Podání – České PIS

Policie ČR má v průběhu vyšetřování trestné činnosti oprávnění vlastními silami dešifrovat zachycenou komunikaci nebo zajištěné datové nosiče.

Abychom si mohli odpovědět na zmíněnou otázku, tak se musíme nejprve zabývat předběžnou otázkou, a to jakým způsobem vůbec policie v rámci vyšetřování zachytává cizí komunikaci a jaké jsou k tomu potřeba povolení? Jak se k tomu staví Listina základních lidských práv a svobod (dále jako LZPS)[1], relevantní právní předpisy a judikatura? Aby policie, či jiný orgán mohl dešifrovat zachycenou komunikaci (odposlech), musí mít, v prvé řadě, povolení tento odposlech získat. Ve druhé fázi se pak budeme zabývat, zda má policie právo zajistit datový nosič, a to jak v režimu online, tak v režimu offline.

LZPS jako náš základní lidskoprávní zákon v článku 7 uvádí, že nedotknutelnost osoby a jejího soukromí je zaručena a omezena může být jen v případech stanovených zákonem. A následně v článku 13 přiznává ochranu listovnímu tajemství a zprávám podávaných telefonem. Může se tedy zdát, že zachycená komunikace, byť možná šifrovaná, je LZPS chráněna, protože se jedná o sféru soukromí těch konkrétních lidí. Ve stejném duchu mluví i nález Ústavního soudu: *„Ústavní soud v minulosti již dospěl k závěru, že právo na ochranu tajemství zpráv podávaných telefonem, plynoucí z čl. 13 Listiny základních práv a svobod, jako ústavně zaručené právo svou povahou a významem spadá mezi základní lidská práva a svobody, neboť spolu se svobodou osobní a dalšími ústavně zaručenými základními právy dotváří osobnostní sféru jedince, jehož individuální integritu jako zcela nezbytnou podmínku důstojné existence jedince a rozvoje lidského života vůbec je nutno respektovat a důsledně chránit“*[2]. Nicméně zákon, konkrétně Trestní Řád[3] (dále jako TŘ) ve svém § 88 připouští povolení provádění odposlechu a to v situaci, kdy: *„Je vedeno trestní řízení pro zločin, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně osm let, pro trestný čin pletichy v insolvenčním řízení podle § 226 trestního zákoníku, porušení předpisů o pravidlech hospodářské soutěže podle § 248 odst. 1 písm. e) a odst. 2 až 4 trestního zákoníku, sjednání výhody při zadání veřejné zakázky, při veřejné soutěži a veřejné dražbě podle § 256 trestního zákoníku, pletichy při zadání veřejné zakázky a při veřejné soutěži podle § 257 trestního zákoníku, pletichy při veřejné dražbě podle § 258 trestního zákoníku, zneužití pravomoci úřední osoby podle § 329 trestního zákoníku nebo pro jiný úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní*

[1] Ústavní zákon č. 2/1993 Sb., Listina základních lidských práv a svobod, ve znění ústavního zákona č. 162/1998 Sb. In: Codexis ACADEMIA [právní informační systém]. [cit. 29. 11. 2018].
[2] Nález Ústavního soudu ČR ze dne 3. 8. 2010, sp. zn. IV. ÚS 1556/07-1. Ústavní soud [cit. 29. 11. 2018]. In: Codexis ACADEMIA [právní informační systém].
[3] Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů. In: Codexis ACADEMIA [právní informační systém]. [cit. 29. 11. 2018].

smlouva." V takových případech může být vydán souhlas k odposlechu a záznamu komunikace, pokud lze předpokládat, že se tímto postupem orgány činné v trestním řízení (Policie České republiky) dopídí k významným skutečnostem nebo informacím. Takové povolení smí vydat, v průběhu vyšetřování trestné činnosti, pouze soudce v přípravném řízení, a to na návrh státního zástupce. I tento postup má svoji výjimku, a to když je prováděn odposlech a záznam telekomunikačního provozu mezi obhájcem a obviněným, což je samozřejmě nepřípustné. Zjistí-li proto policejní orgán při odposlechu, že obviněný komunikuje se svým obhájcem, je povinen odposlech ihned přerušit, záznam o jeho obsahu zničit a informace, které se v této souvislosti dozvěděl, nesmí nijak nepoužít. Stejně tak, jestliže při odposlechu a záznamu nebyly zjištěny skutečnosti významné pro trestní řízení, je nutno záznamy předepsaným způsobem zničit. Význam odposlechu shrnuje ve své judikatuře i Nejvyšší soud: *„Odposlech a záznam telekomunikačního provozu je zajišťovacím institutem, který je svou povahou velmi blízký operativně pátracím prostředkům podle § 158b a násl. tr. ř., a v širším smyslu tedy slouží k předcházení, odhalování a objasňování trestné činnosti, jakož i pátrání po skrývajících se pachatelích, pátrání po hledaných nezvěstných osobách a po věcných důkazech. Lze jej považovat za podklad pro další konání trestního řízení, v němž teprve jsou skutečnosti, které jsou v odposlechu zaznamenány, prověřovány a objasňovány. Použití záznamu telekomunikačního provozu jako důkazu v jiné trestní věci (§ 88 odst 6 věta třetí tr. ř.) nebrání skutečnost, že řízení, ve kterém byl odposlech a záznam telekomunikačního provozu proveden (§ 88 odst 1 tr. ř.), se již nekoná (např. trestní stíhání nebylo vůbec zahájeno), nebo že právní kvalifikace skutku, která podle § 88 odst 1 tr. ř. vedla k vydání příkazu k odposlechu a záznamu telekomunikačního provozu, se v dalším řízení neprokázala a obviněný nebyl takovým trestným činem uznán vinným."*[4]

Formální stránku věci, zejména jakým způsobem musí být povolení uděleno[5] nebo jakým způsobem musí být označen důkaz pocházející z takového provádění odposlechu, nechme pro naše účely stranou. Zaměřme se spíše na materiální stránku věci, kterou řešil ve svém nálezu[6] i Ústavní soud, který zdůraznil, že nezáleží pouze na tom, zda jsou splněny formální podmínky pro použití odposlechu, ale že je potřeba zvážit i materiální podmínky, tedy jak důležitá daná kauza skutečně je. Hodí se uvést, že existují i situace, kdy nemusí být soudní povolení, a to v momentě, kdy účastník odposlouchávané stanice a priori souhlasí. V tomto případě může policejní orgán

[4] Usnesení Nejvyššího soudu ČR ze dne 16. 7. 2014, sp. zn. 8 Tdo 109/2014-63. Nejvyšší soud [cit. 29. 11. 2018]. In: Codexis ACADEMIA [právní informační systém].
[5] Usnesení Nejvyššího soudu ČR ze dne 27. 7. 1995, sp. zn. Tzn 24/95. Nejvyšší soud [cit. 29. 11. 2018]. In: Codexis ACADEMIA [právní informační systém].
[6] Nález Ústavního soudu ČR ze dne 23. 5. 2007, sp. zn. II. ÚS 615/06. Ústavní soud [cit. 29. 11. 2018]. In: Codexis ACADEMIA [právní informační systém].

nařídit odposlech bez povolení soudu, a i pro trestné činy, pro které to zákon nepovoluje.[7] Sluší se uvést judikát, který říká, že článek 13 LZPS chrání pouze účastníka odposlechu, který hovor vede, nikoliv druhého účastníka, který hovor přijímá. Vykládat si článek opačně je zcela absurdní, protože by pak musel dávat svolení k odposlechu každý účastník s kým by byl hovor navázán, což by zcela popíralo smysl a logiku hlavy čtvrté oddílu šestého TŘ.[8]

V souvislosti s tím, co jsme si dosud uvedli, tak již víme, kdy je záznam komunikace ve vyšetřování možný a kdy ne. Můžeme tedy dovodit, že Policie má oprávnění vlastními silami dešifrovat takto zaznamenanou komunikaci. Je to ale v jejich silách? Pojďme si tuto problematiku ještě blíže upřesnit. Šifrovaný text, komunikace, či záznam je sdělení, které je nějakým způsobem chráněno proti každému, komu není určeno. Dešifrováním tedy rozumíme proces, kdy šifrované sdělení převádíme na „otevřený text", kterému jsme schopni porozumět.

V souvislosti se schopností Policie České republiky, respektive jejich orgánů, úspěšně dešifrovat zachycenou komunikaci musíme zmínit, že před 4 lety došlo k zadání veřejné zakázky, kterou zadalo Ministerstvo Vnitra Ústavu výpočetní techniky Masarykovy univerzity. Jedním z bodů zakázky je přímo určení typu šifrované komunikace a její dekódování policejními orgány. Od tohoto záměru si policie slibovala možnost sledovat šifrovanou komunikaci online. Hlavním důvodem byla skutečnost, že pachatelé trestné činnosti začaly využívat mnohé šifrovací systémy.[9] Tuto snahu ovšem experti označili jako marnou, jeden z nich se konkrétně vyjádřil takto: *„S případem, že by české orgány činné v trestním řízení dokázaly prolomit šifrování jsem se ještě nesetkal a předpokládám, že ani nikdy nesetkám. Pokud se české policii podařilo získat přístup k digitálním datům, která uživatelé chtěl utajit, bylo to způsobeno podle všeho nikoliv schopnostmi policejních orgánů, ale neschopností uživatele dobře si ošetřit vlastní elektronickou komunikaci."*[10] O tom, v jakém stavu je současná situace ohledně zakázky a zda již policie používá onen nový dešifrovací systém, se můžeme jen domnívat. Jak ale vyplývá ze zamítavého rozhodnutí ředitele utajovacího odboru, tak brněnská technika svůj úkol skutečně splnila.[11]

Ve druhé části otázky se zabýváme tím, zda má policie právo zajistit datový nosič. Když se vrátíme zpět do TŘ, konkrétně do ustanovení § 78, které nám říká, že ten, kdo má hmotnou věc

[7] STONOVÁ, Michaela. Právní úprava odposlechů a kryptoanalýzy. Právnická fakulta Masarykovy univerzity v Brně. [online]. publikováno 2008 s. 45 [cit. 29. 11. 2018]. Dostupné z: https://is.muni.cz/th/qprwf/Pravni_uprava_odposlechu_a_kryptoanalyzy_51438.pdf

[8] Rozsudek Krajského soudu ČR ze dne 9. 1. 2002, sp. zn. 5 T 104/2001. Krajský soud [cit. 29. 11. 2018]. In: Codexis ACADEMIA [právní informační systém].

[9] Vnitro zadalo zakázku na dekódování šifrované komunikace. Česká justice [online], publikováno 4.8.2014 [cit. 29. 11. 2018]. Dostupné z: http://www.ceska-justice.cz/2014/08/vnitro-zadalo-zakazku-na-dekodovani-sifrovane-komunikace/

[10] Vnitro chce rozbíjet šifry, podle expertů ho čeká neúspěch. Česká justice [online], publikováno 17.8.2014 [cit. 29. 11. 2018]. Dostupné z: http://www.ceska-justice.cz/2014/08/vnitro-chce-rozbijet-sifry-podle-expertu-ho-ceka-neuspech/

[11] Zamítavé rozhodnutí. Paragraphos.pecina.cz [online], publikováno 4.5.2018 [cit. 29. 11. 2018]. Dostupné z: https://paragraphos.pecina.cz/special/doc/pdf?Rozhodnuti_MV_3.5.2018.pdf

u sebe, která je důležitá pro trestní řízení, musí ji na vyzvání soudu předložit soudu, státnímu zástupci nebo policii, pokud tak neučiní, může mu být věc odňata. Tuto povinnost má každý, kdo má věc u sebe, nejen majitel. V případě existence elektronických online důkazů, pak povinnou osobou vydat tyto důkazy může být například poskytovatel služeb hostingu, telekomunikační provozovatel a podobně. Zde je důležité zmínit, že zajištění datových médií může policie provést i při domovní prohlídce a prohlídce jiných prostor. Takovou prohlídku musí, v přípravném řízení, povolit soudce. Judikatura Ústavního soudu se k tomuto postupu staví v souladu s právními předpisy, pro případ si můžeme uvést právní větu důležitého usnesení, které je zveřejněné i ve Sbírce nálezů a usnesení Ústavního soudu a sice: *„Je-li dáno důvodné podezření, že nosiče informací obsahují údaje a informace důležité pro trestní řízení, jsou-li tedy splněny podmínky pro zajištění těchto nosičů, nemůže tvrzení osoby, u níž se prohlídka provádí, či tvrzení jiné osoby při prohlídce přítomné, že nosiče informací obsahují i informace, ve vztahu k nimž je tato osoba vázána povinností mlčenlivosti, zabránit zajištění těchto nosičů. Nelze-li toto tvrzení v průběhu prohlídky ověřit a není-li možno oddělit část nosičů informací, které jsou věcmi důležitými pro trestní řízení, od těch nosičů, které obsahují informace netýkající se trestního řízení a jsou chráněny státem uloženou povinností mlčenlivosti, je třeba při provádění prohlídky s prvkem výpočetní techniky zajistit a zadokumentovat veškerou výpočetní techniku a záznamová média, u nichž lze důvodně předpokládat, že obsahují informace důležité pro trestní řízení.“*[12]

Závěrem můžeme nyní směle konstatovat, že Policie České republiky má, v průběhu vyšetřování trestné činnosti, oprávnění vlastními silami dešifrovat zachycenou komunikaci a také má možnost zajistit datový nosič.

[12] Usnesení Ústavního soudu ze dne 28. 3. 2002 sp. zn. IV. ÚS 2/02. Ústavní soud [cit. 29. 11. 2018]. In: Codexis ACADEMIA [právní informační systém].