a záznamu telekomunikačnej prevádzky v trestnom konaní prislúcha Policajnému zboru SR. Policajt alebo príslušník Policajného zboru počas trvania odpočúvania je povinný neustále skúmať či dôvody na vydanie príkazu trvajú. Ak dôvody pominuli, je povinný odpočúvanie ukončiť.

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.

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 vykladanie požiadavky súčasného vedenia trestného stíhania v inej trestnej veci.

Povinnosť upovedomenia o zničení záznamu, t. j. povinnosť informovať dotknuté osoby voči ktorým bolo využité odpočúvanie je zakotvené v ustanovení § 115 ods. 9, 10 TP. Predmetné ustanovenie sa vzťahuje len na situácie, ak dôjde k zničeniu záznamu z dôvodu, že pri vykonávaní odpočúvania sa nezistili skutočnosti významné pre trestné konanie. Ide o dosť problematickú požiadavku – „ak sa nezistia skutočnosti významné pre trestné konanie". Orgány činné v trestnom konaní majú povinnosť zisťovať skutočnosti, ktoré svedčia v prospech obvineného s rovnakou starostlivosťou ako skutočnosti, ktoré preukazujú jeho vinu. Uvedená povinnosť je uvedená v ustanovení § 2 ods. 10 TP – „orgány činné v trestnom konaní postupujú tak, aby bol zistený skutkový stav veci, o ktorom nie sú dôvodné pochybnosti, a to v rozsahu nevyhnutnom na ich rozhodnutie. Dôkazy obstarávajú z úradnej povinnosti. Právo obstarávať dôkazy majú aj strany. Orgány činné v trestnom konaní s rovnakou starostlivosťou objasňujú okolnosti svedčiace proti obvinenému, ako aj okolnosti, ktoré svedčia v jeho prospech, a v oboch smeroch vykonávajú dôkazy tak, aby umožnili súdu spravodlivé rozhodnutie." Preto, ak sa pri odpočúvaní zistia skutočnosti, ktoré nepreukazujú vinu obvineného, ide taktiež o skutočnosti významné pre trestné konanie, a z toho dôvodu je ťažké posúdiť, aké požiadavky zákonodarca predpokladal. Spravidla všetky informácie zistené využitím odpočúvania možno považovať za skutočnosti významné pre trestné konanie. V zmysle predmetného ustanovenia teda platí, že iba v prípade, ak sa využitím uvedeného prostriedku zistia skutočnosti, ktoré nie sú významné pre trestné konanie, iba vtedy bude zákonom uložená povinnosť informovať dotknutú osobu realizovaná. Skutočnosť, že sa vyvrátilo podozrenie voči konkrétnej osobe v žiadnom prípade nemožno považovať za situáciu, kedy by sa nezistili skutočnosti významné pre trestné konanie. Uvedená osoba, teda nebude mať právo nahliadať do spisu a túto osobu ani nebude potrebné povinne zákone upovedomiť o použití tohto prostriedku voči nej. Takáto osoba nebude mať žiadnu vedomosť o použití prostriedkov voči nej a z toho dôvodu právo na ochranu svojich práv jej nie je garantované.

Skutočnosti, ktoré nie sú významné pre trestné konanie a z toho plynúce ďalšie povinnosti o informovaní dotknutej osoby nastanú v prípadoch, ak všetky zistené informácie nemajú žiadnu súvislosť s trestným konaním v rámci ktorého bol príkaz vydaný. Následne zostáva na zvážení, na základe akého odôvodnenia bol predmetný príkaz na odpočúvanie vydaný. Záznam, ktorý obsahuje skutočnosti, ktoré nie sú významné pre trestné konanie musí byť bez meškania zničený orgánom činným v trestnom konaní alebo príslušným útvarom Policajného zboru. Zničenie sa vykoná napr. zmazaním CD disku príp. iným spôsobom, zničeniu podliehajú všet-

ky formy v ktorých sa vyhotovovanie vykonalo. Povinnosť zničenia nie je vyčerpaná zničením CD nosičov s uvedenými záznamami, pokiaľ súčasne zostali v spise založené v listinnej podobe. K zničeniu má dochádzať *ex officio*.[16]

TP ustanovuje ďalšie povinnosti v prípade zničenia záznamu o vykonanom odpočúvaní:

- vyhotovenie zápisnice o zničení záznamu a jej založenie do spisu,
- upovedomenie určitých osôb o zničení záznamu,
- lehoty na upovedomenie,
- subjekty povinné poskytnúť upovedomenie,
- zákonné výnimky,
- poučenie o možnosti obrany oprávnených osôb, ktorá spočíva v preskúmaní zákonnosti vydania príkazu na odpočúvanie.

Povinnosť informovať osobu, ktorej sa odpočúvanie týkalo (ak je známa) o zničení záznamu a o použití daných prostriedkov má *a posteriori* policajt alebo prokurátor, ktorého rozhodnutím sa vec právoplatne skončila a v konaní pred súdom predseda senátu súdu prvého stupňa po právoplatnom skončení veci. Lehota na upovedomenie je trojročná a začína plynúť právoplatnosťou skončenia trestného stíhania v konkrétnej trestnej veci.[17] V rámci trestného konania za právoplatne skončenú vec možno považovať iba vec, pri ktorej došlo k rozhodnutiu, ktoré zakladá prekážku *res iudicata*.

Informácia obsahuje označenie súdu, ktorý vydal alebo potvrdil príkaz na odpočúvanie a záznam telekomunikačnej prevádzky, dĺžku vykonávania odpočúvania a dátum jeho ukončenia. Súčasťou informácie je aj poučenie o práve podať v lehote dvoch mesiacov od jej doručenia návrh na preskúmanie zákonnosti príkazu na odpočúvanie a záznam telekomunikačnej prevádzky Najvyššiemu súdu SR. Uvedená informácia tvorí povinnú súčasť poskytnutej informácie o zničení záznamu a je vo forme poučenia.

Povinnosť upovedomenia dotknutých osôb sa nevzťahuje všeobecne na všetky dotknuté osoby. Stanovuje sa pomerne obmedzený okruh osôb, ktoré podliehajú informačnej povinnosti. Právna úprava definuje zákonné výnimky z informačnej povinnosti, ktoré sú odôvodnené účelom vykonávaných úkonov a potrebou ich dosiahnutia a najmä potrebou dosiahnuť účel trestného konania. Informačná povinnosť sa neuplatní v uvedených prípadoch:

a) vo vzťahu k osobe, ktorej sa odpočúvanie týka a má zákonné oprávnenie nazerať do spisu[18] (§ 69 TP), uvedené subjekty majú možnosť sa o zničení záznamu dozvedieť zo zápisnice o zničení, ktorá sa zakladá do spisu.
b) v konaní o obzvlášť závažnom zločine alebo zločine spáchanom organizovanou skupinou, zločineckou alebo teroristickou skupinou, alebo ak
c) sa na trestnom čine podieľalo viacero osôb a vo vzťahu aspoň k jednému z nich nebolo trestné stíhanie právoplatne skončené, alebo ak

[16] Nález Ústavného súdu ČR II. ÚS 789/06.

[17] ČENTÉŠ, J., 2015. Trestný poriadok. Veľký komentár. 2. aktualizované vydanie. Bratislava: Eurokódex. 2015. s. 312 – 313.

[18] Osobami oprávnenými nazerať do spisu podľa § 69 TP sú: obvinený, obhajca, poškodený a zúčastnená osoba, splnomocnenec, ustanovený opatrovník a v konaní pred súdom prokurátor, probačný a mediačný úradník, vyšší súdny úradník, súdny tajomník a asistent prokurátora majú právo nazerať do spisov s výnimkou zápisnice o hlasovaní a časti spisu obsahujúcej údaje o totožnosti chráneného svedka, ohrozeného svedka alebo svedka, ktorého totožnosť je utajená, a krycie údaje o totožnosti agenta, robiť si z nich výpisky a poznámky a obstarávať si na svoje trovy kópie spisov a ich častí; také trovy neuhrádza prokurátor, probačný a mediačný úradník, vyšší súdny úradník, súdny tajomník a asistent prokurátora. Také isté právo má zákonný zástupca obvineného, poškodeného a zúčastnenej osoby, ak tieto osoby sú pozbavené spôsobilosti na právne úkony alebo ich spôsobilosť na právne úkony je obmedzená. Iné osoby tak môžu urobiť so súhlasom predsedu senátu a v prípravnom konaní so súhlasom orgánu činného v trestnom konaní, len ak je to potrebné na uplatnenie ich práv.

d) by poskytnutím takej informácie mohol byť zmarený účel trestného konania.

Ak teda dotknutá osoba (ak je známa) nespadá do okruhu osôb oprávnených nazerať do spisu, ani sa na ňu nevzťahujú zákonné výnimky *a posteriori* ju upovedomí orgán, ktorý vydal rozhodnutie, ktorým bola vec právoplatne skončená a v konaní pred súdom predseda senátu súdu prvého stupňa.

Ako už bolo uvedené pri uskutočňovaní odpočúvania dotknuté osoby nemajú vedomosť o tom, že sa voči nim takéto prostriedky využívajú. To, že osoby počas jeho vykonávania nevedia o ich využití je plne v súlade s podstatou, účelom a právnou úpravou týchto prostriedkov. Po ukončení ich používania, ak tomu nebránia zákonné dôvody, by preto mali byť informované a takomto použití prostriedkov a o uskutočnenom zásahu. Ide o základné východisko pre to, aby v konaní mohli uplatniť svoje práva a to vrátane práva na súdnu a inú ochranu svojich práv. Platná právna úprava sa zdá byť v tejto súvislosti problematická.

„Zo znenia § 115 ods. 8 TP vyplýva, že povinnosť upovedomenia sa nevzťahuje na všetkých účastníkov odpočúvanej telekomunikačnej prevádzky, ale len na osobu (ak je známa), ktorej sa odpočúvanie a záznam telekomunikačnej prevádzky týka (§ 115 ods. 3 TP). Zároveň z uvedeného ustanovenia vyplýva, že táto povinnosť sa neuplatňuje vo vzťahu k osobe, ktorá mala možnosť nazerať do spisu (§ 69 TP).“[19]

Okruh osôb, ktoré nemajú právo nazerať do spisu a nevzťahuje sa na nich ani zákonná podmienka informovať sa teda nebudú mať ako dozvedieť o použití týchto prostriedkov vo vzťahu k nim. Takéto osoby sú zbavené možnosti domáhať sa ochrany svojich práv a právom chránených záujmov.

Súčasná právna úprava síce zakotvuje povinnosť informovať dotknuté osoby o zničení záznamu (resp. o vykonanom zásahu), ale ide len o určité skupiny osôb, nie je stanovená všeobecná povinnosť všetky dotknuté osoby informovať. Mnohé osoby sa o uskutočnenom zásahu do ich práv prostredníctvom odpočúvania nikdy nedozvedia. V takýchto prípadoch absentuje právo na súdnu a inú ochranu ich práv a mnohé osoby sú z takejto ochrany vylúčené z dôvodu právnej úpravy obmedzení pre informačnú povinnosť o uskutočnenom zásahu.

Preskúmanie zákonnosti vydaného príkazu na odpočúvanie a záznam telekomunikačnej prevádzky

Ústavný súd SR vo svojom plenárnom náleze č. k. PL. ÚS 10/2014-78 z 29. apríla 2015 uviedol nasledovné: „Účinná ochrana pred neprípustným zásahom do práva na súkromie dotknutých osôb by mala byť zaručená prostredníctvom povinnosti dodatočne informovať osobu užívateľa služieb elektronickej komunikácie o tom, že prevádzkové a lokalizačné údaje komunikujúcich strán, ktoré sa jej týkajú, boli oznámené orgánom činným v trestnom konaní. Zároveň by dotknuté osoby mali mať k dispozícii právny prostriedok, na základe ktorého by sa bolo možné domáhať súdneho prieskumu postupu orgánov činných v trestnom konaní pri získavaní a nakladaní s predmetnými údajmi. Výnimku z tejto povinnosti by bolo možné pripustiť iba za zákonom ustanovených dôvodov, u ktorých by prevážil záujem na zachovaní utajenia tejto informácie.“

Trestný poriadok bol v kontexte s uvedeným nálezom ústavného súdu novelizovaný z dôvodu rozšírenia ochrany súkromia osoby, do ktorej zasiahli orgány verejnej moci pri odpočúvaní a zázname telekomunikačnej prevádzky.

[19] ČENTÉŠ, J., 2012. Legalita, legitimita a proporcionalita odpočúvania a zaznamenávania telekomunikačnej prevádzky. In: Magister Officiorum, 2012, 2/2012.

Novelou zákona č. 397/2015 Z. z. s účinnosťou od 1. 1. 2016 sa do TP doplnila právna úprava podľa § 362f, ktorá umožňuje osobe, ktorá bola príslušným orgánom informovaná o zničení záznamu podľa § 115 ods. 9 TP, podať návrh na preskúmanie zákonnosti príkazu na odpočúvanie a záznam telekomunikačnej prevádzky. „Dôvodom zavedenia osobitného druhu konania (preskúmanie zákonnosti príkazu) do právneho poriadku bola skutočnosť, že osoba, ktorej sa vydané príkazy bezprostredne dotýkali a bola ich „predmetom" v prípade, ak získané skutočnosti neboli použité ako dôkaz v trestnom konaní, nemala účinný prostriedok na preskúmanie zákonnosti vydania príkazov s výnimkou konania pred ústavným súdom. Ak získané skutočnosti boli použité ako dôkaz v trestnom konaní má osoba, ktorej sa dotýkajú možnosť namietať zákonnosť získania a použitia takéhoto dôkazu v priebehu celého konania využijúc svoje obhajobné práva vyplývajúce z jeho procesného postavenia v konaní o riadnych alebo mimoriadnych opravných prostriedkoch."[20]

Ustanovenie § 115 ods. 9 TP poskytuje určitému okruhu osôb širšiu ochranu zo strany orgánov verejnej moci, pričom oprávnenou osobou podať návrh na preskúmanie zákonnosti príkazu na odpočúvanie je podľa § 362f TP iba osoba uvedená v § 115 ods. 9 TP. Teda uvedené konanie je možné iba na návrh osoby, ktorej bola doručená informácia o zničení záznamu podľa § 115 ods. 9 TP. Z takejto dikcie zákona vyplýva, že ide o veľmi obmedzený okruh osôb a teda osoby, ktoré majú podľa TP právo dozvedieť sa o uskutočnenom odpočúvaní zo spisu alebo sa na osoby vzťahujú zákonné výnimky, takéto právo podať návrh nemajú.

Konanie o preskúmaní zákonnosti príkazu na odpočúvanie a záznam telekomunikačnej prevádzky podľa § 362f a § 362g TP predstavuje osobitný ex post prieskum zákonnosti príkazu na odpočúvanie a záznam telekomunikačnej prevádzky.[21] Uvedené konanie odzrkadľuje článok 13 Dohovoru, podľa ktorého každý, koho práva a slobody priznané týmto dohovorom boli porušené, má právo na účinný opravný prostriedok pred vnútroštátnym orgánom bez ohľadu na to, že porušenie spôsobili osoby pri plnení ich úradných povinností.

Predmetom konania o preskúmaní zákonnosti príkazu na odpočúvanie a záznam telekomunikačnej prevádzky podľa § 362f a § 362g TP je zákonnosť vydania príkazu, ako aj zákonnosť jeho vykonania. Pred samotným rozhodnutím si Najvyšší súd SR vyžiada stanovisko sudcu, ktorý rozhodoval o vydaní alebo potvrdení príkazu podľa § 115 TP. V prípade, ak Najvyšší súd SR zistí, že príkaz na odpočúvanie a záznam telekomunikačnej prevádzky bol vydaný alebo vykonaný v rozpore so zákonom, vysloví uznesením porušenie zákona. Proti tomuto uzneseniu nie je prípustný opravný prostriedok (§ 362g TP). V opačnom prípade, ak Najvyšší súd SR zistí, že príkaz na odpočúvanie a záznam telekomunikačnej prevádzky bol vydaný a vykonaný v súlade s podmienkami podľa § 115 TP, vysloví uznesením, že zákon porušený nebol a proti tomuto rozhodnutiu opravný prostriedok taktiež nie je prípustný.

Za problematické možno považovať na základe akých skutočností Najvyšší súd SR o zákonnosti vydaného príkazu bude rozhodovať. Aby mohol súd zodpovedne posúdiť, či v konkrétnom prípade bol vydaný resp. realizovaný príkaz zákonný, musel by mať k dispozícii predovšetkým také informácie, ktoré mal k dispozícii sudca, ktorý príkaz vydal, vrátane poznatkov operatívnej povahy, ktoré nie je možné zaistiť.[22]

---

[20] Uznesenie Ústavného súdu SR IV. ÚS 627/2018-24.

[21] IVOR, J., POLÁK, P., ZÁHORA, J., 2017. Trestné právo procesné II. Bratislava: Wolters Kluwer, 2017, s. 302 – 303.

[22] JELÍNEK, J., 2017. Odposlech a záznam telekomunikačního provozu v České republice – záruky přezkoumání zákonnosti příkazu k odposlechu. In: Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní. Zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou konanej dňa 23. 3. 2017, Jozef Záhora ed. Praha: Leges. 2017. s. 43.

Avšak zavedenie tohto osobitného ex post prieskumu zákonnosti je potrebné hodnotiť jednoznačne pozitívne z pohľadu garancie ochrany práv, avšak z pohľadu efektívnosti s ohľadom na krátku existenciu tohto osobitného spôsobu konania nie je možné zaujať jednoznačné stanovisko.

V súvislosti s ochranou práv dotknutých osôb treba pripomenúť, že príkaz na odpočúvanie a záznam telekomunikačnej prevádzky má povahu rozhodnutia *sui generis*, teda nejde o uznesenie. Z tohto dôvodu nie je proti nemu prípustný opravný prostriedok a osoba dotknutá odpočúvaním teda nemá možnosť domáhať sa ochrany pred všeobecnými súdmi. Ústavný súd vyslovil názor (I. ÚS 274/2005), že oprávnenosť vydania právoplatného príkazu všeobecný súd nemôže preskúmavať, z dôvodu, že príkaz je právoplatným rozhodnutím, ktorým je súd viazaný, resp. z ktorého musí vychádzať. Uvedené sa vzťahuje 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 SR. V uvedenej súvislosti Ústavný súd SR vyslovil názor: „trestné konanie je od jeho začiatku až po právoplatné skončenie procesom, v ktorom môžu orgány činné v trestnom konaní v rámci vykonávania jednotlivých úkonov a realizácie garancií ochrany základných práv a slobôd napravať, resp. korigovať aj ich prípadné pochybenia. Spravidla až po skončení trestného konania možno na Ústavnom súde SR sťažnosťou podľa čl. 127 ods. 1 Ústavy SR namietať prípadné porušenia základných práv alebo slobôd, ktoré neboli odstránené v jeho priebehu."[23]

Zároveň treba podotknúť, že v situácii, ak sa záznam z telekomunikačnej prevádzky má použiť ako dôkaz v trestnom konaní, osoba, voči ktorej bolo vykonané odpočúvanie, môže namietať zákonnosť takéhoto dôkazu pred všeobecnými súdmi, avšak pri kumulatívnom splnení uvedených podmienok:

- trestná vec dospela do štádia súdneho konania a zároveň
- dotknutá osoba je stranou v trestnom konaní.

O takejto námietke nemôže všeobecný súd odmietnuť rozhodovať.[24]

Prísna limitácia využitia inštitútu odpočúvania a záznamu telekomunikačnej prevádzky má svoj logický a právny základ aj v tom, že nejde o bežný dôkazný prostriedok (napr. výsluchy svedkov, výsluch obvineného, zabezpečenie listinných dôkazov, znaleckých posudkov, obhliadka miesta činu), ale ide o tajné – utajované získavanie dôkazu, čo znamená v porovnaní s ostatnými „bežnými" dôkaznými prostriedkami obzvlášť závažný zásah do základných práv a slobôd – najmä do práva na súkromie. Z uvedeného dôvodu je aj právna úprava použitia odpočúvania v porovnaní s právnou úpravou dôkazných prostriedkov bez utajovaného charakteru zužujúca a obmedzujúca. Limitáciou použitia záznamu z odpočúvania stanovuje aj ustanovenie § 115 ods. 8 TP, v ktorom je uvedené, že ak sa pri jeho vykonávaní nezistili skutočnosti významné pre trestné konanie, orgán činný v trestnom konaní alebo príslušný útvar Policajného zboru musí získaný záznam predpísaným spôsobom zničiť. Z uvedeného *argumentum a contrario* vyplýva, že ak by sa pri odpočúvaní zistili skutočnosti významné napríklad pre správne (administratívne) konanie, ale nešlo by o skutočnosti významné pre trestné konanie, získaný záznam by musel byť predpísaným spôsobom a bez meškania zničený. Ak boli takéto záznamy získané podľa TP, ich použitie je možné výlučne iba v trestnom konaní za prísneho splnenia zákonných podmienok uvedených v ustanovení § 115 TP. Vzhľadom na to, že ide o závažný zásah do práva na súkromie použitím uvedeného prostriedku, ustanovenie § 115 ods. 8 TP neumožňuje a vylu-

[23] ČENTÉŠ, J., 2013. Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. Bratislava: C. H. Beck. 2013, s. 209.
[24] Rozsudok ESĽP z 24. augusta 1998 vo veci Lambert vs Francúzsko.

čuje vyhotovený záznam z odpočúvania získaný použitím informačno-technického prostriedku podľa § 115 TP, použiť mimo trestného konania. Iná situácia je v prípade, ak informačno-technické prostriedky boli použité na základe súhlasu sudcu podľa zákona o ochrane pred odpočúvaním, vtedy môžu byť záznamy z ich použitia vo forme záznamu z odpočúvania prebraté do trestného konania. Ich prípustnosť v trestnom konaní umožňuje ustanovenie § 119 ods. 2 TP.[25]

Záver

Na záver treba uviesť, že odpočúvanie a záznam telekomunikačnej prevádzky má jednoznačný zmysel a nenahraditeľný význam v trestnom konaní aj napriek tomu, že jeho prostredníctvom dochádza k jednému z najzásadnejších zásahov do súkromia dotknutých osôb. Trestný poriadok striktne vymedzuje podmienky jeho využitia. Pre odpočúvanie a záznam telekomunikačnej prevádzky je charakteristický utajovaný spôsob použitia, pričom dotknuté osoby o takomto použití informačno-technického prostriedku nemajú vedomosť a o jeho realizácii sa môžu potenciálne dozvedieť až dodatočne ex post, keď už zásah do práva na súkromie bol realizovaný.

Vzhľadom na to je potrebné, aby v demokratickom právnom štáte existoval dostatočný a efektívny systém garancií ochrany práv pred zásahmi, ktoré sú nezákonné, neprimerané a neodôvodnené. Takúto garanciu ochrany práv pred zásahmi by mala zabezpečovať ta právna úprava, ktorá použitie takýchto invazívnych zásahov umožňuje. Garancia ochrany práv by mala byť premietnutá v právnej úprave takým spôsobom, že právna úprava upravuje konkrétne podmienky, za ktorých sa odpočúvanie a záznam telekomunikačnej prevádzky môže využiť, stanovuje sa okruh trestných činov, pri ktorých je daný inštitút možné nariadiť, fázy konania, v ktorých je možné tento inštitút vykonávať, stanovený je aj subjekt oprávnený rozhodnúť o jeho použití, písomná forma príkazu, jeho odôvodnenie, možnosti využitia zistených informácií, úprava spôsobu kontroly dodržiavania zákonnosti pri jeho využívaní a v neposlednom rade sú upravené možnosti informovania dotknutých osôb.

Vzhľadom k princípom právneho štátu je nutné, aby osoba dotknutá vykonávaním odpočúvania bola o takomto zásahu do jej práv a právom chránených záujmov *ex post* informovaná a mala právnym poriadkom garantovanú možnosť v prípade jeho neoprávnenosti sa proti nemu brániť právnou cestou, čo sa javí pri súčasnej právnej úprave, ktorá výrazne obmedzila okruh osôb aktívne legitimovaných domáhať sa ochrany na Najvyššom súde SR, ako značne problematické a vzhľadom na to je potrebné danej problematike venovať väčšiu pozornosť.

Literatúra

ALÁČ, M., 2015. Získavanie informácií na spravodajské účely a na účely trestného konania. Bratislava: C. H. Beck. 2015. s. 165. ISBN 978-80-89603-32-9.

ČENTÉŠ, J., 2013. Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. Bratislava: C. H. Beck. 2013. s. 272. ISBN 978-80-89603-09-1.

ČENTÉŠ, J., a kol., 2015. Trestný poriadok. Veľký komentár. 2. aktualizované vydanie. Bratislava: Eurokódex. 2015. s. 955. ISBN 978-80-8155-057-7.

ČENTÉŠ, 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.

[25] PERHÁCS, Z., 2014. Kolízia verejného záujmu a ochrany práv pred použitím niektorého z dôkazných prostriedkov. In: Bulletin slovenskej advokácie. Bratislava: Slovenská advokátska komora. č. 10–11/2014. s. 16.

IVOR, J., POLÁK, P., ZÁHORA, J., 2017. Trestné právo procesné II. Bratislava: Wolters Kluwer, 2017, s. 528. ISBN 978-80-8168-593-4.

JELÍNEK, J., 2017. Odposlech a záznam telekomunikačního provozu v České republice – záruky přezkoumání zákonnosti příkazu k odposlechu. In: Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní. Zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou konanej dňa 23. 3. 2017, Jozef Záhora ed. Praha: Leges. 2017. s. 37 – 43. ISBN 978-80-7502-206-6.

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.

PERHÁCS, Z., 2014. Kolízia verejného záujmu a ochrany práv pred použitím niektorého z dôkazných prostriedkov. In: Bulletin slovenskej advokácie. Bratislava: Slovenská advokátska komora. č. 10–11/2014. s. 12 – 21. ISSN 1335-1079.

STRÁŽNICKÁ, V., a kol., 2013. Medzinárodná a európska ochrana ľudských práv. Bratislava: Eurokódex. 2013. s. 560. ISBN 978-80-8944-795-4.

ZÁHORA, J.: Uplatňovanie zásady primeranosti a zdržanlivosti pri využívaní informačno-technických prostriedkov v trestnom konaní v Slovenskej republike. In: Časopis pro právní vědu a praxi, XXVI, 1/2018. s. 30 – 39. ISSN 1805-2789.

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

Theoretical and Practical Problems of Using Information and Technical Resources in Criminal Proceeding

Barbora Dorkinová[1]

Abstrakt: *Príspevok sa zaoberá teoretickými a praktickými problémami využívania informačno-technických prostriedkov v trestnom konaní. Cieľom tohto odborného článku je zadefinovať pojem informačno-technické prostriedky v trestnom konaní v medziach právnych predpisov Slovenskej republiky, ako aj v intenciách právnych predpisov medzinárodného, resp. Európskeho práva. V neposlednom rade je snahou poukázať na súčasné a najčastejšie teoretické a praktické problémy využívania tohto inštitútu pri objasňovaní a vyhodnocovaní kriminality, ktorý každým dňom nadobúda na svojom význame.*

Abstract: *The article deals with the theoretical and practical problems with application of information and technical resources in criminal proceeding. The intention of this article is to define the concept of an information and technical resources in criminal proceeding within the legal regulations of the Slovak Republic, as well as in international law, respectively European law. Last but not least to point out the current and most frequent theoretical and practical problems of application of this institute in clarifying and evaluating criminality, that becomes more important every day.*

Kľúčové slová: *informačno-technické prostriedky, trestné konanie, informácie získané informačno-technickými prostriedkami ako dôkaz, dokazovanie, zákonnosť, zásah do základných ľudských práv a slobôd*

Key words: *information and technical resources, criminal proceeding, information obtained by informatical and technical resources as evidence, probation, the legality, interference with fundamental human rights and freedoms*

Úvod

Korektný vzťah medzi štátnou mocou a občanmi možno pokladať za základný predpoklad riadneho fungovania demokratického štátu. V súčasnosti má významné miesto v spoločnosti tzv. informačná moc, ktorá predstavuje určitú tenkú hranicu medzi samotným zásahom a rešpektovaním základných ľudských práv a slobôd garantovaných nielen zákonom č. 460/1992 Zb. Ústava Slovenskej republiky (ďalej len „Ústava SR“), ale aj inými právnymi predpismi Slovenskej republiky, ako aj právnymi predpismi medzinárodného charakteru. Preto akékoľvek vybočenie z tejto pomyselnej sféry by znamenalo zásah do základných ľudských práv a slobôd, čo predstavuje právo relatívne, a to vzhľadom na skutočnosť, že takéto zásahy sú za určitých podmienok a v určitom rozsahu dovolené do takej miery a takým spôsobom, ako to definuje príslušný právny predpis.

Stanovené hranice zákonodarnou mocou nie sú jediným prostriedkom pre efektívne dodržiavanie a rešpektovanie základných ľudských práv dnešnou spoločnosťou. Za ďalší účinný element slúžiaci pre určovanie hraníc využívania informačno-technických prostriedkov možno považovať aj celú judikatúru, vytváranú v tomto smere alebo súvisiacu s využívaním informačno-technických prostriedkov, t. j. v tejto súvislosti prijaté rozhodnutia Ústavného súdu Slo-

[1] Mgr. Barbora Dorkinová, Ústav verejného práva, Fakulta práva, Paneurópska vysoká škola, Bratislava, e-mail: barbora.dorkinova@paneurouni.com.

venskej republiky, Najvyššieho súdu Slovenskej republiky, krajských súdov a okresných súdov Slovenskej republiky na vnútroštátnej úrovni. Na medzinárodnej úrovni sú to rozhodnutia Európskeho súdu pre ľudské práva, ktoré rešpektujú a na základe ktorých rozhodujú naše vnútroštátne súdy.

Vzhľadom na veľmi citlivú problematiku predstavujúcu zásah do základných ľudských práv a slobôd jednotlivca možno konštatovať, že nejde o štandardné procesné postupy získavania informácií ako dôkazu pre potreby trestného konania. Je dôležité, aby takto získané informácie boli len tými nevyhnutnými k dosiahnutiu účelu trestného konania. Tieto informácie nemôžu dotknuté osoby vystaviť ohrozeniu dôstojnosti a spôsobiť ich znevýhodnenie voči ostatným osobám. Súkromie je chápané ako oblasť, do ktorej sa môže zasahovať len na základe súhlasu jednotlivca (okrem zákonom stanovených výnimiek). Toto zohľadňuje zásada zdržanlivosti a primeranosti, ktorá bola v rámci rekodifikácie trestného práva procesného pridaná do zákona č. 301/2005 Z. z. Trestný poriadok (ďalej len „Trestný poriadok“) .

Skúsenosťami a praxou zo zahraničia v oblasti efektívneho využívania informačno-technických prostriedkov v trestnom konaní, sa medzinárodná právna úprava stala inšpiráciou aj pre zákonodarcov Slovenskej republiky.

Právna úprava a pojem „informačno-technický prostriedok ako dôkazný prostriedok v trestnom konaní“

Právna úprava problematiky informačno-technických prostriedkov v trestnom konaní je na území Slovenskej republiky vymedzená zákonným spôsobom, a to v zmysle ust. § 10 ods. 21 Trestného poriadku, a to nasledovne: *„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 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 dovolávať povinnosti mlčanlivosti podľa osobitných zákonov“*.

Druhým podstatným právnym predpisom, na základe ktorého môže dôjsť k použitiu informačno-technických prostriedkov, je 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) (ďalej len „Zákon o ochrane pred odpočúvaním“).

Osobitnými zákonmi upravujúcimi túto problematiku je napr. zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „Zákon o ochrane osobných údajov“), zákon č. 1/2014 Z. z. o organizovaní verejných športových podujatí a o zmene a doplnení niektorých zákonov (ďalej len „Zákon o organizovaní verejných športových podujatí“), ako aj zákon Národnej rady Slovenskej republiky č. 171/1993 Z. z. o Policajnom zbore. Tieto právne predpisy sa použijú vo vzťahu k Trestnému poriadku subsidiárne.

V súvislosti s problematikou využívania informačno-technických prostriedkov v trestnom konaní je možné považovať za dôležité aj vymedzenie pojmu „trestné konanie", a to vzhľadom k tomu, že efektívne využívanie informačno-technických prostriedkov smeruje k rozhodovacej fáze trestného konania.

Podľa ust. § 10 ods. 15 Trestného poriadku: *„Trestné konanie 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."*.

Výsledkom použitia informačno-technických prostriedkov alebo prostriedkov operatívno-pátracej činnosti v trestnom konaní sú informácie, ktoré môžu viesť k úspešnému odhaleniu trestnej činnosti, k objasneniu trestného činu, k zisteniu páchateľa trestného činu a v konečnom dôsledku môžu závažným spôsobom ovplyvniť rozhodovaciu činnosť orgánov činných v trestnom konaní v štádiu prípravného konania, činnosť prokuratúry a v konečnom dôsledku samotnú rozhodovaciu činnosť súdov. Takto získané informácie sa považujú za dôkazný prostriedok podľa ust. § 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"*.

Okrem vyššie uvedeného je však potrebné naplnenie určitých základných podmienok, aby mohla byť informácia získaná použitím informačno-technických prostriedkov vyhodnotená ako dôkaz, a to:

„– *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;*
– *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."*.[2]

Odhaľovanie, objasňovanie, či vyšetrovanie najzávažnejších trestných činov, ako sú trestné činy, ktoré majú vysokú formu organizovanosti a utajovanosti, ich kontrola, či prevencia sa neodmysliteľne spájajú s využívaním inštitútov, ktorých cieľom je zabezpečiť informácie potrebné na úspešné dosiahnutie nielen vyriešenia konkrétnej trestnej činnosti, ale aj páchania ďalšej kriminality.

Využívaním takýchto špecifických prostriedkov získavania informácií však dochádza k obmedzeniam práv jednotlivcov, a to spôsobom zásahu do ich základných práv a slobôd. Tieto práva jednotlivcov vyplývajú z právneho predpisu, ktorý má v rámci Slovenskej republiky najvyššiu právnu silu, a to Ústavy SR. Podľa čl. 1 ods. 1 Ústavy SR: *„Slovenská republika je zvrchovaný, demokratický a právny štát. Neviaže sa na nijakú ideológiu ani náboženstvo."*, pričom ak ide o ochranu práv občanov, takýto zásah je štátom a spoločnosťou tolerovateľný. V prípade, ak je takýto *„zásah považovaný za narušenie práva na súkromie, tak či je považovaný za zásah:*

– *legálny (tzn. že zákon upravujúci štátom nariadené tajné sledovanie musí byť prístupný pre každého, aby mohol prispôsobiť svoje správanie, pričom musí byť formulovaný dostatočne zrozumiteľne a určito, aby bolo možné vymedziť osoby, ktoré môžu byť sledované, určiť pod-*

[2] IVOR, J. a kol.: Optimalizácia prípravného konania trestného. Prvé vydanie. Praha: Leges, 2017, s. 337 – 338.

mienky 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),*
- *subsidiárny(tzn. nevyhnutný, kedy účel trestného konania nemožno dosiahnuť inou, miernejšou formou).".*[3]

Pri takomto prekračovaní zákonných hraníc treba mať na zreteli, že *„medze základných práv a slobôd možno upraviť za podmienok ustanovených touto ústavou len zákonom, že zákonné obmedzenia základných práv a slobôd musia platiť rovnako pre všetky prípady, ktoré spĺňajú ustanovené podmienky a že pri obmedzovaní základných práv a slobôd sa musí dbať na ich podstatu a zmysel. Takéto obmedzenia sa môžu použiť len na ustanovený cieľ."*, a to s poukazom na čl. 13 ods. 2, 3, 4 Ústavy SR.

Takto upravená problematika využívania informačno-technických prostriedkov v trestnom konaní vo svetle slovenskej právnej úpravy má veľký význam pre občanov Slovenskej republiky, ako aj pre vzťah občana a právneho štátu, z hľadiska tzv. sebaobmedzenia štátnej moci právom. Naopak, medzinárodnoprávna, resp. Európska právna úprava má veľký dosah nielen na občanov a štát, t. j. Slovenskú republiku, ale určuje pravidlá dodržiavania legality, legitimity a proporcionality pre všetky členské štáty Európskej únie.

Na základe vyššie uvedenej skutočnosti je potrebné venovať náležitú pozornosť Ústavnému zákonu č. 23/1991 Zb. Ústavný zákon, ktorým sa uvádza Listina základných práv a slobôd ako ústavný zákon Federálneho zhromaždenia Českej a Slovenskej Federatívnej Republiky a Dohovoru o ochrane ľudských práv a základných slobôd, v ktorých sú zakotvené najdôležitejšie práva a slobody patriace a ochraňujúce fyzické osoby.

V uvedených dokumentoch sú v zásade práva fyzických osôb zadefinované veľmi podobne, pričom ich význam zostáva zachovaný.

Trestné konanie ako jeden z druhov súdneho konania sa pokladá za konanie, v ktorom najčastejšie pristupuje štátna moc k obmedzeniam základných ľudských práv a slobôd prostredníctvom najvyšších možných inštancií. Na úrovni vnútroštátnej prostredníctvom Ústavného súdu Slovenskej republiky (nie však výlučne), ako aj na medzinárodnej úrovni prostredníctvom Európskeho súdu pre ľudské práva.

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

Informačno-technické prostriedky v trestnom konaní sa využívajú pri odpočúvaní a záznamе telekomunikačnej prevádzky, vyhotovovaní obrazových, zvukových alebo obrazovo-zvukových záznamov, pri vyhľadávaní, otváraní a skúmaní zásielok, tak ako to ustanovuje Trestný poriadok.

Odpočúvanie a záznam telekomunikačnej prevádzky:

V dnešnej modernej dobe je odpočúvanie telefonických rozhovorov, krátkych textových správ (SMS), poprípade iných foriem elektronickej komunikácie technologicky jednoduchšia záležitosť, a to najmä vzhľadom na moderné a funkčné technické vybavenie, ktoré slúži práve na zisťovanie a spracovanie nadobudnutých údajov.

[3] IVOR, J. a kol.: Optimalizácia prípravného konania trestného. Prvé vydanie. Praha: Leges, 2017, s. 336 – 337.

Prostredníctvom telekomunikačného zariadenia, ako je napr. telefón, telefax, mobilný telefón alebo pager dochádza k prenosu informácie a v tejto súvislosti hovoríme o telekomunikačnej prevádzke.

V súčasnosti neexistuje zákonná definícia tohto pojmu, avšak viacerí odborníci sa zhodujú na tom, že presná terminologická úprava by dopomohla k lepšiemu výkladu tohto pojmu v súvislosti s preukázaním dôkazu v trestnom konaní. Fyzické osoby sa tak odvolávajú na právne predpisy z minulosti, čo môže spôsobovať značné problémy najmä pri výklade alebo nepresnosti tohto pojmu.

Odpočúvanie mobilného telefónu, resp. elektronickej komunikácie podozrivej osoby je jedným z najbežnejších spôsobov získavania informácie, v rámci záznamu telekomunikačnej prevádzky. Príkaz sa vydáva v situáciách, ak by nebolo možné dosiahnuť sledovaný účel iným spôsobom. Náležitosti z formálneho hľadiska takto vydaného príkazu nevyplývajú z Trestného poriadku, aj keď je možné ich predpokladať. Z praktického hľadiska to však môže byť problémom a možno tvrdiť, že „*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, že to, že návrhy nemajú presne určené náležitosti, často spôsobuje ich rôzne posudzovanie z pohľadu posudzujúceho sudcu.*“.[4]

Ďalším problémom môže byť dĺžka využívania tohto informačno-technického prostriedku v trestnom konaní a to z dôvodu, že „*Vydaný príkaz na použitie informačno-technických prostriedkov nemôže byť formulovaný akosi ‚otvorene‘ teda tak, že by sa vzťahoval aj na vopred neznáme osoby, ktoré iba pravdepodobne, na základe domnienok polície, v budúcnosti mali spáchať tzv. vybraný druh trestného činu. Inými slovami, príkaz na použitie informačno-technického prostriedku môže byť vydaný len vtedy, ak už reálne existuje skutok právne kvalifikovaný ako trestný čin, na ktorý možno za splnenia ďalších zákonom stanovených prísnych podmienok príkaz vydať.*“,[5] keďže z Trestného poriadku vyplýva, že maximálna doba ich využívania je stanovená na 6 mesiacov s tým, že je možné túto dobu predĺžiť o ďalšie 2 mesiace, a to aj opakovane. Problém nastáva aj z pohľadu neexistencie zákonného limitu týkajúceho sa možnosti využitia predĺženia týchto informačno-technických prostriedkov alebo v akej lehote by vôbec mohli subjekty žiadať o predĺženie tejto lehoty. Táto skutočnosť tak v mnohých prípadoch spôsobuje, že príslušný sudca rozhoduje o zákonnosti takého odpočúvania, či samotných dôvodov, na základe ktorých sa žiada o predĺženie zákonnej lehoty pod časovým stresom, čo môže spôsobiť nesprávne posúdenie veci.

V súvislosti s vyhľadávacou zásadou môže dôjsť k problému nesprávneho alebo nedostatočného vyhodnotenia orgánov činných v trestnom konaní o skutočnosti, či je alebo nie je významná v trestnom konaní. Je možné tvrdiť, že je na vlastnom uvážení príslušného subjektu ako vyhodnotí dôležitosť daného dôkazu pre ten konkrétny prípad, čo v praktickej rovine môže priniesť viacero problémov.

V zmysle ust. § 115 ods. 7 Trestného poriadku: „*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.*“. Súdy

[4] TITTLOVÁ, M.: Teoretické a praktické problémy odpočúvania telekomunikačnej prevádzky, In Zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou na tému Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní. Bratislava: FP PEVŠ 2017, s. 189 – 190.

[5] PERHÁCS, Z.; PERHÁCSOVÁ, A.: Právna úprava používania informačno-technických prostriedkov (2. časť). Justičná revue č. 5/2013, Bratislava: Ministerstvo spravodlivosti SR, s. 706.

Slovenskej republiky majú na túto problematiku rôzne názory. V rozhodnutí Najvyššieho súdu Slovenskej republiky je dokonca vyjadrený názor tohto súdu, a to že *„Nezodpovedá vecnej logike, aby zákon požadoval ako podmienku dôkaznej použiteľnosti informácie súčasné vedenie trestného konania vo veci, v ktorej bola táto informácia v inom trestnom konaní použitá"*.[6] V prípade splnenia procesnoprávnej podmienky, t. j. podmienky, že je vedené trestné konanie v inej veci je problémom práve samotný výklad tohto ustanovenia, keďže Trestný poriadok nám nedáva presnú definíciu čo možno považovať pod pojmom „súčasné vedenie trestného stíhania". Je možné polemizovať o tom, či ide o situáciu, keď sa uskutočňuje záznam telekomunikačnej prevádzky alebo o situáciu, keď sa už vykonal záznam z telekomunikačnej prevádzky a má byť použitý ako dôkaz v trestnom konaní. Zákonodarca nám nedáva jednotnú odpoveď na túto problematiku, a dokonca dochádza k rozporu so zásadou prejudiciality súdnych rozhodnutí.

Verejná moc však musí za každých okolností rešpektovať princípy právneho štátu a právna ochrana jednotlivca nemôže byť nadmerne obmedzená nakoľko dôkazy nezískané zákonným spôsobom Trestný poriadok jednoznačne vylučuje. Dôležité je naplniť povinnosť zničenia záznamu telekomunikačnej prevádzky a informovanie osoby o skutočnosti, že bola odpočúvaná. Odposluch telefónneho hovoru je veľmi zložité v bežných podmienkach zistiť, alebo zmerať a dotknutá osoba sa častokrát dozvie o vykonaní odpočúvania iba zo spisu.

Vzhľadom k tomu, že pri realizácii takéhoto spôsobu získavania informácií dochádza k zásahom do viacerých základných práv a slobôd, ako je právo na súkromie alebo právo na rodinný život je potrebné narábať s takýmito informáciami opatrne. Každé rozhodnutie o použití informačno-technického prostriedku, či kladné, alebo záporné musí byť príslušným sudcom zdôvodnené.

Platí to najmä pre Policajný zbor Slovenskej republiky, poprípade Slovenskú informačnú službu, Zbor väzenskej a justičnej stráže, Finančnú správu alebo Železničnú políciu, ktoré sú oprávnené disponovať s takýmito informáciami, s čím súvisí aj problém úniku takto získaných údajov. V nedávnej minulosti sa na Slovensku častokrát riešil problém nezákonného, alebo nesprávne vykonaného odpočúvania. Cudzie nám nie sú ani kauzy, kde si inštitúcie, ktoré majú k odpočúvacím systémom prístup nimi samotnými riešia interné problémy úniku informácií. Problémom môže byť aj doba trvania odpočúvania, nakoľko policajní príslušníci, ktorí odpočúvanie samostatne technicky vykonávajú, musia počas celého procesu skúmať trvanie dôvodov pre túto činnosť. To isté platí aj pre sudcu, ktorý je povinný priebežne sledovať, či je ešte na odpočúvanie relevantný dôvod.

Ide najmä o trestné činy korupčné, alebo pri trestnej činnosti, kde je páchateľom verejný činiteľ.

Zásada subsidiarity naznačuje, že takýto postup by sa mal použiť až v prípade, keď je nasadenie iných prostriedkov neefektívne, alebo získať dôkaz týmto spôsobom by bolo nemožné.

Vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov:

Hovoríme o informačno-technickom prostriedku nazývanom aj ako veľký odposluch, resp. priestorový odposluch, ktorý má veľký význam v trestnom konaní. *„Obrazovo-zvukový záznam je teda vo svojej podstate informačno-technický prostriedok vykonávaný utajovaným spôsobom, ktorý má charakter dôkazného prostriedku a slúži na zisťovanie a uchovávanie skutočností významných pre trestné konanie"*.[7]

[6] Rozhodnutie Najvyššieho súdu Slovenskej republiky zo dňa 7. 2. 2012, pod sp. zn. 2 To 5/2011, s. 17.

[7] IVOR, J.: Obrazovo-zvukový záznam ako dôkazný prostriedok v trestnom konaní, In Zborník príspevkov z celoštátnej konferencie s medzinárodnou účasťou na tému Teoretické a praktické problémy dokazovania. Bratislava: FP PEVŠ 2008, s. 72.

Príznačné je teda pre tento inštitút sledovanie získavania informácií, musí sa viazať na vopred získaný príkaz, ide o dôkazný prostriedok v trestno-procesnej rovine. Vzhľadom k vyššie uvedenému možno tvrdiť, že ak by došlo k prezradeniu informácie sledovanej osobe, že je sledovaná a že sa vyhotovuje obrazový, zvukový alebo obrazovo-zvukový záznam jej správania, mohlo by tak dôjsť k zmareniu sledovaného cieľa, a to získania čo najpresnejších a najhodnovernejších informácií vyhotovených na určitom mieste a v určitom čase, najčastejšie spravodajským spôsobom. Vyhotovovanie audio vizuálnych záznamov je možné len na základe súhlasu zákonného sudcu podľa zásady judiciarity. Cieľom je minimalizovať možné negatívne dopady zásahov do garantovaných práv. Súhlas sudcu musí byť vydaný vopred, a to písomnou formou so všetkými minimálne vyžadovanými náležitosťami. Tento súhlas obsahuje aj čas využitia daného prostriedku a špecifikuje miesto využitia aj pre priestory, ktoré nie sú verejne dostupné. Opäť je dôležité daný inštitút využívať len počas najnevyhnutnejšieho časového intervalu na dosiahnutie účelu a aj to však maximálne po dobu 6 mesiacov, ktorá však môže byť predĺžená.

Problém nastáva, ak sú takéto informácie, získavané vyššie spomínaným spôsobom aj na mieste a v čase, keď sa táto osoba nachádza v domáckom prostredí, čím najčastejšie dochádza k porušovaniu práva na súkromie.

Aj v tomto prípade dochádza k výkladovému problému ustanovenia Trestného poriadku (podobne ako aj v prípade inštitútu odpočúvania a záznamu telekomunikačnej prevádzky) v súvislosti s výkladom pojmu skutočnosti, ktoré sú alebo nie sú významné pre trestné konanie. Ani pri tomto využívaní informačno-technického prostriedku nám zákonodarca neustanovuje jasnú odpoveď.

Ďalším relevantným problémom môže byť zlyhanie ľudského faktora, teda neodbornosť a nedostatočná teoretická a technická príprava osôb obsluhujúcich takéto technické zariadenia, čím sa takto získaná informácia stáva v praxi nepoužiteľnou, a práve preto je potrebné pracovať s takýmito údajmi podľa uváženia a potreby. V konečnom dôsledku je teda najväčšou obavou práve zmarenie účelu trestného konania.

Vyhľadávanie, otváranie a skúmanie zásielok:

Inštitút vyhľadávania, otvárania a skúmania zásielok ako prostriedok na zaistenie dôkazov sa v bežnej praxi používa často. Je s ním spojená výhoda, že môže mať rôznu formu, či už ako listina, audio-video záznam, resp. inú zaznamenateľnú formu dôkazu v trestnom konaní. V štádiu pred vydaním príkazu na otvorenie alebo zadržanie obsahu zásielky musel existovať dôvodný predpoklad, že zásielka môže obsahovať informácie, ktoré významnou mierou môžu ovplyvniť trestné konanie. Toto je aj dôvodom kedy je ústavou garantované právo na listové tajomstvo, tajomstvo dopravovaných správ a iných písomností upravené zákonom.

V súvislosti s trestným konaním hovoríme o zásielke v zmysle ust. § 108 ods. 1 a 2 Trestného poriadku, a teda: *„zásielke, ktorá pochádza od obvineného alebo je mu určená“* a *„zásielke, pri ktorej je dôvodné podozrenie, že ňou bol spáchaný taký trestný čin alebo s takým trestným činom súvisí“*. Vzhľadom ku skutočnosti, že prepravu takýchto zásielok zabezpečuje Slovenská pošta alebo súkromný prepravca, aj v tomto prípade môže dôjsť k zlyhaniu ľudského faktora, a teda k strate takejto zásielky, a tak nie je možné jej prípadné zadržanie a následné otvorenie a skúmanie jej obsahu.

Orgány činné v trestnom konaní využívajú tento inštitút získavania zásielok ojedinele a jednorázovo.

Záver

Využívanie informačno-technických prostriedkov v trestnom konaní predstavuje veľmi zložitú problematiku v oblasti Trestného práva, či už z pohľadu odbornej alebo laickej verejnosti.

Využívanie informačno-technických prostriedkov za účelom zisťovania dôležitých informácií pre trestné konanie je častokrát zdrojom konfliktu záujmov jednotlivca a spoločnosti pri odhaľovaní najzávažnejších foriem trestných činov. Problémom sa stáva účasť štátu a jeho intervencia do sféry osobných práv občanov. Miniaturizácia a rapídny vývoj na poli využívania informačno-technických prostriedkov v posledných rokoch spôsobili, že fyzické osoby si mnohokrát ani nie sú vedomé a priamo nevnímajú, že tieto technológie a prostriedky boli v súvislosti s nimi samými využité. Bez dodatočného informovania dotknutej osoby, alebo možnosti domáhania sa preverenia legitímnosti tohto konania verejnej moci, je veľmi ťažké definovať nástroj, ktorý dokáže vylúčiť neopodstatnené využitie informačno-technických prostriedkov a ich nelegitímny, resp. nadbytočný zásah do súkromia.

Otázkou a predpokladom pre diskusiu je, či je možné považovať síce zákonne získaný dôkaz, ktorý je súčasne dôkazom získaným protiústavne (t. j. v tom zmysle, že pri jeho získavaní boli narušené určité ústavné práva jednotlivca), za dôkaz získaný v súlade s právom na spravodlivé súdne konanie.

Dôležitou úlohou zákonodarcu je práve tvorba akejsi rovnováhy medzi vyššie spomínanými odlišnými záujmami. V týchto intenciách je pozitívom skutočnosť, že v súčasnosti sú dobre spracované teoretické stanoviská týkajúce sa využívania informačno-technických prostriedkov v trestnom konaní, ktoré sa využívajú najmä pri získavaní dôkazov pri trestných činoch, pre ktoré je charakteristická vysoká organizovanosť. V praxi sa však často vyskytujú určité nezrovnalosti, a to najmä pri výklade niektorých ustanovení alebo už pri ich samotnej aplikácii do praxe. Zákonodarca nám teda nedáva presnú a jednoznačnú odpoveď na otázku, či dôkaz získaný cestou protiústavnou možno považovať za dôkaz získaný v súlade s právom na spravodlivé súdne konanie.

Je tak potrebné, ba až žiaduce prísne posudzovanie a dodržiavanie splnenia zákonných podmienok ustanovených k využívaniu informačno-technických prostriedkov v trestnom konaní tak, aby čo najmenej, resp. vôbec nedochádzalo k zásahom do súkromia a práv jednotlivca.

Prostriedky zabezpečovania informácií sú neodmysliteľnou súčasťou získavania dôkazov zákonným spôsobom, prostredníctvom ktorých je možné dosiahnuť účel trestného konania.

Bez využívania informačno-technických prostriedkov by v dnešnej dobe dochádzalo k značným komplikáciám v štádiu zabezpečovania informácií, ako aj v štádiu rozhodovacej činnosti príslušného subjektu v trestnom konaní. Dostupnosť týchto nástrojov poskytuje priestor na objektívnejšie posúdenie všetkých okolností a môže významným spôsobom v konečnom dôsledku ovplyvniť správne a zákonné rozhodnutie v konkrétnom trestnom konaní.

Na záver si dovolím vyjadriť svoj názor, a to že pristupujem k využívaniu informačno-technických prostriedkov v trestnom konaní kladne, a to najmä, avšak nielen vzhľadom na skutočnosť, že aj na základe takto získaných a zabezpečených informácií dochádza k úspešnému odhaľovaniu trestnej činnosti, jej vyšetrovaniu a jej spravodlivému a zákonnému postihovaniu. V kontexte s celkovým trestným konaním tak využívanie informačno-technických prostriedkov prispieva aj k napĺňaniu jednak preventívnej a jednak sankčnej funkcii trestného konania.

Vzhľadom na veľmi rozsiahlu a komplikovanú problematiku je nutné dodať, že aj napriek uvedeným skutočnostiam je potrebné mať na zreteli obavu z legislatívneho, procesného a metodického riešenia týchto teoretických, ako aj praktických problémov, čo súvisí so stále pribúdajúcimi novými technickými možnosťami. V technologickej dobe, ktorej sme súčasťou by sme mali

využiť jej možnosti a zohľadniť všetky dostupné prostriedky na kvalitné zanalyzovanie a spracovanie údajov v každom trestnom konaní.

Boj s kriminalitou sa stáva čím ďalej tým viac nebezpečnejším a dokonca sa stáva každodennou súčasťou života, čo má dopad na všetky činnosti, ktoré vykonávame. Pomoc automatizácie získavania podkladov a informácií pre rýchle riešenie závažných trestných činov je urgentnou otázkou, ktorá naberá na dôležitosti viac, ako kedykoľvek v minulosti.

Dúfam, že mojim výstupom na celoštátnej konferencii s medzinárodnou účasťou som dostatočne poukázala a preukázala, že využívanie informačno-technických prostriedkov v trestnom konaní na účely dokazovania je okrem samotného rozhodovania dôležitým úkonom v trestnom konaní.

Ak je konštruktívna kritika argumentačne zdôvodnená, akceptujem ju s vedeckou pokorou.

Literatúra

ČENTÉŠ, J.; LAZAREVA, N.: Legalita, legitimita a proporcionalita odpočúvania a zaznamenávania telekomunikačnej prevádzky, In Zborník príspevkov z celoštátnej konferencie s medzinárodnou účasťou na tému *Aktuálne otázky trestného zákonodarstva*. Bratislava: FP PEVŠ 2012.

Dohovor o ochrane ľudských práv a základných slobôd

IVOR, J.: Obrazovo-zvukový záznam ako dôkazný prostriedok v trestnom konaní, In Zborník príspevkov z celoštátnej konferencie s medzinárodnou účasťou na tému *Teoretické a praktické problémy dokazovania*. Bratislava: FP PEVŠ 2008.

IVOR, J. a kol.: Trestné právo procesné. Druhé, doplnené a prepracované vydanie. Bratislava.: Iura Edition, 2010.

IVOR, J. a kol.: Optimalizácia prípravného konania trestného. Prvé vydanie. Praha: Leges, 2017.

IVOR, J.; ZÁHORA, J.: Repetitórium trestného práva. Tretie vydanie. Bratislava.: Wolters Kluwer, 2018.

PERHÁCS, Z.; PERHÁCSOVÁ, A.: Právna úprava používania informačno-technických prostriedkov (2. časť). Justičná revue č. 5/2013. Bratislava: Ministerstvo spravodlivosti SR

POLÁK, P.; TALAPKA, M.: Prípustnosť využitia dôkazov získaných použitím informačno-technických prostriedkov pre účely trestného konania, In Zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou na tému *Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní*. Bratislava: FP PEVŠ 2017.

Rozhodnutie Najvyššieho súdu Slovenskej republiky zo dňa 7. 2. 2012, pod sp. zn. 2 To 5/2011

SVÁK, J.: Ústavné hranice využívania informačno-technických prostriedkov v trestnom konaní, In Zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou na tému *Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní*. Bratislava: FP PEVŠ 2017.

Ústavný zákon č. 23/1991 Zb. Ústavný zákon, ktorým sa uvádza Listina základných práv a slobôd ako ústavný zákon Federálneho zhromaždenia Českej a Slovenskej Federatívnej Republiky

ZÁHORA, J.: Neprípustnosť dôkazu získaného donútením, In Zborník príspevkov z celoštátnej konferencie s medzinárodnou účasťou na tému *Teoretické a praktické problémy dokazovania*. Bratislava: FP PEVŠ 2008.

Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Zákon č. 1/2014 Z. z. o organizovaní verejných športových podujatí a o zmene a doplnení niektorých zákonov

Zákon č. 301/2005 Z. z. Trestný poriadok

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)

Zákon č. 171/1993 Z. z. Zákon Národnej rady Slovenskej republiky o Policajnom zbore

Zákon č. 460/1992 Zb. Ústava Slovenskej republiky

Operatívno-pátracia činnosť *de lege lata*[1]

Operative-search Activity de lege lata

Jakub Jagnešák[2]

Abstrakt: *Používanie informačno-technických prostriedkov a prostriedkov operatívno-pátracej činnosti mimo trestného konanie prebieha v rámci operatívno-pátracej činnosti. Autor príspevku analyzuje súčasnú definíciu operatívno-pátracej činnosti a ponúka návrhy de lege lata.*

Abstract: *Using of the intelligence-technical tools and the operative criminal tools out of the criminal process is called operative-search activity. Author of the paper analyses the current definition of the operative-search activity and offers suggestions de lege lata.*

Kľúčové slová: *operatívno-pátracia činnosť, prostriedky operatívno-pátracej činnosti, informačno-technické prostriedky.*

Keywords: *operative-search activity, operative criminal tools, intelligence-technical tools.*

Úvod

Informačno-technické prostriedky a prostriedky operatívno-pátracej činnosti tvoria významný element, ktorý Policajný zbor, Zbor väzenskej a justičnej správy a Finančná správa[3] využívajú pri odhaľovaní, objasňovaní a dokumentovaní trestných činov. Činnosť, v rámci ktorej vymenované štátne orgány aplikujú informačno-technické prostriedky a prostriedky operatívno-pátracej činnosti môže prebiehať dvoch variantoch. Prvý z nich predstavuje **operatívno-pátracia činnosť**, ktorá je vykonávaná v mimo trestno-procesnej rovine. V tomto prípade sa postupuje v intenciách zákona č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov (ďalej aj „ZoPZ"), zákona č. 652/2004 Z. z. o orgánoch štátnej správy v colníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej aj „ZoC"), zákona č. 4/2001 Z. z. o Zbore väzenskej a justičnej stáže v znení neskorších predpisov (ďalej aj „ZoZVJS") alebo zákona č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Druhý variant používania informačno-technických prostriedkov a prostriedkov operatívno-pátracej činnosti spočíva v postupe príslušníkov Policajného zboru, ZVJS alebo Finančnej správy, ktorý je uskutočňovaný v zmysle ustanovení zákona č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov (ďalej aj „TP"), t. j. aplikácia informačno-technických prostriedkov a prostriedkov operatívno-pátracej činnosti prebieha v trestno-procesnej rovine. Tento právny stav vyvoláva polemiku, či oba varianty predstavujú operatívno-pátraciu činnosť, resp. druhý variant je

---

[1] Príspevok vychádza účinného právneho stavu k 4. aprílu 2019 v Slovenskej republike. Od 1. júna 2019 nadobudne plnú platnosť a účinnosť zákon č. 35/2019 Z. z. o finančnej správe a o zmene a doplnení niektorých zákonov, ktorý nahrádza zákon č. 652/2004 Z. z. o orgánoch štátnej správy v colníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a zákon č. 200/1998 Z. z. o štátnej službe colníkov a o zmene a doplnení niektorých ďalších zákonov v znení neskorších predpisov.

[2] Mgr. et Bc. Jakub Jagnešák, Katedra kriminálnej polície, Akadémia Policajného zboru v Bratislave, e-mail: Jakub.Jagnesak@minv.sk.

[3] Ustanovenie § 2 ods. 2 zákona č. 652/2004 Z. z. o orgánoch štátnej správy v colníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov: „Finančné riaditeľstvo, colné úrady a Kriminálny úrad finančnej správy sú súčasťou finančnej správy."

potrebné zahrnúť pod inštitút vyšetrovania. Autor príspevku zastáva názor, že používanie informačno-technických prostriedkov a prostriedkov operatívno-pátracej činnosti podľa Trestného poriadku je potrebné subsumovať pod pojem **vyšetrovanie**.[4] Tento príspevok je venovaný pojmu operatívno-pátracia činnosť.

Problematika operatívno-pátracej činnosti v neprocesnej rovine je v súčasnosti parciálne riešená vo viacerých normatívnych právnych aktoch (všeobecne záväzných právnych predpisoch a interných právnych predpisoch).

Cieľom autora je poukázanie na nekonzistentnú právnu úpravu a zdôvodnenie potreby uskutočniť legislatívne zmeny tak, aby sa aj laik aspoň čiastočne vedel zorientovať v predmetnej tematike a aj týmto spôsobom preventívne pôsobiť na osoby, ktoré rozmýšľajú o začatí kriminálnej kariéry. V tejto súvislosti je potrebné poznamenať, že vykonávanie operatívno-pátracej činnosti zväčša súvisí s ingerenciou do základných práv a slobôd osôb (napr. čl. 19 ods. 2,[5] 3,[6] čl. 22 ods. 1[7] Ústavy SR) a preto je dôležité, aby táto činnosť bola uskutočňovaná v medziach zákona. Autor zastáva názor, že vhodnou unifikáciou právnej úpravy v rámci jedného zákona by sa mala legálne jednotne definovať operatívno-pátracia činnosť, resp. zmeniť jej názov napr. na operatívno-poznávacia činnosť, takýto zákon by ďalej určoval účel operatívno-pátracej činnosti, taxatívne vymenovával a vymedzoval jednotlivé prostriedky operatívno-pátracej činnosti, stanovoval by podmienky na ich aplikáciu, a zároveň by aj určoval kompetentný subjekt, ktorý by používanie toho-ktorého prostriedku operatívno-pátracej činnosti schvaľoval a túto aplikáciu predmetných prostriedkov aj kontroloval. Takto precíznou úpravou by podstatne došlo k sprehľadneniu zákonnej úpravy operatívno-pátracej činnosti.

1 Operatívno-pátracia činnosť *de lege lata*

Legálna definícia operatívno-pátracej činnosť je momentálne uvedená v zákone o Policajnom zbore a v zákone o orgánoch štátnej správy v colníctve. V zmysle ZoPZ sa predmetnou činnosťou sa rozumie: *„systém spravidla utajených, spravodajských opatrení vykonávaných Policajným zborom na účely:*

a) predchádzania, zamedzovania, odhaľovania a dokumentovania trestnej činnosti a zisťovania jej páchateľov,

b) zabezpečovania ochrany určených osôb a strážených objektov, technicky chránených objektov,

c) zabezpečovania a poskytovania ochrany a pomoci ohrozenému svedkovi a chránenému svedkovi,

[4] Zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov neobsahuje definíciu pojmu vyšetrovanie, preto autor využil českú právnu úpravu, in concreto ustanovenie § 161 ods. 1 zákona č. 141/1961 Sb. Trestní řád v znení neskorších predpisov: „Vyšetrovaním sa označuje úsek trestného stíhania pred podaním obžaloby, návrhu na schválenie dohody o vine a treste, postúpením veci inému orgánu alebo zastavením trestného stíhania, vrátane schválenia zmieru a podmienečného zastavenia trestného stíhania pred podaním obžaloby, návrhu na schválenie dohody o vine a treste."

[5] Čl. 19 ods. 2 zákona č. 460/1992 Zb. Ústava Slovenskej republiky v znení neskorších predpisov: „Každý má právo na ochranu pred neoprávneným zasahovaním do súkromného a rodinného života."

[6] Čl. 19 ods. 3 zákona č. 460/1992 Zb. Ústava Slovenskej republiky v znení neskorších predpisov: „Každý má právo na ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe."

[7] Čl. 22 ods. 3 zákona č. 460/1992 Zb. Ústava Slovenskej republiky v znení neskorších predpisov: „Listové tajomstvo, tajomstvo dopravovaných správ a iných písomností a ochrana osobných údajov sa zaručujú."

d) ochrany štátnej hranice a
e) vypátrania osôb a vecí."[8]

Obdobne, i keď s menšími odchýlkami je definovaná operatívno-pátracia činnosť v ZoC, podľa ktorého je to *„systém spravidla utajených spravodajských opatrení vykonávaných finančnou správou na účely:*

a) predchádzania, zamedzovania, odhaľovania a dokumentovania trestnej činnosti a zisťovania jej páchateľov,
b) zabezpečovania ochrany určených osôb, zabezpečovania ochrany strážených objektov, technicky chránených objektov a
c) vypátrania osôb a vecí."[9]

Z vyššie uvedených ustanovení zákonov môžeme v najvšeobecnejšej rovine konštatovať, že **operatívno-pátracia činnosť je systém spravidla utajených spravodajských opatrení vykonávaných kompetentným štátnym orgánom na zákonom určené účely za súčasného dodržiavania zákona.**

2 Explanácia definície operatívno-pátracia činnosť

1. **Systém –** (*gr. sýstéma = „členitý celok zložený z viacerých častí*").[10] Komplex entít, ktoré vytvárajú operatívno-pátraciu činnosť je tvorený z:[11]
   a. Metód operatívno-pátracej činnosti,
   b. Prostriedkov operatívno-pátracej činnosti,
   c. Foriem operatívno-pátracej činnosti a
   d. Síl operatívno-pátracej činnosti.

   Ad a. Metóda = *„premyslený postup (práce) na dosiahnutie cieľa.*"[12] Vhodnými metódami operatívno-pátracej činnosti sa kompetentný štátny orgán (Policajný zbor, Zbor väzenskej a justičnej stráže, Finančná správa, príp. veliteľ námornej lode – pozri Ad d.) snaží spravidla utajene a čo najefektívnejšie využiť prostriedky, sily a formy operatívno-pátracej činnosti. Pre potreby Policajného zboru metódy operatívno-pátracej činnosti sa rozdeľujú na základné a špecifické a sú podrobnejšie upravené v nariadení Ministerstva vnútra SR č. 92/2016 o operatívno-pátracej činnosti v znení neskorších predpisov.[13]

   Ad b. Prostriedok = *„vec, pomôcka, nástroj, opatrenie a pod. na uskutočnenie niečoho.*"[14] Prostriedky operatívno-pátracej činnosti preto môžeme definovať ako súhrn nástrojov uvedených v zákone, resp. inom normatívnom právnom akte, ktoré je oprávnený kompe-

[8] Ustanovenie § 38a ods. 1 zákona č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov.
[9] Ustanovenie § 30 ods. 1 zákona č. 652/2004 Z. z. o orgánoch štátnej správy v colníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
[10] https://sk.wikipedia.org/wiki/Syst%C3%A9m [dostupné online 27. 9. 2018].
[11] STIERANKA, J. a kol. Spravodajská činnosť. Bratislava: Akadémia PZ v Bratislave, 2013, s. 33. Pozri aj: METEŇKO, J. Systémový prístup a teória operatívnych a spravodajských činností. s. 312. In: PORADA,V. Teoretická reflexe a identifikace spoločenských potřeb ve vazbě na aktuálni problémy policejní praxe. Zborník z medzinárodní konference konané na Policejní akademii České republiky v Praze ve dnech 29.–30. září 2003.
[12] http://slovniky.juls.savba.sk/?w=met%C3%B3da&s=exact&c=Bd39&d=kssj4&d=psp&d=sssj&d=scs&d=sss&d=peciar&d=ma&d=hssjV&d=bernolak&d=obce&d=priezviska&d=un&d=locutio&d=pskcs&d=psken&d=noundb&ie=utf-8&oe=utf-8# dostupné online [27. 9. 2018].
[13] STIERANKA, J. a kol. Spravodajská činnosť. Bratislava: Akadémia PZ v Bratislave, 2013, s. 32–35.
[14] http://slovniky.juls.savba.sk/?w=prostriedok&s=exact&c=O851&d=kssj4&d=psp&d=sssj&d=scs&d=sss&d=peciar&d=ma&d=hssjV&d=bernolak&d=obce&d=priezviska&d=un&d=locutio&d=pskcs&d=psken&d=noundb&ie=utf-8&oe=utf-8# dostupné online [27. 9. 2018].

tentný subjekt, v medziach zákona pri plnení zákonom určených úloh, aplikovať.[15] Aj napriek tomu, že pojem operatívno-pátracia činnosť je definovaný len v ZoPZ a ZoC, prostriedky operatívno-pátracej činnosti enumerujú okrem už skôr spomenutých zákonov aj zákon o ZVJS a Trestný poriadok. V zmysle Trestného poriadku sa prostriedkami operatívno-pátracej činnosti rozumejú *„kontrolovaná dodávka, zámena obsahu zásielok, agent, predstieraný prevod, sledovanie osôb a vecí.“*[16] Tie sú bližšie špecifikované vo všeobecnej časti, štvrtej hlavy Trestného poriadku – Zaistenie osôb a vecí a v piatej hlave Trestného poriadku – Zabezpečovanie informácií. Prostriedky operatívno-pátracej činnosti podľa zákona o Policajnom zbore sú: *„sledovanie osôb a vecí, monitorovanie osôb a dopravných prostriedkov, kontrolovaná dodávka, kriminálne spravodajstvo, používanie krycích dokladov, nástrahová a zabezpečovacia technika a využívanie osôb konajúcich v prospech Policajného zboru, objekty a miesta používané pod legendou a predstieraný prevod veci.“*[17] Zároveň je dôležité upozorniť, že Policajný zbor je oprávnený predmetné prostriedky operatívno-pátracej činnosti použiť len pri odhaľovaní úmyselných trestných činov a pri zisťovaní ich páchateľov, pri zabezpečovaní ochrany určených osôb, ochrany strážených objektov, ochrany štátnej hranice, pri plnení úloh vyplývajúcich z Dohovoru, ktorým sa vykonáva Schengenská dohoda zo dňa 14. júna 1985, v prípadoch podľa § 36 ZoPZ[18] a v súvislosti s činnosťou kriminálneho spravodajstva ak vykonáva bezpečnostnú previerku podľa zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov.[19] Zákon o colníctve ustanovuje nasledovné prostriedky operatívno-pátracej činnosti: *„sledovanie osôb a vecí, cezhraničné sledovanie osôb podľa medzinárodnej zmluvy, kontrolovaná dodávka, krycie doklady, nástrahová a zabezpečovacia technika a využívanie osôb konajúcich v prospech finančnej správy.“*[20] Formálny predpoklad na to, aby Finančná správa mohla v rámci operatívno-pátracej činnosti použiť prostriedky operatívno-pátracej činnosti je, že musí ísť o odhaľovanie úmyselnej trestnej činnosti, čo zahŕňa aj úmyselnú trestnú činnosť páchanú pracovníkmi finančnej správy pri výkone štátnej služby alebo práce vo verejnom záujme.[21] Posledným právnym predpisom, ktorý menuje prostriedky operatívno-pátracej činnosti je ZoZVJS, podľa ktorého sú nimi: *„sledovanie osôb a vecí, nástrahová a zabezpečovacia technika a využívanie osôb konajúcich v prospech zboru.“*[22] ZVJS je oprávnený používať prostriedky operatívno-pátracej činnosti pri plnení

[15] Pozri aj RŮŽIČKA, M. In: HUNDÁK, Š. Použití operativně pátracích prostředků k získaní důkazů pro trestní řízení. Praha: Vydavatelství PA ČR, 2004, s. 10.

[16] Ustanovenie § 10 ods. 22 zákona č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov.

[17] Ustanovenie § 39 ods. 1 zákona č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov.

[18] „Pri plnení úloh v boji proti terorizmu, v boji proti legalizácii príjmov z trestnej činnosti a financovaniu terorizmu[1)] pri odhaľovaní trestnej činnosti a financovaniu terorizmu organizovanej v spojení s cudzinou a organizovanej trestnej činnosti a financovaniu terorizmu súvisiacej s nedovolenou výrobou, držaním a rozširovaním omamných a psychotropných látok, jedov, prekurzorov a jadrových materiálov, s falšovaním a pozmeňovaním peňazí, známok a cenných papierov, pri odhaľovaní iných zločinov[18)] pri poskytovaní ochrany a pomoci ohrozenému svedkovi a chránenému svedkovi podľa osobitného predpisu,[2a)] pri operatívnej ochrane legalizanta a agenta pri odhaľovaní daňových únikov a nezákonných finančných operácií, pri odhaľovaní úmyselných trestných činov podľa druhého a tretieho dielu ôsmej hlavy druhej časti Trestného zákona, za ktoré možno uložiť trest odňatia slobody s hornou hranicou najmenej dva roky, alebo iných úmyselných trestných činov, ktorých stíhanie upravuje medzinárodná zmluva, ktorou je Slovenská republika viazaná, a pri zisťovaní ich páchateľov a pátraní po nich je.“

[19] Ustanovenie § 39 ods. 2 zákona č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov.

[20] Ustanovenie § 31 ods. 1 zákona č. 652/2004 Z. z. o orgánoch štátnej správy v colníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

[21] Ustanovenie § 31 ods. 2 zákona č. 652/2004 Z. z. o orgánoch štátnej správy v colníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

[22] Ustanovenie § 26 ods. 1 zákona č. 4/2001 Z. z. o Zbore väzenskej a justičnej stáže v znení neskorších predpisov.

úloh v boji proti terorizmu a organizovanému zločinu, pri predchádzaní a odhaľovaní pripravovanej trestnej činnosti alebo spáchanej trestnej činnosti obvinených vo výkone väzby, odsúdených vo výkone trestu odňatia slobody, príslušníkov alebo zamestnancov ZVJS a pri zabezpečovaní ochrany chránených objektov.[23] Pre jednoduchšie zorientovanie jednotlivé právne úpravy demonštrujeme v nasledovnej tabuľke:

Prostriedky operatívno-pátracej činnosti v zmysle jednotlivých zákonov.

§ 39 ods. 1 ZoPZ	§ 31 ods. 1 ZoC	§ 26 ods. 1 ZoZVJS	§ 10 ods. 22 TP
Sledovanie osôb a vecí	Sledovanie osôb a vecí	Sledovanie osôb a vecí	Sledovanie osôb a vecí
Predstieraný prevod veci			Predstieraný prevod veci
Kontrolovaná dodávka	Kontrolovaná dodávka		Kontrolovaná dodávka
Používanie krycích dokladov	Krycie doklady		
Nástrahová a zabezpečovacia technika	Nástrahová a zabezpečovacia technika	Nástrahová a zabezpečovacia technika	
Využívanie osôb konajúcich v prospech Policajného zboru	Využívanie osôb konajúcich v prospech finančnej správy	Využívanie osôb konajúcich v prospech zboru	
Kriminálne spravodajstvo			
Objekty a miesta používané pod legendou			
Monitorovanie osôb a dopravných prostriedkov			
	Cezhraničné sledovanie osôb podľa medzinárodnej zmluvy		
			Zámena obsahu zásielok
			Agent

[23] Ustanovenie § 26 ods. 3 zákona č. 4/2001 Z. z. o Zbore väzenskej a justičnej stáže v znení neskorších predpisov.

Možnosti použitia prostriedkov operatívno-pátracej činnosti v zmysle jednotlivých zákonov.

§ 39 ods. 2 ZoPZ	§ 31 ods. 2 ZoC	§ 26 ods. 3 ZoZVJS
odhaľovanie úmyselných trestných činov a zisťovanie ich páchateľov	odhaľovanie úmyselnej trestnej činnosti (vrátane úmyselnej trestnej činnosti páchanej pracovníkmi finančnej správy pri výkone štátnej služby alebo práce vo verejnom záujme)	predchádzanie a odhaľovanie pripravovanej alebo spáchanej trestnej činnosti v priestoroch ZVJS osobami vo výkone väzby, výkone trestu odňatia slobody, a príslušníkmi alebo zamestnancami ZVJS
ochrana určených osôb		
ochrana strážených objektov		ochrana chránených objektov
ochrana štátnej hranice		boj proti terorizmu a organizovanému zločinu
plnenie úloh vyplývajúcich Dohody, ktorou sa vykonáva Schengenská dohoda		
s činnosťou kriminálneho spravodajstva pri vykonávaní bezpečnostnej previerky podľa zákona č. 215/2004 Z. z.		

Ad c. Forma = *„spôsob spracovania."*[24] Vzájomné vzťahy medzi jednotlivými zložkami operatívno-pátracej činnosti predstavujú formy operatívno-pátracej činnosti, ktoré sú prejavom jednotlivých metód, síl a prostriedkov operatívno-pátracej činnosti. Pre potreby Policajného zboru sú bližšie špecifikované v nariadení ministerstva vnútra č. 92/2016 o operatívno-pátracej činnosti v znení neskorších predpisov.[25]

Ad d. Sily operatívno-pátracej činnosti možno vymedziť v širšom a užšom zmysle. Z extenzívneho hľadiska sú to štátne orgány, ktorým zákon umožňuje realizovanie operatív-

[24] http://slovniky.juls.savba.sk/?w=forma&s=exact&c=Q111&d=kssj4&d=psp&d=sssj&d=scs&d=sss&d=peciar&d=ma&d=hssjV&d=bernolak&d=obce&d=priezviska&d=un&d=locutio&d=pskcs&d=psken&d=noundb&ie=utf-8&oe=utf-8# dostupné online [1. 10. 2018].

[25] STIERANKA, J. a kol. Spravodajská činnosť. Bratislava: Akadémia PZ v Bratislave, 2013, s. 32–35. Bližšie pozri aj LISOŇ, M. Operatívno-pátracia činnosť (všeobecná časť). Bratislava: Akadémia PZ v Bratislave, 2012, s. 150 a nasl.

no-pátracej činnosti. *In concreto* je to Policajný zbor,[26] Finančná správa[27] a ZVJS.[28] Reštriktívny pohľad na sily operatívno-pátracej činnosti ich vymedzuje ako exekutívny orgán tvorený personálnym substrátom, ktorý predmetnú činnosť vykonáva. Pre potreby zákona o Policajnom zbore sú ním určené služby Policajného zboru, konkrétne je to služba kriminálnej polície, služba finančnej polície, služba ochrany objektov, služba hraničnej polície, služba ochrany určených osôb a inšpekčná služba. Tieto služby môžu využívať okrem metód, prostriedkov a foriem operatívno-pátracej činnosti aj dostupné evidencie, spolupracovať s ostatnými útvarmi Policajného zboru, so zahraničnými políciami, využívať osobitné finančné prostriedky a pod.[29] Pre účely trestného konania, na základe schválenia toho-ktorého prostriedku kompetentným orgánom, vykonáva aplikáciu prostriedku operatívno-pátracej činnosti alebo informačno-technického prostriedku, resp. paralelného použitia viacerých prostriedkov, príslušný subjekt, ide najmä o útvary Prezídia Policajného zboru – napr. Úrad zvláštnych policajných činností (vykonáva sledovanie osôb a vecí) a eventuálne prichádza do úvahy aj činnosť veliteľa námornej lode, ktorý pri zabezpečovaní potrebných dôkazov pri spáchaní skutku vykazujúceho znaky trestného činu, má postupovať v zmysle Trestného poriadku.[30, 31]

2. Systém **spravidla utajených spravodajských opatrení –** (opatrenie = *„zákrok na dosiahnutie istého cieľa;*[32] spravodajský – syn. informačný = *„ktorý informuje, prináša informácie*"[33]). Pre úplnosť je dôležité definovať pojem spravodajská činnosť, ktorou sa rozumie *„cieľavedomá, systematická poznávacia činnosť, ktorou kompetentné štátne orgány využívaním špecifických metód, prostriedkov (techník) a foriem utajene, plánovito získavajú (zhromažďujú), triedia, analyzujú, uchovávajú a distribuujú (poskytujú) informácie pre konkrétnych používateľov (adresátov) s cieľom zvýšiť úroveň ich poznania, ktoré je potrebné na výkon ich činností.*"[34] V tomto kontexte možno konštatovať, že pojem operatívno-pátracia činnosť a spravodajská činnosť majú určitú podobu, o. i. tým, že kooperujú s termínom spravodaj-

[26] Ustanovenie § 1 ods. 1 zákona č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov: „Policajný zbor je ozbrojený bezpečnostný zbor, ktorý plní úlohy vo veciach vnútorného poriadku, bezpečnosti, boja proti zločinnosti vrátane jej organizovaných foriem a medzinárodných foriem a úlohy, ktoré pre Policajný zbor vyplývajú z medzinárodných záväzkov Slovenskej republiky." Ustanovenie § 38a ods. 2 zákona č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov: „Operatívno-pátraciu činnosť vykonávajú na to určené služby Policajného zboru."

[27] Ustanovenie § 2 ods. 2 zákona č. 652/2004 Z. z. o orgánoch štátnej správy v colníctve a o zmene a doplnení niektorých zákonov: „Operatívno-pátraciu činnosť vykonávajú určení colníci finančného riaditeľstva a určení colníci Kriminálneho úradu finančnej správy, ktorí sú na tento účel oprávnení využiť aj služobného psa na pachové práce."

[28] Ustanovenie § 26 ods. 3 zákona č. 4/2001 Z. z. o Zbore väzenskej a justičnej stáže v znení neskorších predpisov: „Zbor je oprávnený používať prostriedky operatívno-pátracej činnosti pri plnení úloh na úseku boja proti terorizmu a organizovanému zločinu, pri odhaľovaní trestnej činnosti podľa § 23 a pri zabezpečovaní ochrany chránených objektov."

[29] STIERANKA, J. a kol. Spravodajská činnosť. Bratislava: Akadémia PZ v Bratislave, 2013, s. 32 – 35.

[30] Ustanovenie § 30 ods. 3 zákona č. 435/2000 Z. z. o námornej plavbe v znení neskorších predpisov.

[31] Veliteľ námornej lode nie je štátnym orgánom, ale v zmysle ustanovenia § 8 písm. g) zákona č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov je policajtov na účely predmetného zákona.

[32] http://slovniky.juls.savba.sk/?w=opatrenie&s=exact&c=Pf8c&d=kssj4&d=psp&d=sssj&d=scs&d=sss&d=peciar&d=ma&d=hssjV&d=bernolak&d=obce&d=priezviska&d=un&d=locutio&d=pskcs&d=psken&d=noundb&ie=utf-8&oe=utf-8# dostupné online [2. 10. 2018].

[33] http://slovniky.juls.savba.sk/?w=spravodajsk%C3%BD&s=exact&c=o1dd&d=kssj4&d=psp&d=sssj&d=scs&d=sss&d=peciar&d=ma&d=hssjV&d=bernolak&d=obce&d=priezviska&d=un&d=locutio&d=pskcs&d=psken&d=noundb&ie=utf-8&oe=utf-8# dostupné online [2. 10. 2018].

[34] STIERANKA, J. a kol. Spravodajská činnosť. Bratislava: Akadémia PZ v Bratislave, 2013, s. 38. Pozri aj LISOŇ, M. Spravodajská činnosť Policajného zboru (úvod do štúdia). Bratislava: Akadémia PZ v Bratislave, 2002, s. 16.

ské opatrenie. Spravodajské opatrenie gramatickým výkladom možno stanoviť ako cieľavedomú činnosť na dosiahnutie určitého, žiadaného stupňa poznania, ktoré sa ďalej distribuuje. Spravodajské opatrenia ovplyvňujú ciele, resp. úlohy, ktoré má ten-ktorý kompetentný subjekt v rámci operatívno-pátracej činnosti definované v zákone. Avšak generálne možno ustáliť, že úlohou operatívno-pátracej činnosti je najmä predchádzanie trestnej činnosti, jej odhaľovanie a tým vytváranie vhodných podmienok na začatie trestného stíhania. Zároveň je potrebné upozorniť na to, že cieľom operatívno-pátracej činnosti môže byť napr. aj zmapovanie kriminálnych skupín pôsobiacich na území Slovenskej republiky (väzby, členovia, legálne/nelegálne podnikateľské aktivity a pod.).[35] K pojmu **spravidla utajených** – subjekty realizujúce operatívno-pátraciu činnosť zväčša majú záujem na tom, aby neboli videní pri vykonávaní spravodajských opatrení, pretože v dôsledku ich odhalenia by s najväčšou pravdepodobnosťou podozrivá osoba ešte intenzívnejšie pracovala na zničení existujúcich stôp, ktoré sa kompetentné orgány snažia zhromaždiť a vytvoriť tak podmienky na začatie trestného stíhania voči konkrétnemu páchateľovi ilegálnej činnosti. Výnimku zo stany Policajného zboru kedy je pozitívne vnímané to, že osoba podozrivá zo spáchania trestného činu vie, že sa o ňu zaujíma služba kriminálnej polície je v prípade menej sofistikovaných trestných činov ekonomického charakteru (napr. § 277 TZ – Neodvedenie dane a poistného, § 278 – Nezaplatenie dane a poistného apod.), kedy si podozrivá osoba uvedomí, že jej protiprávne konanie bolo odhalené a svoju zákonnú povinnosť si dodatočne splní.[36]

3. Systém spravidla utajených spravodajských opatrení **vykonávaných kompetentným štátnym orgánom** – (kompetentný – syn. oprávnený = *„ktorý má oprávnenie;“*[37] kompetencia – stanovená aktivita pre štátny orgán v rámci jemu vymedzenom okruhu štátnych vecí, v ktorých má byť činný,[38] syn. hmotnoprávneho pojmu pôsobnosť a procesnoprávneho pojmu príslušnosť[39]). Jednotlivé oprávnené subjekty na vykonávanie operatívno-pátracej činnosti (Policajný zbor, Finančná správa a Zbor väzenskej a justičnej stáže) predstavujú štátne orgány, ktoré uskutočňujú funkcie štátu a konajú v jeho mene.[40] Bližšie pozri bod **1. Ad. d.**

4. Systém spravidla utajených spravodajských opatrení vykonávaných kompetentným štátnym orgánom **na zákonom určené účely –** (účel – syn. *„zámer, zmysel, ku ktorému smeruje istá činnosť“*).[41] Pri vymedzení účelu na ktorý môže Policajný zbor a Finančná správa uskutočňovať operatívno-pátraciu činnosť je potrebné vychádzať zo zákonných noriem, ktoré *expressis verbis* stanovujú legálne účely. V zmysle ZoPZ účelom operatívno-pátracej činnosti je predchádzanie, zamedzovanie, odhaľovanie a dokumentovanie trestnej činnosti, vrátane jej páchateľov, zabezpečovanie ochrany určených osôb a strážených objektov, technicky chránených objektov, zabezpečovanie a poskytovanie ochrany a pomoci ohrozenému svedkovi a chránenému svedkovi, ochrany štátnej hranice a vypátranie osôb a ve-

[35] STIERANKA, J. a kol. Spravodajská činnosť. Bratislava: Akadémia PZ v Bratislave, 2013, s. 32–35.

[36] Autor sa nezameriava v tomto článku na aplikáciu inštitútu – Účinná ľútosť v zmysle ustanovenia § 85 a nasl. zákona č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov.

[37] http://slovniky.juls.savba.sk/?w=kompetentn%C3%BD&s=exact&c=Ma22&d=kssj4&d=psp&d=sssj&d=scs&d=sss&d=peciar&d=ma&d=hssjV&d=bernolak&d=obce&d=priezviska&d=un&d=locutio&d=pskcs&d=psken&d=noundb&ie=utf-8&oe=utf-8# dostupné online [2. 10. 2018].

[38] MACHAJOVÁ, J. a kol. Všeobecné správne právo. Žilina: Eurokódex, 2009, s. 86.

[39] VRABKO, M. a kol. Správne právo hmotné. Všeobecná časť. Bratislava: C. H. Beck, 2012, s. 117.

[40] VRABKO, M. a kol. Správne právo hmotné. Všeobecná časť. Bratislava: C. H. Beck, 2012, s. 4.

[41] http://slovniky.juls.savba.sk/?w=%C3%BA%C4%8Del&s=exact&c=k045&d=kssj4&d=psp&d=sssj&d=scs&d=sss&d=peciar&d=ma&d=hssjV&d=bernolak&d=obce&d=priezviska&d=un&d=locutio&d=pskcs&d=psken&d=noundb&ie=utf-8&oe=utf-8# dostupné online [2. 10. 2018].

cí.[42] Reštriktívnejšie je definovaný účel operatívno-pátracej činnosti v ZoC, kde je vynechaný účel ochrana štátnej hranice a zabezpečovanie a poskytovanie ochrany a pomoci ohrozenému svedkovi a chránenému svedkovi.[43] ZoZVJS na rozdiel od vyššie uvedených zákonov exaktne neobsahuje uvedenie účelu, pre ktorý je možné vykonávať operatívno-pátraciu činnosť. Ten môžeme len dedukovať a je ním predchádzanie, zamedzovanie, odhaľovanie a dokumentovanie trestnej činnosti osôb, ktoré sú vo výkone väzby, vo výkone trestu odňatia slobody alebo sú v služobnom pomere, resp. štátnozamestnaneckom pomere k ZVJS a zabezpečovanie ochrany chránených objektov. Pre väčší prehľad, zákonom určené účely demonštrujeme v nasledujúcej tabuľke.

Zákonné účely, pre ktoré možno vykonávať operatívno-pátracia činnosť.

§ 38a ods. 1 ZoPZ	§ 30 ods. 1 ZoC	ZoZVJS
Predchádzanie, zamedzovanie, odhaľovanie a dokumentovanie trestnej činnosti a zisťovanie jej páchateľov	Predchádzanie, zamedzovanie, odhaľovanie a dokumentovanie trestnej činnosti zisťovanie jej páchateľov	Predchádzanie, zamedzovanie, odhaľovania a dokumentovanie trestnej činnosti a zisťovanie jej páchateľov
Zabezpečovanie ochrany určených osôb, strážených objektov a technicky chránených objektov	Zabezpečovanie ochrany určených osôb, strážených objektov, technicky chránených objektov	Zabezpečovanie ochrany chránených objektov
Zabezpečovanie a poskytovanie ochrany a pomoci ohrozenému svedkovi a chránenému svedkovi		
Ochrana štátnej hranice		
Vypátranie osôb a vecí	Vypátranie osôb a vecí	

5. Operatívno-pátracia činnosť je systém spravidla utajených spravodajských opatrení vykonávaných kompetentným štátnym orgánom na zákonom určené účely **za súčasného dodržiavania zákona**. V zmysle základného zákona Slovenskej republiky, ktorým je Ústava Slovenskej republiky, sú štátne orgány oprávnene konať iba na základe ústavy, v jej medziach a v rozsahu a spôsobom, ktorý ustanoví zákon.[44] Na základe uvedeného, každá činnosť štátneho orgánu, v našom prípade, toho ktorý uskutočňuje operatívno-pátraciu činnosť musí byť vykonávaná v intenciách zákona. Zároveň predmetná činnosť aj musí byť v takej kvalite, aby v prípade podania sťažnosti dotknutej osoby pre porušenie základných práv a slobôd na Ústavný súd Slovenskej republiky tento zásah prešiel testom proporcionality.[45] Obdobne ku kvalite zákonnosti konania štátneho orgánu to platí aj pre konanie pred Európskym súdom pre ľudské práva, ktorý posudzuje či došlo k porušeniu ustanove-

[42] Ustanovenie § 38 ods. 1 zákona č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov.
[43] Ustanovenie § 30 ods. 1 zákona č. 652/2004 Z. z. o orgánoch štátnej správy v colníctve a o zmene a doplnení niektorých zákonov.
[44] Čl. 2 ods. 2 zákona č. 460/1992 Zb. Ústava Slovenskej republiky v znení neskorších predpisov.
[45] KROŠLÁK, D. a kol. Ústavné právo. Bratislava: Wolters Kluwer, 2016, s. 285 a nasl.

ní Charty základných práv Európskej únie,[46] pretože Slovenská republika uznáva a dodržiava o. i. medzinárodné zmluvy, ktorými je viazaná.[47]

Sumarizujúc vyššie uvedené poznatky autor *de lege ferenda* navrhuje všeobecnú definíciu operatívno-pátracej činnosti vymedzenú na začiatku článku modifikovať presnejšie, a to: **operatívno-pátracia činnosť je systém spravidla utajených spravodajských opatrení vykonávaných kompetentným štátnym orgánom (Policajný zbor, Finančná správa, Zbor väzenskej a justičnej stráže) na účely predchádzania, zamedzovania, odhaľovania a dokumentovanie trestnej činnosti a zisťovania jej páchateľov, zabezpečovanie ochrany určených objektov a na ďalšie zákonom určené účely za súčasného dodržiavania zákona**.

Záver

Z vyššie uvedených informácií vyplýva, že právna úprava je nekonzistentná, tak ako to autor prezentuje v úvode. V tejto súvislosti autor *de lege ferenda* navrhuje, aby bola uskutočnená legislatívna zmena v podobe unifikácie operatívno-pátracej činnosti, ktorá prebieha mimo trestného konania do jedného zákona, ktorý by obsahoval jednotnú definíciu operatívno-pátracej činnosti a účel, ktorý sa ňou sleduje, enumeráciu všetkých prostriedkov operatívno-pátracej činnosti, ich vymedzenie, definovanie podmienok pre aplikáciu toho-ktorého prostriedku pri výkone operatívno-pátracej činnosti a stanovenie kompetentného subjektu, ktorý by povoľoval použitie prostriedku operatívno-pátracej činnosti a zabezpečoval kontrolu ich používania. Týmto spôsobom by došlo k prevzatiu ustanovení, ktoré v súčasnosti upravujú predmetnú problematiku, zo zákona č. 171/1993 Z. z. o Policajnom zbore, zákona č. 652/2004 Z. z. o orgánoch štátnej správy v colníctve a o zmene a doplnení niektorých zákonov a zo zákona č. 4/2001 Z. z. o Zbore väzenskej a justičnej stáže v znení neskorších predpisov do osobitného všeobecne záväzného právneho predpisu. Touto formou by sa každý mohol oboznámiť s možnosťou zásahu do základných práv a slobôd osôb štátnym orgánom a tomu aj prispôsobiť svoje konanie a zároveň takto exaktnou právnou úpravou by bol naplnený princíp právnej istoty[48] a prezentované legislatívne riešenie by bolo aj v súlade s judikatúrou Európskeho súdu pre ľudské práva.[49] Jednotlivé formy, metódy a sily (z reštriktívneho hľadiska) majú ostať v súčasnom režime interných právnych predpisov, ktoré podliehajú utajeniu. Podľa autorovho názoru pre orgány uskutočňujúce operatívno-pát-

[46] Napr. čl. 7 Charty základných práv Európskej únie: „Každý má právo na rešpektovanie svojho súkromného a rodinného života, obydlia a komunikácie.“. Čl. 8 ods. 1, 2 Charty základných práv Európskej únie: „Každý má právo na ochranu osobných údajov, ktoré sa ho týkajú. Tieto údaje musia byť riadne spracované na určené účely na základe súhlasu dotknutej osoby alebo na inom oprávnenom základe ustanovenom zákonom...“.

[47] Čl. 1 ods. 2 zákona č. 460/1992 Zb. Ústava Slovenskej republiky v znení neskorších predpisov. Napr.: čl. 52 ods. 1 Charta základných práv Európskej únie: „Akékoľvek obmedzenie výkonu práv a slobôd uznaných v tejto charte musí byť ustanovené zákonom a rešpektovať podstatu týchto práv a slobôd. Za predpokladu dodržiavania zásady proporcionality možno tieto práva a slobody obmedziť len vtedy, ak je to nevyhnutné a skutočne to zodpovedá cieľom všeobecného záujmu, ktoré sú uznané Úniou, alebo je to potrebné na ochranu práva a slobôd iných.“

[48] Ten je implicitne uvedený v čl. 1 ods. 1 Ústavy Slovenskej republiky a predstavuje požiadavku jasnosti, zrozumiteľnosti a predvídateľnosti právnych noriem a postupu orgánov verejnej moci, ochrany práv nadobudnutých v dobrej viere a zákazu retroaktivity právnych noriem. Bližšie pozri: HOLOTA, J. Počuli ste už niekedy o doktríne legitímneho očakávania? https://www.epravo.sk/top/clanky/poculi-ste-uz-o-doktrine-legitimneho-ocakavania-3876.html dostupné online [3. 10. 2018].

[49] „Podľa ustálenej judikatúry súdu je určitá norma predvídateľná vtedy, ak je formulovaná dostatočne presne na to, aby umožnila každej osobe – v prípade potreby za pomoci znalých poradcov – prispôsobiť chovanie.“ Rozhodnutie ESĽP Malone proti Spojenému kráľovstvu, 1984. Bližšie pozri: SOKOL, T. Odposlech. In: Státní zastupitelství, 2008, roč. 6, č. 3, s. 17.

raciu činnosť nie je vhodné prezradiť najmä svoje taktické postupy, prípadne aj špeciálne útvary, ktoré určitú špecifickú činnosť zabezpečujú pre potreby Policajného zboru, ZVJS a Finančnú správu, pretože tým by sa ich efektívnosť mohla znížiť.

Zoznam bibliografických odkazov

- Zákon č. 141/1961 Sb. Trestní řád v znení neskorších predpisov.
- Zákon č. 460/1992 Zb. Ústava Slovenskej republiky v znení neskorších predpisov.
- Zákon č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov.
- Zákon č. 435/2000 Z. z. o námornej plavbe v znení neskorších predpisov.
- Zákon č. 4/2001 Z. z. o Zbore väzenskej a justičnej stráži v znení neskorších predpisov.
- Zákon č. 652/2004 Z. z. o orgánoch štátnej správy v colníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
- Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov.
- Zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov.
- Charta základných práv Európskej únie 2012/C 326/02.
- Rozhodnutie ESĽP *Malone proti Spojenému kráľovstvu, 1984.*
- HUNDÁK, Š. Použití operativně pátracích prostředků k získání důkazů pro trestní řízení. Sborník příspěvků z mezinárodního semináře uskutečněného na Policejní akademii ČR dne 2. listopadu 2004. Praha: Vydavatelství Policejní akademie ČR, 2004, 162 s. ISBN 80-7251-170-X.
- KROŠLÁK, D. a kol. *Ústavné právo.* Bratislava: Wolters Kluwer, 2016, 804 s. ISBN 978-80-8168-511-8.
- LISOŇ, M. *Operatívno-pátracia činnosť (všeobecná časť).* Bratislava: Akadémia PZ v Bratislave, 2012, 226 s. ISBN 978-80-8054-541-3.
- LISOŇ, M. – VAŠKO, A. *Teória kriminálno-policajného poznania.* Bratislava: Wolters Kluwer, 2018, 389 s. ISBN 978-80-8168-838-6.
- MACHAJOVÁ, J. a kol. *Všeobecné správne právo.* Žilina: Eurokódex, 2009, 512 s. ISBN 978-80-89447-05-3.
- METEŇKO, J. *Systémový prístup a teória operatívnych a spravodajských činností.* s. 312. In: PORADA,V. Teoretická reflexe a identifikace spoločenských potřeb ve vazbě na aktuálni problémy policejní praxe. Zborník z medzinárodní konference konané na Policejní akademii České republiky v Praze ve dnech 29.–30. září 2003.
- STIERANKA, J. a kol. *Spravodajská činnosť.* Bratislava: Akadémia PZ v Bratislave, 2013, 316 s. ISBN 978-80-8054-549-9.
- VRABKO, M. a kol. *Správne právo hmotné. Všeobecná časť.* Bratislava: C. H. Beck, 2012, 480 s. ISBN 978-80-89603-03-9.
- ZACHAR, A. Prostriedky operatívno-pátracej činnosti a možnosti ich používania na území Slovenskej republiky. In: Trestní právo, roč. 2009, č. 10, s. 35 – 40.
- https://www.epravo.sk/top/clanky/poculi-ste-uz-o-doktrine-legitimneho-ocakavania-3876.html
- https://www.wikipedia.org/
- http://slovniky.juls.savba.sk/

Vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov – úvahy *de lege ferenda*[1]

Production Video, Audio or Video-audio Records – Consideration de lege ferenda

Jozef Záhora[2]

Abstrakt: *Vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov možno považovať za dôkazný prostriedok, pomocou ktorého je možné získavať informácie dôležité pre trestné konanie. Jeho význam spočíva predovšetkým v tom, že odhaľovanie a dokazovanie tých najzávažnejších druhov trestnej činnosti prostredníctvom klasických prostriedkov je iba málo efektívne, v niektorých prípadoch dokonca nemožné. Právna úprava a viaceré aplikačné problémy predstavujú veľmi aktuálne otázky. Autor poukazuje na niektoré nedostatky právnej úpravy a predstavuje možné návrhy na riešenie.*

Abstract: *Production video, audio or video-audio records can be considered as a means of proof; which can be obtained information relevant to criminal proceedings. Its importance lies primarily in that detecting and proving the most serious types of crime through conventional means is little effective, in some cases even impossible. Legislation and multiple application problems represent a very curent question. The author points to some deficiencies in the legislation and presents possible proposals for solution.*

Kľúčové slová: *audio záznam, dôkaz, trestné konanie, video záznam, tajné sledovanie, právo na súkromie, GPS sledovanie.*

Key words: *audio record, evidence, criminal procedure, video record, secret surveillance, right to privacy, surveillance via GPS.*

Úvod

Inštitút vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov v zmysle § 114 Trestného poriadku č. 301/2005 Z. z. (ďalej len TP) patrí medzi „najmladšie" dôkazné prostriedky. Uvedený inštitút bol do právneho poriadku SR prvýkrát zavedený novelou č. 422/2002 Z. z.[3] s účinnosťou od 1. októbra 2002 do ustanovenia § 88d – štvrtej hlavy Trestného poriadku č. 141/1961 Zb. nazvanej Zaistenie osôb a vecí. Okrem iných inštitútov, bol citovanou novelou doplnený aj ďalší dôkazný prostriedok – § 88d Sledovanie osôb a vecí. Uvedená zmena bola zrejme ovplyvnená krátko pred tým prijatou obdobnou úpravou v Českej republike. Sledovanie osôb a vecí bolo do českého trestného poriadku zavedené novelou č. 265/2001 Sb.,[4] s účinnosťou od 1. januára 2002 do druhej časti Trestného poriadku č. 141/1961 Sb. do deviatej hlavy nazvanej postup pred začatím trestného stíhania. Podľa dôvodovej správy do trestného poriadku sa v modifikovanej podobe preberá úprava používania tzv. operatívne pátracích prostriedkov do-

---

[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] Prof. JUDr. Jozef Záhora, PhD., Ústav verejného práva, Fakulta práva, Paneurópska vysoká škola, e-mail: jozef.zahora@paneurouni.com.

[3] Zákon č. 422/2002 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 dopln ení niektorých zákonov.

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

posiaľ obsiahnutá v zákone č. 283/1991 Sb., o Policii České republiky. Zmyslom bolo nie len odstránenie určitej miery duplicitnej právnej úpravy ale a rozšírenie možnosti štátneho zástupcu vykonávať dozor aj v tejto oblasti ale aj zaistenia procesnej využiteľnosti výstupu z tejto činnosti pre ďalšie trestné konanie.

Slovenský zákonodarca „nad rámec" českého vzoru, okrem uvedeného sledovania osôb a veci, do právneho poriadku doplnil aj inštitút vyhotovovanie obrazových, zvukových alebo iných záznamov. Podľa dôvodovej správy bolo dôvodom na zavedenie tohto inštitútu to, že „*prax ukazuje, že vyšetrovanie niektorých trestných činov, najmä tých, pre ktoré je charakteristická vysoká organizovanosť páchateľov a používanie konšpiratívnych metód práce, je veľmi obtiažne a zdĺhavé, v niektorých prípadoch aj nemožné, bez použitia niektorých špecifických prostriedkov, akými sú aj sledovanie osôb a vecí. Vzhľadom na to, že ide prevažne o závažné zásahy do ústavných práv občanov, ktoré sú aj verejnosťou veľmi citlivo vnímané, navrhuje sa, aby jednotlivé ustanovenia veľmi podrobne upravovali postupy orgánov činných v trestnom konaní tak, ako pri iných obdobných úkonoch upravených v Trestnom poriadku – ustanovuje sa, pri ktorých trestných činoch bude možné tieto úkony použiť, za akých podmienok sa bude dávať príkaz na tieto úkony, určuje sa doba ich použitia, ako aj podmienky ich použitia a ďalšie náležitosti*."

V súvislosti s touto zmenou boli v Trestnom poriadku z roku 1961vykonané ďalšie zmeny. V § 10 ods. 13 Trestného poriadku z roku 1961sa doplnil výklad pojmu „*informačno-technické prostriedky*". Následne bola do § 26a Trestného poriadku z roku 1961 doplnená aj osobitná príslušnosť súdu na vydanie príkazu na niektoré úkony pred začatím trestného stíhania a v prípravnom konaní. Na vydanie príkazu na vyhotovovanie obrazových, zvukových a iných záznamov bol pred začatím trestného stíhania a v prípravnom konaní príslušný krajský súd a vyšší vojenský súd, v ktorého obvode bol činný prokurátor, ktorý podal príslušný návrh.

V rámci rekodifikácie v roku 2005 bolo do § 114 TP prebraté ustanovenie o vyhotovovaní obrazových, zvukových alebo obrazovo-zvukových záznamov s viacerými zmenami. V názve inštitútu sa „iných záznamov" nahradilo spojením „obrazovo-zvukových záznamov". Tiež sa sprísnili podmienky vyhotovenia takýchto záznamov spojených s priamym vstupom do obydlia len za zločiny a taxatívne vymenované prečiny. V odseku 8 sa ustanovili pravidlá pre zničenie záznamov a informovanie dotknutých osôb o vyhotovení záznamov.[5]

Súčasná právna úprava vyhotovovania obrazových, zvukových alebo obrazovo-zvukových záznamov (§ 114 TP) spôsobuje množstvo aplikačných problémov v súvislosti s ich využitím v praxi, čo v konečnom dôsledku spôsobuje rôzne pochybnosti o zákonnosti postupu orgánov činných v trestnom konaní pri objasňovaní konkrétneho trestného činu a následnej prípustnosti takto získaných informácií. Vo svojom vystúpení upriamim svoju pozornosť na niektoré nedostatky právnej úpravy a prestavím návrhy del lege ferenda. Ďalšie nedostatky a návrhy sú uvedené v odbornej literatúre.[6]

Diskusia

Prevažne teoretickým problémom je skutočnosť, že zákonodarca používa nesprávnu terminológiu. Ako jeden z dôkazných prostriedkov je aj vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov (§ 114 TP). Zákonodarca v § 119 ods. 2 TP nesprávne ozna-

[5] Bližšie ZÁHORA, J. et al. Obrazové a zvukové záznamy v trestnom konaní. Bratislava: Wolters Kluwer 2018, s. 56.

[6] ZÁHORA, J. et al. Obrazové a zvukové záznamy v trestnom konaní. Bratislava: Wolters Kluwer 2018, s. 219 a nasl.

čuje za dôkazný prostriedok „informácie získané použitím informačno-technických prostriedkov". Informácie (poznatky) získané použitím ITP však predstavujú dôkaz. Za dôkaz sa považuje priamy poznatok získaný na základe a v súlade s Trestným poriadkom z dôkazného prostriedku. Dôkazný prostriedok je konkrétna procesná činnosť orgánov činných v trestnom konaní a súdu, všetky prostriedky, z ktorých možno získať dôkazy.[7] Z uvedeného vyplýva, že povahu dôkazného prostriedku má vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov a samotný obrazový, zvukový alebo obrazovo-zvukový záznam, na ktorom je zachytená osoba alebo vec, resp. zaznamenaný skutkový dej je prameňom dôkazu.[8]

Vzhľadom na to, že pri sledovaní osôb a vecí pripadá do úvahy aj využitie systémov na zistenie presnej pozície, známych ako GPS, európsky systém Galileo, resp. ruský Glonass, alebo čínsky BeiDou, bolo by potrebné upraviť definíciu informačno-technických prostriedkov (§ 10 ods. 21 TP) Európsky súd pre ľudské práva, vo viacerých rozhodnutia sa zaoberal problematikou sledovania prostredníctvom GPS zariadení vo vzťahu k práva na súkromie.[9] V prípade Uzun proti Nemecku[10] ESĽP posudzoval, či je sledovanie podozrivého z terorizmu primeraným zásahom do práva na súkromie. Sťažovateľ namietal skutočnosť, že sledovanie pomocou GPS a následné využitie v trestnom konaní porušuje právo na súkromie a následne aj právo na spravodlivý proces. Podľa názoru ESĽP samotné sledovanie prostredníctvom GPS, už s ohľadom na jeho povahu, je potrebné odlišovať od ostatných metód vizuálneho alebo akustického sledovania, ktoré spravidla môžu citlivejšie zasiahnuť do práva osoby na rešpektovanie súkromného života, keďže odhaľujú viacej informácií o konaní danej osoby, o jej názoroch či pocitoch. V záveroch ESĽP dospel k názoru, že zásah do súkromia sťažovateľa bol v súlade s čl. 8 Európskeho dohovoru o ochrane ľudských práv a základných slobôd. Vzhľadom na to, že išlo o vyšetrovanie veľmi závažných skutočností, ESĽP konštatoval, že sledovanie GPS bolo primerané. ESĽP dodáva, že policajné monitorovanie za pomoci údajov získaných z GPS neporušuje ľudské práva a v prípade závažných trestných činov je primeraným prostriedkom na odhaľovanie zločincov.

V inom prípade, Ben Faiza[11] ESĽP dospel k opačnému záveru. Pri posudzovaní otázky, či zásah bol „v súlade so zákonom", ESĽP zdôraznil, že čl. 81 francúzskeho trestného poriadku, ktorý bol aplikovaný na daný prípad, obsahoval len veľmi všeobecný pojem – informačné úkony, ktoré sa považujú za potrebné na preukázanie pravdy (*„les actes d'information qu'il juge utile à la manifestation de la vérité" – preklad autora*). Súd zdôraznil, že takáto právna úprava nemala atribút „predvídateľnosti", ako to vyžaduje čl. 8 Európskeho dohovoru. Okrem toho ESĽP zistil, že nedostatočná precíznosť francúzskej právnej úpravy v predmetnom čase nemohla byť kompenzovaná ani judikatúrou vnútroštátnych súdov.

Z uvedených dôvodov by bolo potrebné rozšíriť definíciu aj o „použité utajovaným spôsobom [...] pri sledovaní osôb a vecí", aby takáto právna úpravy napĺňala atribúty „predvídateľnosti", ako to vyžaduje ESĽP.

---

[7] Porovnaj IVOR, J., POLÁK, P., ZÁHORA, J. Trestné právo procesné1. Bratislava: Wolters Kluwer, 2017, s. 406.

[8] Porovnaj KUBIČKA, R. Informačno-technické prostriedky v trestnom konaní – analýza niektorých aspektov aktuálnej právnej úpravy s dôrazom na interpretačné problémy. In ZÁHORA, J. (ed.). Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní. Praha: Leges, 2017, s. 210.

[9] Bližšie ZANNONI, D. GPS Surveillance from the Perspective of the European Convention on Human Rights. In. European Criminal Law Review. 8/2018. s. 294 a nasl.

[10] Rozsudok ESĽP z 2. septembra 2010, Uzun proti Nemecku, č. 35623/05.

[11] Rozsudok ESĽP z 8. februára 2018, Ben Faiza proti Francúzsku, č. 31446/12.

Pochybnosti môže vyvolávať aj delenie dôkazných prostriedkov slúžiacich na získavanie informácií na ITP (§ 10 ods. 21 TP) a na prostriedky OPČ (§ 10 ods. 22 TP), keďže v praxi spravidla splývajú do jedného procesného postupu a ich účelom je získavanie zhodných dôkazov.[12]

V odbornej literatúre sa vyskytujú pochybnosti aj o tom, že právna úprava sledovania osôb a vecí s využitím ITP (§ 113 ods. 4 TP) a vyhotovovania obrazových, zvukových alebo obrazovo-zvukových záznamov (§ 114 TP) je zbytočne duplicitná, pretože spoločným menovateľom či podstatou týchto dôkazných prostriedkov je to, že ide vždy o sledovanie osôb, resp. vecí s následným vyhotovením obrazového a zvukového záznamu.[13]

Ako už bolo uvedené, sledovanie osôb a vecí bolo do slovenského Trestného poriadku po „vzore" Českej republiky doplnené novelou č. 422/2002 Z. z. s účinnosťou od 1. októbra 2002 do ustanovenia § 88d – štvrtej hlavy Trestného poriadku z roku 1961 nazvanej „Zaistenie osôb a vecí". Zároveň, bez hlbšej analýzy bolo do Trestného poriadku doplnené aj ustanovenie § 88e TP – „Vyhotovovanie obrazových, zvukových alebo iných záznamov", hoci česká úprava takýto inštitút neobsahovala.

V súčasnosti možno obrazové, zvukové alebo obrazovo-zvukové záznamy získavať v trestnom konaní v „dvoch režimoch".

Prvý režim je vyhotovenie takýchto záznamov v rámci inštitútu sledovania osôb a vecí (§ 113 ods. 4 TP). Ak [...] sa má popri sledovaní súčasne použiť ITP a sledovanie nie je spojené so vstupom do obydlia, príkaz na sledovanie vydáva predseda senátu, pred začatím trestného stíhania alebo v prípravnom konaní sudca pre prípravné konanie na návrh prokurátora, ak skutočnosti významné pre trestné konanie nemožno získať pri vykonaní sledovania iným spôsobom; v príkaze sa uvedie [...] druh ITP, ktorý sa má použiť. V tomto prípade sledovanie možno vykonať v trestnom konaní o **úmyselnom trestnom čine**, ak možno dôvodne predpokladať, že ním budú zistené skutočnosti významné pre trestné konanie.

Druhým režimom je samotné vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov (§ 114 TP), ktoré je prípustné v trestnom konaní pre **úmyselný trestný čin**, za 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. Vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov spojených **s priamym vstupom do obydlia** 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, a len s predchádzajúcim súhlasom predsedu senátu, pred začatím trestného stíhania alebo v prípravnom konaní sudcu pre prípravné konanie.

Z uvedeného vyplýva, že požiadavky na vyhotovovanie takýchto záznamov v zmysle sledovania osôb a veci(§ 113 ods. 4 TP) sú „benevolentnejšie" ako pri samotnom vyhotovovaní obrazových, zvukových alebo obrazovo-zvukových záznamov (§ 114 TP).

V prvom prípade je to možné „v trestnom konaní o **úmyselnom trestnom čine**", čiže môže to byť akýkoľvek úmyselný trestný čin, ak možno dôvodne predpokladať, že sledovaním budú zistené skutočnosti významné pre trestné konanie. V druhom prípade je to možné až pri závažnejších trestných činoch *„úmyselný trestný čin, za ktorý zákon ustanovuje trest odňatia slobody s **hornou hranicou trestnej sadzby prevyšujúcou tri roky**, korupciu [...]"*, ak možno dôvodne

[12] Bližšie ŠAMKO, P. Aplikačné problémy pri vyhotovovaní obrazových záznamov zo sledovania osôb alebo vecí. In Zo súdnej praxe. 2017, č. 1, s. 10.

[13] Bližšie ZÁHORA, J. et al. Obrazové a zvukové záznamy v trestnom konaní. Bratislava: Wolters Kluwer 2018, s. 220.

predpokladať, že vyhotovením obrazových, zvukových alebo obrazovo-zvukových záznamov budú zistené skutočnosti významné pre trestné konanie.

Podmienky na postup podľa § 114 TP sú oproti § 113 TP prísnejšie – len vybrané trestné činy. Postup podľa § 113 ods. 4 TP nemožno využiť, ak by sa malo vykonať sledovanie v obydlí (*„sledovanie nie je spojené so vstupom do obydlia"*), naproti tomu, postup podľa § 114 ods. 2 TP možno aplikovať aj v obydlí (*„vyhotovenie obrazových, zvukových alebo obrazovo-zvukových záznamov spojených s priamym vstupom do obydlia..."*). Rozsah postupu podľa § 114 ods. 2 TP je oproti ustanoveniu § 113 ods. 4 TP širší a s vážnejšími dôsledkami pre právo na súkromie.

K rozdielom medzi uvedenými inštitútmi sa pokúsil zaujať stanovisko aj Najvyšší súd SR,[14] ktorý zdôrazňuje, že postup podľa § 114 TP je špeciálnym vo vzťahu k postupu podľa § 113 TP, pričom procesný postup podľa § 113 ods. 4 TP (sledovanie so súčasným použitím ITP – za ITP treba považovať aj vyhotovenie obrazových, zvukových alebo obrazovo-zvukových záznamov v zmysle § 114 a § 10 ods. 21 TP) možno použiť len v prípade, ak nepôjde o trestné činu spadajúce do katalógu trestných činov vymenovaných v ustanovení § 114 ods. 1 a 2 TP a sledovanie nebude spojené so vstupom do obydlia. Inými slovami, ak je potrebné vykonať sledovanie spojené s použitím ITP (§ 113 ods. 4 TP) a so vstupom do obydlia, s tým, že pôjde o úmyselný trestný čin, za ktorý zákon ustanovuje trest odňatia slobody s hornou hranicou trestnej sadzby prevyšujúcou 3 roky, korupciu alebo iný úmyselný trestný čin, o ktorom na konanie zaväzuje medzinárodná zmluva (§ 114 ods. 1 TP), zločin, korupciu, trestný čin zneužívania právomoci verejného činiteľa, trestný čin legalizácie príjmov z trestnej činnosti alebo iný úmyselný trestný čin, o ktorom na konanie zaväzuje medzinárodná zmluva (§ 114 ods. 2 TP), musí sa postupovať podľa špeciálneho ustanovenia, a to podľa § 114 TP. Je pochopiteľné, že v rámci postupu podľa § 114 TP, napríklad pri použití kamery na zaznamenávanie obrazu i zvuku, dochádza k sledovaniu objektov i osôb v širšom slova zmysle, čo je ale logickým dôsledkom činnosti označeného technického zariadenia. Najvyšší súd SR dochádza k záverom, že postup podľa § 113 TP možno označiť ako tzv. ***„in move"***, a teda sledovanie v pohybe, naproti tomu, postup podľa § 114 TP je určený prioritne na stacionárne „sledovanie" ako tzv. ***„steady"*** procesný prostriedok.

S takýmito závermi Najvyššieho súdu SR nemožno súhlasiť, keďže nemajú oporu v žiadnom ustanovení Trestného poriadku. Hoci v § 113 TP sa predpokladá „získavanie informácií o pohybe a činnosti osoby alebo pohybe veci", v zmysle postupu podľa § 114 TP to nemusí byť „stacionárne sledovanie", ako to zdôrazňuje Najvyšší súd SR.

Máme za to, že takáto situácia je v trestnom konaní nežiaduca a podmienky na získavanie dôkazov by mali byť jasne a jednoznačne ustanovené. Určitým „námetom" by nám na základe odbornej analýzy znova mohla byť česká právna úprava, ktorá v § 158d českého trestního řádu (zákon č. 141/1961 Sb.) upravuje tri typy sledovania osôb a vecí:

a) všeobecné sledovanie osôb a vecí (odsek 1) **bez toho**, aby sa o takomto sledovaní vyhotovovali zvukové, obrazové alebo iné záznamy,
b) sledovanie, pri ktorom sú vyhotovované zvukové, obrazové alebo iné záznamy (odsek 2),
c) sledovanie, ktoré zasahuje do niektorých ústavne chránených práv a slobôd – nedotknuteľnosť obydlia, listové tajomstvo, tajomstvo iných písomností a záznamov uchovaných v súkromí (odsek 3)

Jednotlivé typy sledovania sa líšia aj druhom povoľovacieho režimu. V zmysle situácie uvedenej v odseku 1 citovaného ustanovenia (bez vyhotovovania záznamov ani nezasahujúce do ústavne chránených práv a slobôd) je plne v právomoci policajného orgánu. Ak sú pri sledovaní vyhotovované zvukové, obrazové alebo iné záznamy (odsek 2), tam sa vyžaduje písomné povo-

[14] Uznesenie Najvyššieho súdu SR zo 14. septembra 2016, sp. zn. 6 Tdo 31/2016.

lenie štátneho zástupcu, a v prípade sledovania so zásahom do ústavne chránených práv a slobôd sa vyžaduje povolenie sudcu.[15]

Ďalším z problémov, na ktorý by sme chceli poukázať pri vyhotovovaní obrazových a zvukových záznamov, je explicitné ustanovenie kategórií trestných činov, pre ktoré je možno vydať príkaz na vyhotovovanie takýchto záznamov. Táto požiadavka je v súlade s minimálnymi zárukami definovanými ESĽP,[16] v zmysle ktorých zákonná úprava musí jasne určiť **kategórie trestných činov**, vo vzťahu ku ktorým je možné nariadiť tajné sledovanie. ESĽP tiež pripomenul, že požiadavka **predvídateľnosti** zákonnej úpravy má v kontexte tajného sledovania odlišný obsah ako v iných oblastiach. Keďže v týchto prípadoch sa výkonná moc realizuje utajovaným spôsobom, riziko zneužitia je zjavné. **Je preto celkom zásadné, aby zákon obsahoval jasné a podrobné pravidlá pre toto tajné sledovanie.** Zákon musí byť dostatočne jasný, aby jednotlivcovi poskytol adekvátny návod ohľadom okolností a podmienok, za ktorých sú orgány príslušné k takémuto oprávneniu pristúpiť.[17] V podobnom duchu je aj judikatúra Súdneho dvora EÚ,[18] v zmysle ktorej pri zásahu do práva na súkromie právna úprava musí *„stanoviť jasné a presné pravidlá upravujúce rozsah a uplatnenie predmetného opatrenia."* V rozhodnutí *Sallinen*[19] ESĽP vyslovil záver, že vnútroštátne právo musí poskytovať jednotlivcovi ochranu proti arbitrárnemu zásahu do jeho práv zaručených čl. 8 Európskeho dohovoru, preto musí dostatočne **jasne v pojmoch** poskytovať občanovi náležitú indikáciu podľa okolností a podmienok, za akých je verejná autorita zmocnená na zásahy do jeho práva na súkromie.

Domnievame sa, že „prvé dve" kategórie trestných činov, pri ktorých možno povoliť vyhotovenie obrazových a zvukových záznamov (trestný čin, za ktorý zákon ustanovuje trest odňatia slobody s hornou hranicou trestnej sadzby **prevyšujúcou tri roky** a **korupcia**), sú pomerne jasne vymedzené a nespôsobujú aplikačné problémy. Problémy môžu nastať až pri **„tretej kategórii"** (iný úmyselný trestný čin, o ktorom na konanie **zaväzuje medzinárodná zmluva**). Problematický je aj výklad slovného spojenia „na konanie zaväzuje medzinárodná zmluva". Je diskutabilné, či v predmetnej zmluve musí byť výslovne uvedené napríklad: *„Každá zmluvná strana prijme potrebné legislatívne a iné opatrenia, aby zabezpečila, že **nasledujúce úmyselné konanie je trestné**"*[20] alebo stačí všeobecná formulácia: *„Štáty, ktoré sú zmluvnou stranou Dohovoru, robia všetky opatrenia nevyhnutné na zabezpečenie obnovy starostlivosti o dieťa zo strany rodičov alebo iných osôb, ktoré nesú za dieťa finančnú zodpovednosť, nech už na území štátu, ktorý je zmluvnou stranou Dohovoru, alebo v zahraničí."*[21]

Čentéš[22] zdôrazňuje, že tento pojem nemožno vykladať tak, že ide len o trestné činy, na ktorých stíhanie zaväzuje **priamo či bezprostredne** medzinárodná zmluva, pretože v takom prípade by bol ich okruh veľmi obmedzený, 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

[15] Porovnaj ŠÁMAL, P. a kol. Trestní řád. Komentář. 7. vydání. Praha: C. H. Beck, 2013, s. 2001 a nasl.

[16] Napríklad rozsudok ESĽP z 24. apríla 1990, Kruslin proti Francúzsku, č. 11801/85, § 35; rozsudok ESĽP zo 4. decembra 2015, Roman Zakharov proti Rusku, č. 47143/06, § 231; rozsudok ESĽP z 12. januára 2016, Szabó a Vissy proti Maďarsku, č. 37138/14, § 56; rozsudok ESĽP zo 7. novembra 2017, Akhlyustin proti Rusku, č. 21200/05, § 41; rozsudok ESĽP z 19. júna 2018, Centrum för Rättvisa proti Švédsku, č. 35252/08, § 103.

[17] Bližšie ZÁHORA, J. Minimálne záruky pre tajné sledovanie štátnymi orgánmi. In Justičná revue. 2018, č. 3, s. 338 a nasl.

[18] Rozsudok Súdneho dvora (veľká komora) z 8. apríla 2014, spojené veci C 293/12 a C 594/12, § 54.

[19] Rozsudok ESĽP z 27. septembra 2005, Petri Sallinen proti Fínsku, č. 50882/99.

[20] Napríklad čl. 18 Dohovoru Rady Európy o ochrane detí pred sexuálnym vykorisťovaním a sexuálnym zneužívaním (oznámenie MZV a EZ SR č. 164/2016 Z. z.).

[21] Článok 27 ods. 4 Dohovoru o právach dieťaťa (oznámenie FMZV č. 104/1991 Zb.).

[22] ČENTEŠ, J. Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. Bratislava: C. H. Beck, 2013, s. 100.

vykonáva podľa skutkových podstát trestných činov, ktoré sú súčasťou vnútroštátneho právneho poriadku. Šámal[23] citovanú formuláciu z Dohovoru o právach dieťaťa považuje okrem iných prípadov aj za záväzok stíhať trestný čin zanedbania povinnej výživy podľa § 207 TZ. Takýto výklad je značne problematicky a chýba mu predvídateľnosť právnej úpravy.

Z dôvodu, aby sme predišli možným interpretačným a aplikačným problémom, navrhujeme nahradiť slovné spojenie ***„iný úmyselný trestný čin, o ktorom na konanie zaväzuje medzinárodná zmluva"*** napríklad taxatívnym výpočtom ďalších trestných činov, pri ktorých je možné vykonať vyhotovovanie obrazových a zvukových záznamov alebo toto spojenie vypustiť bez náhrady.

Medzi najčastejšie nedostatky príkazov na vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov, ktoré sú najčastejšie napádané v rámci súdneho prieskumu, patrí aj absencie, resp. nedostatočnosť, odôvodnenia príkazu.

Na rozdiel od iných príkazov, ktorými sa zasahuje do základných práv a slobôd, napríklad odpočúvanie a záznam telekomunikačnej prevádzky (§ 115 ods. 3 TP), oznámenie údajov o telekomunikačnej prevádzke (§ 116 ods. 2 TP), agent (§ 117 ods. 5 TP), pri príkaze na vyhotovenie obrazových, zvukových alebo obrazovo-zvukových záznamov zákonodarca *„opomína"* ako obligatórnu náležitosť príkazu aj **odôvodnenie**.

Trestný poriadok v § 114 ods. 2 vymedzuje, že príkaz na vyhotovovanie takýchto záznamov musí byť **písomný**, pričom v § 114 ods. 3 dopĺňa, že v príkaze musí byť ustanovený **čas**, v ktorom bude vykonávané vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov. Citované ustanovenie však neobsahuje ani zmienku o odôvodnení príkazu, v § 114 ods. 2 TP sú vymedzené iba náležitosti „návrhu". 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. Obdobne ani zákon o ochrane pred odpočúvaním neustanovuje náležitosti „súhlasu" na použitie ITP. V § 4 ods. 3 zákona o ochrane pred odpočúvaním[24] sú ustanovené iba náležitosti „žiadosti o použitie ITP".

Ústavný súd SR už v rámci svojej judikatúry viackrát vyslovil, že podľa jeho názoru nemôžu byť nijaké pochybnosti o tom, že príkaz a súhlas musia byť odôvodnené v každom prípade, či už boli vydané na základe Trestného poriadku, alebo na základe zákona o ochrane pred odpočúvaním. Hoci predmetné zákony používajú rozdielnu terminológiu, nemôžu byť pochybnosti o tom, že tak súhlas, ako aj príkaz, majú formálne, ale aj obsahové náležitosti rozhodnutia. Aj napriek absencii výslovnej požiadavky na odôvodnenie uvedeného príkazu alebo súhlasu, máme za to, že uvedené rozhodnutia **musia byť odôvodnené**. Požiadavka odôvodnenosti súdnych rozhodnutí, ktorými sa zasahuje do základných práv a slobôd, vyplýva z rozhodovacej činnosti Ústavného súdu SR. Obsahom základného práva na súdnu ochranu podľa čl. 46 ods. 1 Ústavy SR a práva na spravodlivé súdne konanie podľa čl. 6 ods. 1 Európskeho dohovoru je aj právo či už 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.[25]

Je to tak preto, že hoci ide o závažný zásah do základného práva, dotknuté osoby nemajú možnosť podať opravný prostriedok a o vydaní súhlasu či príkazu sa dozvedia spravidla až dodatočne, keď už zásah do práva na súkromie bol realizovaný. Majú preto možnosť žiadať o preskúmanie opodstatnenosti súhlasu či príkazu až dodatočne. Pri dodržaní režimu utajenia sa

[23] ŠÁMAL, P. a kol. Trestní řád. Komentář. 7. vydání. Praha: C. H. Beck, 2013, s. 1121.

[24] 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.

[25] Nález Ústavného súdu SR z 27. septembra 2011, sp. zn. III. ÚS 133/2010-67.

dotknuté osoby môžu o vydaní súhlasu či príkazu a o dôvodoch, ktoré k tomu viedli, dozvedieť len dodatočne, teda iba po realizácii potrebných úkonov. Pokiaľ v rámci odôvodnenia príkazu nie sú uvedené žiadne konkrétne skutočnosti, ktoré viedli k jeho vydaniu, ale text odôvodnenia iba cituje žiadosť, na základe ktorej má byť súhlas vydaný, a zákonom ustanovené podmienky na vydanie príkazu, resp. súhlasu, takýto spôsob odôvodnenia nemožno akceptovať a treba ho považovať za zjavne neodôvodnený. Rozhodne si z neho nemožno utvoriť obraz o tom, aké konkrétne skutočnosti viedli k jeho vydaniu.[26] Preskúmateľnosť dôvodnosti vydania súhlasu či príkazu si vyžaduje relevantnú, konkrétnu vysvetľujúcu argumentáciu, akými skutočnosťami boli naplnené zákonom ustanovené podmienky na tento zásah do práva na súkromie. Bez takéhoto odôvodnenia, opierajúceho sa o konkrétne skutočnosti, je súhlas či príkaz spravidla nepreskúmateľný.[27] Z odôvodnenia musí vyplývať, aké konkrétne dôkazy boli sudcovi predložené, ako aj odkaz na konkrétny spisový materiál obsahujúci všetky relevantné informácie spôsobilé z pohľadu súdu ospravedlniť zásah do práva na súkromie.[28]

Ústavný súd SR zdôrazňuje, že zmyslom vymedzenia nevyhnutných obsahových náležitostí priamo na úrovni zákona je zabezpečiť, aby súd pri svojom rozhodovaní disponoval všetkými potrebnými informáciami, ktoré sú pre orgány činné v trestnom konaní bez väčších ťažkostí dostupné. V tejto súvislosti Ústavný súd SR zdôrazňuje požiadavku dôslednosti a efektivity súdnej kontroly, a to s ohľadom na povahu daného konania, ktoré **nepredpokladá účasť protistrany pred rozhodnutím súdu**. Úloha súdu tak spočíva i vo *„vyvažovaní"* procesnej situácie, pričom je neprípustné, aby sa súd dostal do pozície „pomocníka" verejnej žaloby, pretože musí byť vždy nestranný.[29]

Ako už bolo uvedené, zastávame názor, že príkaz na vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov **musí byť odôvodnený**. Je to tak preto, že hoci ide o závažný zásah do základného práva, dotknuté osoby nemajú možnosť podať proti takému rozhodnutiu opravný prostriedok a o jeho vydaní sa dozvedia spravidla až dodatočne (ak vôbec), keď už zásah do práva na súkromie bol realizovaný. Majú preto možnosť žiadať o jeho preskúmanie až dodatočne. Obsahom základného práva na súdnu ochranu podľa čl. 46 ods. 1 Ústavy SR a práva na spravodlivé súdne konanie podľa čl. 6 ods. 1 Európskeho dohovoru je aj 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. Ústavný súd SR pripomína, že všeobecný súd nemusí dať odpoveď na všetky otázky, ale len na tie, ktoré majú pre vec podstatný význam, prípadne dostatočne objasňujú skutkový a právny základ rozhodnutia bez toho, aby zachádzali do všetkých detailov veci. Absencia relevantného odôvodnenia rozhodnutí (aj napriek tomu, že zákonná úprava výslovne odôvodnenie nevyžadovala) zakladá porušenie práva na súdnu ochranu a práva na spravodlivé súdne konanie.[30]

Máme za to, že je nevyhnutné priamo v texte § 114, resp. aj § 113 TP ustanoviť ako obligatórnu súčasť príkazu aj odôvodnenie, obdobne ako pri príkaze na odpočúvanie a záznam telekomunikačnej prevádzky podľa § 115 ods. 3 TP. Ako možné legislatívne vyjadrenie by sme navrhovali: ***„Príkaz na vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov sa musí vydať písomne a odôvodniť aj skutkovými okolnosťami a podozrením z konkrétnej***

[26] Nález Ústavného súdu SR z 13. júna 2012, sp. zn. I. ÚS 114/2012.
[27] Uznesenie Ústavného súdu SR z 20. novembra 2012, sp. zn. III. ÚS 97/2012-124.
[28] PERHÁCS, Z. O nevyhnutných atribútoch rozhodnutia sudcu na použitie informačno-technických prostriedkov. In Bulletin slovenskej advokácie. 2013, č. 12, s. 15.
[29] Nález pléna Ústavného súdu SR z 29. apríla 2015, sp. zn. PL. ÚS 10/2014.
[30] Nález Ústavného súdu SR zo 4. februára 2009, sp. zn. I. ÚS 117/07.

trestnej činnosti a tiež údajmi o osobách a veciach, ktorých sa vyhotovovanie obrazových, zvukových alebo obrazovo-zvukových záznamov týka, ak sú tieto údaje známe." Obdobná úprava by mohla byť obsiahnutá aj v § 4 zákona o ochrane pred odpočúvaním. Zmyslom vymedzenia nevyhnutných obsahových náležitostí priamo na úrovni zákona je zabezpečiť, aby súd pri svojom rozhodovaní v príkaze uviedol všetky relevantné skutočnosti, ktorými disponoval pri vydávaní príkazu, resp. súhlasu.

Záver

Ako už bolo v úvode zdôraznené, vzhľadom na obmedzený časový rozsah vo vystúpení sa nedalo venovať všetkým nedostatkom právnej úpravy. Pozornosť sme zamerali iba na vybrané problém, s ďalšími návrhmi sa môže čitateľ zoznámiť v odbornej literatúre.[31]

Ako už v predchádzajúcich príspevkoch odznelo, osobitnú pozornosť, si vyžaduje aj nejednotná súdna prax týkajúca sa prípustnosť súkromnej nahrávky. Niektoré súdy pripúšťajú takto získané dôkazy, iné takto získané dôkazy, získané bez súhlasu zaznamenávanej osoby považujú za záznam získaný v rozpore so zákonom, čím je takýto dôkazný prostriedok v trestnom konaní neprípustný. V tomto prípade je dosť ťažko si predstaviť legislatívne riešenie, ktoré by uspokojivo vyriešilo tento problém. Ako najvhodnejšie riešenie prezentovanej rozdielnej praxe slovenských súdov týkajúcej sa prípustnosti súkromnej nahrávky v trestnom konaní, ktorá nespĺňa podmienky prístupu a predvídateľnosti, by bolo potrebné prijať zjednocujúce stanovisko trestnoprávneho kolégia Najvyššieho súdu, kde by boli naznačené hlavné východiská, podľa ktorých by sa posudzovala prípustnosť súkromných nahrávok v trestnom konaní.

Literatúra

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

IVOR, J., POLÁK, P., ZÁHORA, J. *Trestné právo procesné 1*. Bratislava: Wolters Kluwer, 2017.

KUBIČKA, R. Informačno-technické prostriedky v trestnom konaní – analýza niektorých aspektov aktuálnej právnej úpravy s dôrazom na interpretačné problémy. In ZÁHORA, J. (ed.). *Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní*. Praha: Leges, 2017, s. 209 – 220.

ŠÁMAL, P. a kol. *Trestní řád. Komentář.* 7. vydání. Praha: C. H. Beck, 2013.

ŠAMKO, P. Aplikačné problémy pri vyhotovovaní obrazových záznamov zo sledovania osôb alebo vecí. In *Zo súdnej praxe*. 2017, č. 1, s. 10 – 13.

ZÁHORA, J. Minimálne záruky pre tajné sledovanie štátnymi orgánmi. In *Justičná revue*. 2018, č. 3, s. 335 – 349.

ZÁHORA, J. et al. *Obrazové a zvukové záznamy v trestnom konaní*. Bratislava: Wolters Kluwer 2018.

ZANNONI, D. GPS Surveillance from the Perspective of the European Convention on Human Rights. In. *European Criminal Law Review*. 8/2018. s. 294 – 312.

[31] Záhora, J. et al. Obrazové a zvukové záznamy v trestnom konaní. Bratislava: Wolters Kluwer 2018, s. 219 a nasl.