

ZÍSKÁVÁNÍ TELEKOMUNIKAČNÍCH DAT JAKO NÁSTROJ V BOJI S INTERNETOVOU KRIMINALITOU

LENKA POŠÍKOVÁ

Internet, celosvětově propojený systém počítačových sítí, se stal součástí našeho života. Revoluce v informačních technologiích zásadním způsobem změnila svět. Důsledkem rychlého rozvoje telekomunikačních prostředků v poslední době došlo nejenom ke vzniku nových forem trestné činnosti, ale i tradiční trestné činy jsou páčány pomocí nových technologií. Internetová kriminalita už dávno není spojena jen s počítačem či notebookem. Na trh přicházejí nové technické prostředky,¹ které obsahují výkonné mikroprocesory a operační paměť,² takže umožňují obdobné operace. Kriminální jednání se stává dalekosáhlejším, neboť není omezeno zeměpisnými hranicemi, což navíc i komplikuje vyšetřování.

1. K VÝVOJI PRÁVNÍ ÚPRAVY V OBLASTI UCHOVÁVÁNÍ ÚDAJŮ O USKUTEČNĚNÉM TELEKOMUNIKAČNÍM PROVOZU

Hrozba zneužití elektronických informačních systémů k páčání trestné činnosti si vyžádala rychlou odezvu i v oblasti trestního práva procesního. Již v roce 1995 bylo Výborem ministrů přijato Doporučení č. R (95) 13, které radí členským státům přijmout odpovídající právní prostředky pro boj s internetovou kriminalitou. Jako jeden z nástrojů bylo doporučeno vložit do rukou vyšetřujících orgánů pravomoc nařídít provozovatelům telekomunikačních služeb poskytnutí potřebných dat a informací. Providerům,³ kteří nabízejí telekomunikační služby pro veřejnost, ať už veřejných nebo soukromých sítí, měla být podle tohoto Doporučení uložena zvláštní povinnost poskytnout informace vedoucí k identifikaci uživatele.⁴

Ustanovení § 88a zákona č. 141/1961 Sb., o trestním řízení soudním (dále jen TŘ), zakotvující postup při získávání údajů o uskutečněném telekomunikačním provozu bylo do trestního řádu doplněno novelou č. 265/2001 Sb., s účinností od 1. 1. 2002, a to

¹ Novými technickými prostředky v této oblasti jsou například mobilní telefony tzv. nové generace s přístupem na internet apod.

² VOLEVECKÝ, P. K pojmu počítačová kriminalita. *Bezpečnostní teorie a praxe*, č. 4, 2008, s. 68.

³ Pojmem provider se rozumí poskytovatel internetového připojení.

⁴ Recommendation No. R (95) 13 of the Committee of Ministers to Member States, bod 12.

na základě pozměňovacího návrhu Výboru pro obranu a bezpečnost. Důvodem k novelizaci bylo několik nálezů Ústavního soudu⁵ týkajících se práva na ochranu zpráv podávaných telefonem. Stěžovatelé se obraceli na Ústavní soud, neboť se domnívali, že způsob, kterým policejní orgán získal údaje o telekomunikačním provozu, byl nezákonný. Telekomunikační společnost tento výpis poskytla orgánům policie na základě blíže nespecifikované žádosti a bez souhlasu stěžovatele, čímž došlo k zásahu do jejich zaručených základních lidských práv a svobod.⁶ Jádrem věci bylo posoudit, zda se čl. 13 Listiny základních práv a svobod vztahuje nejen na samotný obsah zpráv podávaných telefonem, ale i na údaje o volaných číslech, datum a čas hovoru, dobu jeho trvání atd. Ústavní soud se ve svých rozhodnutích ztotožnil s názorem Evropského soudu pro lidská práva vyjádřeným ve věci *Malone v. Spojené království*,⁷ že „je třeba takové údaje považovat za nedílnou součást komunikace. Článek 13 Listiny nezakládá pouze ochranu tajemství vlastního obsahu zpráv, ale i tzv. vedlejších složek“. Pojem „záznam“ telekomunikačního provozu se tak vztahuje i na údaje získané jeho evidencí.

Orgány činné v trestním řízení byly napříště povinny při získávání údajů o telekomunikačním provozu postupovat přiměřeně dle § 88 TR, tedy obdobně jako při získávání odposlechu a záznamu telekomunikačního provozu.⁸ A to do doby, než byla přijata specifická úprava opatřování těchto údajů. Ve vztahu k § 88 TR byly podmínky pro poskytnutí údajů o uskutečněném telekomunikačním provozu stanoveny o poznání benevolentněji. Za dostatečný důvod byla považována již potřeba *objasnění skutečností důležitých pro trestní řízení*.

Uchovávání provozních a lokalizačních údajů a jejich poskytování oprávněným orgánům je upraveno zákonem č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (ZEK) a do dubna roku 2011 i prováděcí vyhláškou Ministerstva informatiky č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání. Ta byla zrušena nálezem Ústavního soudu sp. zn. Pl. ÚS 24/10 vydaným 22. března 2011.

Dne 15. března 2006 byla za účelem harmonizace předpisů členských států přijata Směrnice Evropského parlamentu a Rady 2006/24/ES o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES (dále jen „směrnice o data retention“ či „směrnice o uchovávání údajů“). Pro větší flexibilitu ve vztahu ke specifikům jednotlivých právních řádů členských států byla zvolena právě forma směrnice.⁹ Cílem harmonizace právních předpisů jednotlivých

⁵ Např. nálezy Ústavního soudu pod sp. zn. II. ÚS 502/2000 ze dne 22. 1. 2001; sp. zn. IV. ÚS 536/2000 ze dne 13. 2. 2001 a sp. zn. IV. ÚS 78/2001 ze dne 27. 8. 2001.

⁶ K tomu blíže: nálezy Ústavního soudu sp. zn. II. ÚS 502/2000 ze dne 22. 1. 2001.

⁷ *Malone* proti Spojenému království, rozsudek ESLP (plenary session) ze dne 2. 8. 1984, stížnost č. 8691/79 (srov. *Klass* a další proti Německu, rozsudek ESLP (plenary session) ze dne 6. září 1978, stížnost č. 5029/71; *Kruslin* proti Francii, rozsudek ESLP (Chamber) ze dne 24. dubna 1990, stížnost č. 11801/85; *Kopp* proti Švýcarsku, rozsudek ESLP (Chamber) ze dne 25. března 1998, stížnost č. 23224/94; *Amann* proti Švýcarsku, rozsudek ESLP (Grand Chamber) ze dne 16. února 2000, stížnost č. 27798/95).

⁸ Nálezy Ústavního soudu sp. zn. IV. ÚS 536/2000 ze dne 13. 2. 2001; stejně nálezy Ústavního soudu sp. zn. IV. ÚS 78/2001 ze dne 27. 8. 2001.

⁹ REDING, V. The European data protection framework for the twenty-first century. *International Data Privacy Law*, 2012, roč. 2, č. 3, s. 120–121.

členských států bylo zajistit dostupnost provozních a lokalizačních údajů pro účely odhalování, vyšetřování a stíhání závažných trestných činů. Implementace směrnice do právních řádů měla být provedena do 15. září 2007, s výjimkou pro uchovávání údajů o internetové komunikaci. V tomto případě byl umožněn odklad do 15. března 2009. Česká republika svou povinnost splnila 1. září 2008, kdy zákon č. 247/2008 Sb. nabyl účinnosti. Některé státy,¹⁰ a šlo především o ty, kde byla směrnice přezkoumávána tamními Ústavními soudy, však směrnici nestihly transponovat ani v prodloužené lhůtě. Její následné promítnutí do vnitrostátní úpravy pak bylo spíše projevem obavy z vysokých pokut ze strany EU.

Povinnost uchovávat technická data a na požádání je poskytnout oprávněným orgánům, však český zákonodárce poskytovatelům veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí ukládal již dříve. Bylo ale třeba implementovat některé články směrnice o data retention, k jejichž promítnutí do vnitrostátní úpravy dosud nedošlo. Jednalo se především o nově uloženou povinnost uchovávat provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány a uchovávány nebo zaznamenávány při neúspěšném pokusu o volání, což zvýšilo finanční a administrativní zátěž povinných subjektů.

Ke zpřesnění právní úpravy došlo v tom, že vyžádané údaje musí být oprávněným orgánům poskytnuty bezodkladně.¹¹ Dále byla uložena povinnost zajistit ochranu uchovávaných údajů, jejich likvidaci po uplynutí stanovené doby a evidenci případů, kdy byly údaje oprávněnými orgány vyžádány.

V původním znění odstavce 3 § 97 zákona č. 127/2005 Sb. před provedenou novelizací doba uchovávání dat nesměla být delší než 12 měsíců, v tomto směru došlo ke zpřesnění právní úpravy tak, že doba uchovávání technických dat nesmí být kratší než 6 měsíců a delší než 12 měsíců. Směrnice přitom umožňuje, aby členské státy na základě svého uvážení lhůtu k uchovávání provozních a lokalizačních údajů stanovily až na 24 měsíců, nejméně však vždy po dobu 6 měsíců. V průběhu tvorby směrnice některé státy dokonce navrhovaly lhůtu mnohem delší, v řádu několika let. Česká republika naopak zastávala stanovisko opačné, neboť byly vzneseny pochybnosti o přínosnosti starších dat. Delší lhůta navíc zvyšuje administrativní zátěž operátorů a tím i náklady, které nese stát.¹² V pozměňovacích návrzích zákona č. 247/2008 Sb., kterým se novelizuje zákon č. 127/2005 o elektronických komunikacích, bylo původně navrhováno, aby lhůta pro uchovávání provozních a lokalizačních údajů činila nejvýše 6 měsíců.¹³ Nakonec bylo zvoleno, jak víme, kompromisní řešení zahrnující časové

¹⁰ Mezi státy, které nestihly diskutovanou směrnici transponovat v určené lhůtě, patří např. Rumunsko či Švédsko.

¹¹ Důvodová zpráva k zákonu č. 247/2008 Sb., sněmovní tisk 398/0, Novela zákona o elektronických komunikacích – EU – RJ; Poslanecká sněmovna, 2008, 5. volební období 2006–2010. Dostupná z: <http://www.psp.cz/sqw/text/tiskt.sqw?o=5&ct=398&ct1=0#prilohy>.

¹² Důvodová zpráva k návrhu zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), a některé další zákony, 2012, s. 14. Dostupná z: http://eklep.vlada.cz/eklep/getAttachment?id=zd_rack8rveqpl.doc. Souladně: MARAS, M.-H. The economic costs and consequences of mass communications data retention: Is the data retention directive a proportionate measure? *European Journal of Law and Economics*, 2012, roč. 33, č. 2, s. 447–472.

¹³ Sněmovní tisk 398/4, Pozměňovací a jiné návrhy k tisku 398/0. Poslanecká sněmovna, 2008, 5. volební období 2006–2010. Dostupný z: <http://www.psp.cz/sqw/text/tiskt.sqw?o=5&ct=398&ct1=4>.

rozmezí 6 až 12 měsíců. Vedle České republiky jsou to další tři členské státy Evropské unie, které stanovily dobu uchovávání telekomunikačních dat na nejnižší hranici, a těmi jsou Kypr, Lucembursko a Litva. Naopak nejdéle uchovávají tyto citlivé údaje v Polsku (2 roky). Jiné státy rozlišují, zda se jedná o telekomunikační údaje z mobilní/pevné sítě nebo z internetu a shodně pak pro prvně jmenovanou kategorii stanovují obecně lhůtu delší.

Po uplynutí dané lhůty musí dojít k likvidaci shromážděných dat, pokud nebyly poskytnuty oprávněným orgánům dle zvláštního předpisu nebo nejsou používány poskytovatelem telekomunikačních služeb pro vlastní potřebu. Způsob likvidace však neupravuje ani prováděcí předpis. Zákodárce providerům ukládá povinnost zničit údaje, pokud ovšem nejsou poskytnuty oprávněným orgánům. Avšak jaká je nejvyšší přípustná doba, po kterou mohou být uchovávány, v případě, že poskytnuty oprávněným orgánům jsou? Na tuto otázku odpověď dána není. Řešením by mohlo být stanovení konkrétní lhůty od vyžádání, případně údaje smazat poté, co budou poskytnuta orgánu, který si je vyžádal, nejdříve však po uplynutí šestiměsíční lhůty.

2. VYŠETŘOVACÍ NÁSTROJ V RUKOU OPRÁVNĚNÝCH ORGÁNŮ

Vylákání finanční hotovosti za účelem poskytnutí půjčky a její následné nevrácení, zjištění místa posledního pobytu zavražděného, určení pohybu mobilního telefonu podezřelé osoby, odhalení pachatelů loupežného přepadení i sériových krádeží vloupáním do motorových vozidel,¹⁴ šíření dětské pornografie, rozpletení případu organizovaného obchodu s drogami a další trestná činnost¹⁵ – to je ilustrativní výčet situací, ve kterých bylo využito informací získaných podle § 88a TŘ, jež významným způsobem přispěly k objasnění trestné činnosti. Provozní a lokalizační údaje bývají často prvotní informací, kterou policisté při vyšetřování trestného činu mají a která je rozhodující pro určení dalšího postupu policejního orgánu. Policejní orgány jsou tak při vyšetřování odkázány především na spolupráci se soukromými subjekty, tzv. providery.

Získání provozních údajů může být klíčem k odhalení pachatele trestného činu nebo alespoň místa posledního připojení k síti. Díky komunikaci pachatele s okolím je možno vystopovat IP adresu jeho PC a následně lokalizovat místo připojení k síti internet. To bude mít význam především tehdy, pokud půjde o nepřenositelné zařízení. Avšak vypátrání místa připojení neznamená zároveň i najít pachatele. Identifikace pachatele jako klíčový úkol v boji proti kyberkriminalitě je velice obtížná. Důležitým pomocníkem pro vyšetřovací orgány je tzv. IP adresa.¹⁶ Každé zařízení připojené k síti obdrží od poskytovatele internetu IP adresu. Bez ní se k internetu připojit nelze. Práci policejnímu orgánu ulehčí

¹⁴ Důvodová zpráva k návrhu zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), a některé další zákony, 22. 2. 2012, s. 4, 5. Dostupná z: eklep.vlada.cz/eklep/getAttachment?id=zd_rack8rveqlpl.doc.

¹⁵ Provozní a lokalizační údaje jsou využívány nejen při vyšetřování majetkové trestné činnosti či kriminality počítačové, ale i násilné trestné činnosti (vraždy, loupež, znásilnění...) či obchodování s lidmi, šíření pornografie, kuplířství, obchodování s drogami atd.

¹⁶ Značka IP je zkratkou pro Internet Protocol.

tzv. statická IP adresa, neboť v takovém případě pod touto unikátní adresou vystupuje pouze jediný počítač, což umožní stálou identifikaci majitele zařízení. Proto je pachateli dáвана přednost tzv. dynamické IP adrese. Při každém dalším připojení počítače k internetu dojde ke změně IP adresy. IP adresa či její část se může měnit v závislosti na tom, v jakém pořadí se uživatel do sítě přihlásí. Nicméně policejní orgán alespoň obdrží informaci o tom, odkud se pachatel k síti připojil. Existují však i způsoby, jak svou IP adresu skrýt.¹⁷

V souvislosti s vyšetřováním kyberkriminality vyvstává několik problémů, se kterými se musí orgány činné v trestním řízení potýkat. Jde nejen o obtíže s identifikací pachatele, ale i nestálost elektronických dat či posouzení rozsahu a dopadu trestné činnosti. Orgány činné v trestním řízení se musí vyrovnávat s nehmotnou povahou důkazních prostředků. Navíc je třeba pracovat rychle, neboť je nutné zachytit důkazy dříve, než jsou smazány, změněny či přepsány jinými informacemi. Některé provozní údaje nejsou trvale uchovávány a v paměti počítačového systému zůstanou jen po krátkou dobu.¹⁸ Zničení důkazů tak může být otázka i několika vteřin – ať již jde o úmyslné odstranění dat, jejich ztrátu neopatrnou manipulací či rutinní smazání údajů, které již nemusí být uchovávány. Často se stává, že na přenosu sdělení se podílí více providerů, to ale také znamená, že klíčové provozní či lokalizační údaje týkající se dané činnosti jsou rozptýleny mezi více poskytovatelů služeb, kdy „každý má jen část skládačky“.¹⁹ Tyto dílky je nutné složit, aby bylo možné vysledovat zdroj nebo naopak místa určení. V kyberprostoru jsou denně zaznamenávány, shromažďovány a případně i dále zpřístupňovány miliony dat zasahující do soukromí jednotlivce.

3. EFEKTIVNÍ VYŠETŘOVACÍ NÁSTROJ VERSUS PRÁVO NA SOUKROMÍ

V posledních dvou letech byly vydány dva klíčové nálezy Ústavního soudu, a to nález Pl. ÚS 24/10 ze dne 22. března 2011, publikovaný ve Sbírce zákonů pod č. 94/2011 Sb. a dále nález Pl. ÚS 24/11²⁰ (č. 43/2012 Sb.), který navazuje na právní závěry obsažené v nálezu předešlém. V prvním ze dvou výše zmiňovaných nálezu se předmětem přezkumu z hlediska souladu s ústavním pořádkem stal § 97 odst. 3 a 4 zákona č. 127/2005 Sb. o elektronických komunikacích a prováděcí vyhláška k tomuto zákonu č. 485/2005 Sb.²¹ Bylo třeba vypořádat se s otázkou, zda plošné shromažďování a využívání provozních a lokalizačních údajů o telekomunikačním provozu v rozsahu vymezeném napadenými právními předpisy je vzhledem k užítku z těchto informací

¹⁷ Pro další informace týkající se změny či skrytí IP adresy odkazují např. na: <http://czblog.cz/co-je-to-ip-adresa-jak-zmenit-ip-adresu/>.

¹⁸ Council of Europe. *Convention on cybercrime*. Budapest, 23. 11. 2001. Explanatory report. Dostupné z: <http://conventions.coe.int/treaty/en/reports/html/185.htm>.

¹⁹ Council of Europe. *Convention on cybercrime*. Budapest, 23. 11. 2001. Explanatory report, bod 167. Dostupné z: <http://conventions.coe.int/treaty/en/reports/html/185.htm>.

²⁰ Autorka si dovoluje upozornit, že se v některých případech můžeme setkat s nesprávným číselným označením nálezu Ústavního soudu, kdy je na místo sp. zn. Pl. ÚS 24/11 označován sp. zn. Pl. ÚS 42/2011.

²¹ Vyhláška č. 485/2005 Sb. o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání.

plynoucímú proporcionálným zásahem do základných práv a svobod zaručených v Listině základných práv a svobod a Úmluvě o ochraně lidských práv a svobod.

Jde jen o důslednou ochranu našich základních práv a svobod, nebo si orgány činné v trestním řízení oprávněně stěžují, že jim Ústavní soud bere jeden z nejúčinnějších prostředků v boji s kriminalitou? Na to nelze dát jednoznačnou odpověď.

Podle napadeného ustanovení § 97 odst. 3 a 4 zákona č. 127/2005 Sb. měly fyzické a právnické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací povinnost uchovávat provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování jejich veřejných komunikačních sítí a při poskytování jejich veřejně dostupných služeb elektronických komunikací. Zjednodušeně řečeno se tato povinnost týkala především mobilních operátorů a poskytovatelů internetového připojení, kterým zákon takto ukládal povinnost po dobu šesti až dvanácti měsíců uchovávat telekomunikační data, např. telefonní číslo volajícího a volaného, datum a čas zahájení komunikace i její délku, geografické souřadnice veřejných telefonních automatů a další údaje o telefonní, faxové či SMS komunikaci. V případě internetového spojení jde o datum a čas zahájení a ukončení připojení, IP adresu či adresu elektronické pošty odesílatele stejně jako příjemců, množství přenesených dat, informace o navštívených webových stránkách apod. Ústředním problémem jsou citlivé informace, které nám tyto digitální stopy o jednotlivých osobách prozrazují – jejich zájmy, politickou příslušnost, aktuální zdravotní stav či dokonce sexuální orientaci. Lokalizační údaje Vašeho mobilního telefonu nám zase poskytnou informace o tom kdy, kde a s kým jste se setkali. Dostaneme tak „komunikační a pohybový profil jednotlivce, z kterého lze získat nejen údaje o jeho minulých aktivitách, ale s vysokou mírou pravděpodobnosti i správně předvídat jeho aktivity v budoucnosti“.²² To vše představuje významný zásah do ústavně zaručeného práva na ochranu soukromí.

Sama směrnice o data retention již od svého počátku čelí kritice i ze strany jiných členských států. K přezkumu transpozičních právních předpisů z hlediska jejich ústavnosti došlo i v Rumunsku, Německu a na Kypru. Kontrola transponujících právních předpisů stále probíhá v Polsku. Tamní ústavní soudy shledaly právní předpisy zakotvující *preventivní uchovávání dat protiústavními pro zásah do práva na soukromí. Shodně bylo právní úpravě vytýkáno porušení zásady proporcionality, nedostatečné vymezení účelu uchovávání dat, vágní regulace práv a povinností, nedostatečné záruky proti zneužití či absence soudní kontroly apod.*²³ Právní problémy spojené s transpozicí směrnice řešilo i Bulharsko, Rakousko, Irsko²⁴ či Švédsko. The High Court of Ireland se v červenci roku 2012 obrátil na Evropský soudní dvůr a požádal jej o zodpovězení předběžné otázky, zda je směrnice 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně do-

²² Nález pléna Ústavního soudu sp. zn. Pl. ÚS 24/10 ze dne 22. 3. 2011, bod 7. Publikovaný ve Sbírce zákonů jako předpis č. 94/2011 Sb. In: *Sbírka zákonů*, 2011, částka 35, s. 931–951. Dostupný z: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5908>.

²³ K tomu blíže: MARKOU, Ch. The Cyprus and other EU court rulings on data retention: The Directive as a privacy bomb. *Computer Law and Security Review*, 2012, roč. 28, č. 4, s. 468–475.

²⁴ K vývoji irské právní úpravy ukládání telekomunikačních dat a problémů s tím spojených odkazují na: MCINTYRE, T. J. Data retention in Ireland: Privacy, policy and proportionality. *Computer Law and Security Review*, 2008, roč. 24, č. 4, s. 326–334.

stupných služeb elektronických komunikací služeb nebo veřejných komunikačních sítí v souladu s právem Evropských společenství.²⁵

I přes vyjmenované nedostatky trvá Evropská komise na transpozici dotčené směrnice k zajištění plného souladu s pravidly EU. Ve většině zemí nakonec k provedení směrnice došlo. Například rumunskému parlamentu byl předložen nový návrh zákona transponujícího směrnici o data retention. Tento návrh byl v prosinci roku 2011 nejdříve projednán senátem,²⁶ který jednomyslně rozhodl o jeho zamítnutí. Dolní komorou rumunského parlamentu byl však zákon přijat. Za přijetím zákona se pravděpodobně skrývá obava z vysokých sankcí ze strany EU v případě neprovedení směrnice.²⁷ Vedle Rumunska došlo k přijetí transponujícího právního předpisu také ve Švédsku. Poté, co Evropská komise proti Švédsku vznesla stížnost u ESD a hrozilo uložení vysoké pokuty, transponující předpis byl tamním parlamentem v březnu 2012 přijat.²⁸ Evropská komise uvažuje, že podá u Evropského soudního dvora žalobu za nesplnění povinnosti v podobě promítnutí směrnice do národního právního řádu i proti Německu.²⁹ Německo sice původně zákon transponující směrnici o data retention v listopadu 2007 zavedlo, nicméně měsíc poté byla proti tomuto právnímu předpisu vznesena ústavní stížnost, které německý Ústavní soud 2. března 2010 vyhověl a předpis zrušil. Německý ústavní soud byl doslova zaplaven vlnou individuálních stížností proti implementaci směrnice 2006/24/EC do vnitrostátní úpravy. Uvádí se, že ústavní stížnost podalo 34 000 jednotlivců.³⁰

Po vydání nálezu Pl. ÚS 24/10 byl Ústavnímu soudu dne 27. května 2011 doručen návrh Obvodního soudu pro Prahu 6 na zrušení § 88a TŘ. Ústavní soud rozhodl o zrušení předmětného ustanovení trestního řádu k 30. září 2012. Ministerstvo vnitra ve spolupráci s Ministerstvem spravedlnosti a Ministerstvem průmyslu a obchodu začalo připravovat novelu trestního řádu ještě před derogací § 88a TŘ nálezem ÚS vydaného pod č. 43/2012 Sb. Zákodárce měl upravit tento právní nástroj tak, aby splnil test proporcionality³¹ a požadavek předvídatelnosti, jak to vyžaduje Ústavní soud pro zachování ústavní konformity. Zejména jedná-li se o automatické zpracování údajů patřících pod ochranu článků 10 odst. 3 a 13 Listiny i článku 8 Evropské úmluvy o ochraně lidských práv a svobod. „Právo na soukromí taktéž garantuje právo jednotliv-

²⁵ Do data uzavření rukopisu nebyla předběžná otázka Evropským soudním dvorem zodpovězena.

²⁶ Návrh zákona je v Rumunsku vždy nejdříve projednán horní komorou Parlamentu a až následně je předložen dolní komoře.

²⁷ Romanian Parliament Adopts The Data Retention Law. Again. *Digital Civil Right*. Květen 2012. Dostupné z: <http://www.edri.org/edriagram/number10.10/romanian-parliament-adopts-data-retention-law-again>.

²⁸ Swedish parliament passes controversial data storage bill. *EUbusiness*. Březen 2012. Dostupné z: <http://www.eubusiness.com/news-eu/sweden-telecom.frt>.

²⁹ Commission still seeking proof of the necessity of mandatory data retention. *Statewatch organization*. Leden 2012. Dostupné z: <http://www.statewatch.org/news/2012/jan/09eu-pnr.htm>.

³⁰ HORNUNG, G., SCHNABEL, Ch. Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention. *Computer Law and Security Review*, 2009, roč. 25, č. 2, s. 115–122.

³¹ Nález pléna Ústavního soudu sp. zn. Pl. ÚS 24/10 ze dne 22. 3. 2011, bod 37. Publikovaný ve Sbírce zákonů jako předpis č. 94/2011. In: *Sbírka zákonů*. 2011, částka 35, s. 931–951. Dostupný z: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5908>. Test proporcionality zahrnuje tři kritéria. Zda je daný prostředek schopen dosáhnout zamýšleného cíle, zda se jedná o prostředek k základnímu právu nejšetnější a v neposlední řadě je třeba zkoumat přiměřenost v užším smyslu. Tedy zda pozitivní, která z toho zásahu plynou, převáží negativní důsledky spojené se zásahem do základních lidských práv.

*ce sám rozhodnout, zda a v jakém rozsahu, jak a za jakých okolností mají být informace z jeho soukromí zpřístupněny jiným subjektům.*³²

Zároveň byly začátkem ledna 2012 zahájeny práce na přípravě nového prováděcího předpisu na místo zrušené vyhlášky č. 485/2005 Sb. Prováděcí předpis blíže upravuje nejen rozsah a formu uchovávaných provozních a lokalizačních údajů, způsob jejich předávání oprávněným orgánům, ale i způsob likvidace těchto citlivých dat,³³ což v minulé prováděcí vyhlášce chybělo.

4. CO PŘINESLA NOVELIZOVANÁ ÚPRAVA

Obecně se zpřísňují podmínky pro získání příkazu k zjištění provozních a lokalizačních údajů. Zákonodárce tak reaguje na výtky Ústavního soudu, který shledal § 88a TŘ ústavně nekonformním z důvodu neomezeného okruhu trestných činů, k jejichž objasnění lze tento vyšetřovací nástroj použít, neexistence principu subsidiarity a selhání tohoto institutu v testu proporcionality ve vztahu k zásahu do práva na informační sebeurčení, obsaženém v čl. 10 odst. 3 a čl. 13 Listiny. Pro futuro bylo nezbytné jednoznačně vymezit okruh oprávněných orgánů, zamyslet se nad délkou uchovávání provozních a lokalizačních údajů, zpřísnit pravidla pro jejich uchovávání i následnou likvidaci, zakotvit povinnost zpětně informovat uživatele o nařízeném zjišťování údajů o telekomunikačním provozu a současně možnost obrátit se na příslušný soud s žádostí o přezkum, zda nedošlo v daném případě ke zneužití tohoto institutu.

Směrnice o data retention pracuje s pojmem „závažné trestné činy“, aniž by jej definovala. Toto vymezení se neshoduje s žádnou kategorií trestných činů v § 14 odst. 3 trestního zákoníku. Zůstalo tak na zákonodárci, aby sám vymezil, co pokládá za tzv. závažný trestný čin. Ústavní soud zákonodárci vytkl, že tak v původním znění ustanovení § 88a TŘ činil příliš vágně. Ústavní soud se navíc vyslovil, že je nezbytné, aby možnost použití uchovávaných údajů byla omezena jen pro účely trestních řízení vedených pro zvlášť závažné trestné činy.³⁴ Opřel se zde o úpravu v § 88 TŘ a Směrnici o data retention. Avšak jak vyplývá z výše uvedeného, Směrnice o uchovávání údajů v tomhle směru tak striktní není a členským státům neukládá, aby použitelnost tohoto institutu omezily jen na vedení trestního stíhání pro zvlášť závažné zločiny.

V novém znění § 88a TŘ již získání příkazu k zjištění údajů o telekomunikačním provozu nestačí odůvodnit potřebností objasnit „skutečnosti důležité pro trestní řízení“. Toto vágní vymezení bylo na místo toho nahrazeno třemi skupinami trestných

³² Nález pléna Ústavního soudu sp. zn. Pl. ÚS 24/10 ze dne 22. 3. 2011. Publikovaný ve Sbírce zákonů jako předpis č. 94/2011. In: *Sbírka zákonů*. 2011, částka 35, s. 931–951. Dostupný z: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5908>.

³³ Důvodová zpráva k návrhu zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), a některé další zákony, 22. 2. 2012, s. 27, 33. Dostupná z: eklep.vlada.cz/eklep/getAttachment?id=zd_rack8rveqlpl.doc.

³⁴ Nález pléna Ústavního soudu sp. zn. Pl. ÚS 24/10 ze dne 22. 3. 2011, bod 47, 48. Publikovaný ve Sbírce zákonů jako předpis č. 94/2011. In: *Sbírka zákonů*. 2011, částka 35, s. 931–951. Dostupný z: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5908>.

činů, k jejichž objasnění budou moci orgány činné v trestním řízení provozní a lokalizační údaje získat.

První skupinu tvoří úmyslné trestné činy, na které zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně tři roky. Jak již bylo řečeno výše, dotčená směrnice sama pojem „závažné trestné činy“ nevymezuje a zůstalo tak na členských státech, aby tento pojem samy vymezily ve vztahu k svým trestněprávním předpisům. Důvodová zpráva uvádí, že horní hranice trestní sazby byla odvozena analogicky od institutu vazby jako nejintenzivnějšího prostředku trestního práva vedoucího k zbavení osobní svobody obviněného.³⁵ Ve srovnání s ostatními členskými státy tak tato hranice byla stanovena zhruba uprostřed. Stejně učinilo i Estonsko. V Irsku naopak je vedle taxativně vymezených trestných činů možné tyto údaje získat až pro trestné činy, na něž trestní zákon stanovuje trest odnětí svobody nejméně 5 let. V jiných členských státech je hranice horní hranice trestní sazby stanovena naopak níže (Maďarsko 2 roky; Lucembursko 1 rok) nebo dokonce takové omezení neexistuje a provozní a lokalizační údaje je možné žádat ve vztahu ke všem trestným činům, jakož i k prevenci trestné činnosti a obecně národní a veřejné bezpečnosti, bezpečnosti státu (Belgie, Dánsko, Francie, Itálie, Lotyšsko, Polsko, Slovensko, Slovinsko).³⁶

Druhá skupina je stanovena taxativním výčtem jednotlivých trestných činů, jejichž objasnění by bez provozních a lokalizačních údajů bylo značně ztíženo. Pro ně výše uvedená omezení neplatí. V těchto případech pachatel často využívá ke spáchání trestné činnosti prostředků elektronické komunikace.³⁷ Jde o například o trestný čin podvodu dle § 209 TZ, porušení tajemství dopravovaných zpráv (§ 182 TZ), nebezpečné vyhrožování (§ 353 TZ), nebezpečné pronásledování (§ 354 TZ) a další trestné činy postihující počítačovou kriminalitu; trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací (§ 230 TZ), pro trestný čin opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 TZ).

Úmyslné trestné činy, k jejichž stíhání zavazuje vyhlášená mezinárodní smlouva, kterou je Česká republika vázána, jsou třetí a poslední skupinou trestných činů, u které lze vyžádat údaje o telekomunikačním provozu, jež jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat.

Příkaz k zjištění údajů o telekomunikačním provozu může být vydán jen tehdy, pokud není možné trestný čin objasnit prostřednictvím jiných důkazních prostředků. Sledovaného účelu tedy nelze dosáhnout jinak nebo by jeho dosažení bylo podstatně ztíženo. Nová úprava po vzoru § 88 TŘ zavádí princip subsidiarity.³⁸ Byť Ústavní soud netvrdí, že by znění § 88a TŘ mělo být totožné s úpravou odposlechnů, v mnohém se jí

³⁵ Důvodová zpráva k návrhu zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), a některé další zákony, 22. únor 2012, s. 27. Dostupná z: <http://eklep.vlada.cz/eklep/getAttachment?id=zdrack8rveqlpl.doc>.

³⁶ Evropská komise. Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES) z 18. dubna 2011, Brusel. Dostupná z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:CS:PDF>.

³⁷ Důvodová zpráva k návrhu zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), a některé další zákony, 22. únor 2012, s. 20. Dostupná z: eklep.vlada.cz/eklep/getAttachment?id=zdrack8rveqlpl.doc.

³⁸ Srov. § 88 trestního řádu, zákon č. 141/1961 Sb., o trestním řízení soudním.

bliží. Vedle zásady subsidiarity a proporcionality byla zakotvena povinnost předsedy senátu v řízení před soudem, případně státního zástupce či policejního orgánu, byla-li věc pravomocně skončena jejich rozhodnutím, zpětně informovat uživatele o nařízeném zjišťování údajů o telekomunikačním provozu.³⁹ Z tohoto důvodu bylo třeba upravit i související ustanovení trestního řádu upravující řízení o přezkumu. Nepředpokládá se však, že by tento nový přezkumný prostředek představoval výrazné zatížení pro příslušný soud, neboť počet žádostí o přezkum u odposlechů stěží překročí 10 případů ročně.⁴⁰

Vydat příkaz ke zjištění údajů o uskutečněném telekomunikačním provozu byl před novelizací oprávněn předseda senátu a v přípravném řízení soudce. Zpravidla se tak dělalo na návrh státního zástupce, byť tento postup § 88a TŘ výslovně neuváděl. Postupovalo se analogicky dle ustanovení § 88 odst. 2 TŘ. Nebylo však vyloučeno, aby v případech, které nesnesly odkladu, podal návrh na vydání příkazu i policejní orgán.⁴¹ Novým zněním ustanovení § 88a TŘ došlo k zakotvení povinnosti v přípravném řízení předkládat žádost o vydání příkazu ke zjištění údajů o uskutečněném telekomunikačním provozu pouze prostřednictvím státního zástupce. Zákonodárce si od toho slibuje větší uvážení při podávání návrhu na vydání příkazu. I ostatní členské státy Evropské unie podmiňují získání příkazu k zjištění provozních a lokalizačních údajů zpravidla souhlasem soudce. Ovšem není tomu tak ve všech případech. Některé z členských států stanovují podmínky přísnější, např. souhlas předsedy senátu krajského soudu,⁴² jiné naopak svěřují tuto pravomoc i do rukou jiného orgánu než soudu.⁴³

Z příkazu musí vyplývat, jaký druh údajů, za jaké období a za jakým účelem se vyžaduje, kterému orgánu v trestním řízení a v jaké podobě (listinné či elektronické) se poskytují. Dále se uvádí známé údaje o účastníkovi telekomunikace, ohledně něhož se dané skutečnosti sdělují.⁴⁴ Nově právní úprava kromě písemného odůvodnění také vyžaduje, aby bylo odkazováno na konkrétní mezinárodní smlouvu, která zavazuje ke stíhání daného trestného činu a dále se ukládá povinnost uvést totožnost uživatele, je-li známa.⁴⁵ V tomto směru opět napodobuje ustanovení § 88 TŘ.

³⁹ Podle důvodové zprávy bude uživateli sděleno, který soud příkaz vydal, jaká data byla poskytnuta a doba, za kterou byly provozní a lokalizační údaje vyžádány. Zároveň musí být uživatel poučen o možnosti podat návrh na přezkoumání zákonnosti příkazu, které provede Nejvyšší soud. Viz Důvodová zpráva k návrhu zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), a některé další zákony, 22. únor 2012, s. 21. Dostupná z: eklep.vlada.cz/eklep/getAttachment?id=zdrack8rveqpl.doc.

⁴⁰ Důvodová zpráva k návrhu zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), a některé další zákony, 22. únor 2012, s. 32. Dostupná z: eklep.vlada.cz/eklep/getAttachment?id=zdrack8rveqpl.doc.

⁴¹ ŠAMAL, P. et al. *Trestní řád. Komentář*. 1. díl. 6. vydání. C. H. Beck, Praha, 2008, s. 747.

⁴² Souhlas předsedy senátu krajského soudu je vyžadován v Bulharsku. Viz Evropská komise. Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES) z 18. dubna 2011, Brusel. Tabulka č. 2, s. 10. Dostupná z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:CS:PDF>.

⁴³ V Belgii, Itálii či Nizozemsku může vydání příkazu k zjištění provozních a lokalizačních údajů povolit i státní zástupce. Viz Evropská komise. Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES) z 18. dubna 2011, Brusel. Tabulka č. 2, s. 10. Dostupná z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:CS:PDF>.

⁴⁴ ŠAMAL, P. et al. *Trestní řád. Komentář*. 1. díl. 6. vydání. C. H. Beck, Praha, 2008, s. 748.

⁴⁵ Důvodová zpráva k návrhu zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), a některé další zákony, 22. únor 2012, s. 28. Dostupná z: <http://eklep.vlada.cz/eklep/getAttachment?id=zdrack8rveqpl.doc>.

5. K NADUŽÍVÁNÍ § 88a TRESTNÍHO ŘÁDU

V odůvodnění nálezu Ústavního soudu Pl. ÚS 24/10 bylo negativně hodnoceno nadužívání tohoto nástroje orgány činnými v trestním řízení i k vyšetřování bagatelní trestné činnosti. Uvádí, že dle Zprávy o bezpečnostní situaci v ČR za rok 2008 bylo na území České republiky zjištěno celkem 343 799 trestných činů, z toho bylo objasněno 127 906 trestných činů. Počet žádostí o poskytnutí provozních a lokalizačních údajů činil ve stejném roce dle statistických údajů 131 560.⁴⁶ Statistika říká, že v Evropské unii je každoročně vzneseno více než 2 miliony takových žádostí. Počet vznesených žádostí tak ve vztahu k objasněným trestným činům je obrovský a vede k domněnce o nadužívání tohoto institutu i pro vyšetřování méně závažné trestné činnosti. Policejní statistiky se však od těch Českého telekomunikačního úřadu značně liší.⁴⁷ A to proto, že v České republice je třeba žádost o poskytnutí údajů o telefonní komunikaci v mobilní síti předložit všem významným mobilním operátorům, tedy minimálně třem.⁴⁸ Stejná žádost je pak ve statistice poskytovatelů telekomunikačních služeb evidována hned třikrát, zatímco ve statistikách policie se objeví jen jednou. Z tohoto důvodu jsou uváděná čísla zkreslena.

Ze statistických dat⁴⁹ vyplývá, že orgány činné v trestním řízení nejčastěji vyžadují data, která nejsou starší víc než 3 měsíce. Jedná se o více jak 80 % z celkového počtu žádostí. Stejně závěry vykazují i jiné státy.⁵⁰ Data starší více jak 9 měsíců jsou vyžadována pouze sporadicky a údaje, od jejichž záznamu uběhlo víc než 12 měsíců, nejsou vyžadovány vůbec. To je však dáno tím, že legislativa umožňovala a zároveň nařizovala provozní a lokalizační údaje uchovávat nejméně po dobu 6 měsíců, nejvýše však po dobu 12 měsíců. Následně musí být tyto údaje zničeny. Nejvíce orgány činné v trestním řízení zajímají technické údaje o telekomunikaci v mobilní síti,⁵¹ počet těchto žádostí několikanásobně převyšuje oblast pevné sítě i internetového prostoru. Jak již bylo zmíněno výše, je třeba vzít v úvahu, že počet případů, ke kterým byly dané údaje vyžádány,

⁴⁶ Nález pléna Ústavního soudu sp. zn. Pl. ÚS 24/10 ze dne 22. 3. 2011, bod 49. Publikovaný ve Sbírce zákonů jako předpis č. 94/2011. In: Sbírka zákonů. 2011, částka 35, s. 931–951. Dostupný z: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5908>. Souladně: Evropská komise. Hodnoticí zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES) z 18. dubna 2011, Brusel, s. 35–43. Dostupná z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:CS:PDF>.

⁴⁷ Z důvodové zprávy k návrhu zákona, kterým se mění zákon č. 127/2005 Sb. a zákon č. 141/1961 Sb.: „Podle údajů Policie České republiky byl v roce 2010, tedy před zrušením příslušných ustanovení Ústavním soudem, celkový počet úkonů podle § 88a trestního řádu 82 639. Celkový počet spisů, k nimž byly úkony podle § 88a trestního řádu provedeny, je pak 10972.“

⁴⁸ Evropská komise. Hodnoticí zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES) z 18. dubna 2011, Brusel. Dostupná z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:CS:HTML>. Souladně: Důvodová zpráva k návrhu zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), a některé další zákony, 22. únor 2012, s. 30. Dostupná z: [eklep/vlada.cz/eklep/getAttachment?id=zdrack8rveqplp.doc](http://eklep.vlada.cz/eklep/getAttachment?id=zdrack8rveqplp.doc).

⁴⁹ Evropská komise. Hodnoticí zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES) z 18. dubna 2011, Brusel, tabulky č. 7 a 8 na s. 34, 35. Dostupná z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:CS:HTML>.

⁵⁰ *Liberty and security: Striking the balance*. UK Presidency Paper, 2005, s. 1–5. Dostupné z: <http://www.edri.org/docs/UKPresidencypaper.pdf>.

⁵¹ Za rok 2008 se jednalo v České republice o 125 040 žádostí o poskytnutí technických dat v mobilní síti, v pevné síti byl tento počet 4983 žádostí a na zjištění lokalizačních a provozních údajů v rámci internetové komunikace bylo vydáno žádostí 1537.

je ve skutečnosti menší, neboť žádost o poskytnutí technických dat k jednomu případu může být současně podána hned k několika mobilním operátorům.⁵²

Komise v závěrečné části své Hodnoticí zprávy o směrnici o uchovávání údajů doporučuje harmonizovat dobu povinného uchovávání dat a její případné zkrácení. Je tak možné, že ke starším technickým údajům se vyšetřovatelé trestné činnosti nedostanou již vůbec. Přitom právě u organizované kriminality, složitějších finančních deliktů, kde samotné odhalení trestného činu trvá delší dobu, či u závažnější trestné činnosti obecně hraje dostupnost starších provozních a lokalizačních údajů velmi významnou roli. Mohou totiž zachycovat přípravnou fázi trestné činnosti, její plánování, rozdělení rolí mezi jednotlivé pachatele a jejich vzájemné vztahy. Kolik pachatelů se podaří na základě provozních a lokalizačních údajů odsoudit, však zjistit nelze.

Přesto se dá říci, že hodnota uchovávaných technických údajů je pro policejní orgány nesmírná. Kromě toho, že představují indicie cenné pro vyšetřování trestných činů, vykreslují vazby mezi podezřelými a jejich role. Zároveň jsou i usvědčujícími důkazy a jindy pomohou kontaktovat svědka činu či zbavit podezření ze spáchání trestného činu nevinného, aniž by bylo třeba použít jiné operativně pátrací prostředky. V některých případech jsou dokonce jedinou stopou. Například při objasňování vyhrůzek zasílaných prostřednictvím internetových diskuzních skupin jsou provozní údaje zásadním vodítkem.

Přímo se tedy nabízí otázka, zda omezení povinnosti poskytovat provozní a lokalizační údaje nepovede ke zhoršení postavení policejních orgánů v boji s kriminalitou?

Důvodová zpráva uvádí, že úkonů podle § 88a trestního řádu bylo nejčastěji využito při šetření trestné činnosti násilné (vražda, loupež, usmrcení z nedbalosti), mravnostní (znásilnění, šíření pornografie, kuplířství), hospodářské, majetkové (krádež, vloupání do bytů, krádež motorového vozidla) a u další trestné činnosti (obchodování s lidmi, počítačová kriminalita, toxikomanie).⁵³ Avšak u většiny z těchto úmyslných trestných činů můžeme o vydání provozních a lokalizačních údajů žádat i nadále, za podmínky, že sledovaného účelu nelze dosáhnout jinak nebo bylo-li by jeho dosažení podstatně ztíženo. Trestný čin vraždy (§ 140 TZ), znásilnění (§ 185 TZ), loupeže (§ 173 TZ), kuplířství (§ 189 TZ), obchodování s lidmi (§ 168 TZ), výroba a jiné nakládání s dětskou pornografií (§ 192 TZ) stejně jako drogové delikty (§ 283, 286, 287 TZ) jsou úmyslnými

⁵² Směrnice náhradu nákladů vznikajících v důsledku uložené povinnosti neupravuje, tuto otázku přenechává vnitrostátní úpravě. Postup a rozsah náhrady efektivně vynaložených nákladů upravuje vyhláška Českého telekomunikačního úřadu č. 486/2005 Sb. Poskytovatelé telekomunikačních služeb se mohou se svým nárokem obrátit na subjekt, který si úkon vyžádal nebo jej nařídil, zpravidla tedy Policii ČR, respektive Ministerstvo vnitra. Česká republika nahrazovala do zrušení § 97 odst. 3 a 4 nálezem Ústavního soudu jak provozní, tak kapitálové výdaje. Pro představu uvádím, že v roce 2009 Česká republika zaplatila za náhradu nákladů částku 6,8 mil. Eur. V roce 2010 Policie ČR vyčísila úhradu operátorům na více než 50 mil. Kč a v prvním čtvrtletí roku 2011 stihly náklady dosáhnout 17,4 mil. Kč. Novelizující právní úprava oproti předchozímu stavu nic nového nepřináší. Lze předpokládat, že vzhledem k omezení § 88a TR pouze na závažnější trestnou činnost budou výdaje za poskytování údajů o telekomunikačním provozu v příštích letech nižší.

Blíže k přímým a nepřímým nákladům spojeným s uchováváním údajů odkazují na publikaci: MARAS, M.-H. The economic costs and consequences of mass communications data retention: is the data retention directive a proportionate measure? *European Journal of Law and Econom*, 2012, roč. 33, č. 3; s. 447–472.

⁵³ Důvodová zpráva k návrhu zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), a některé další zákony, 22. únor 2012, s. 13. Dostupná z: eklep.vlada.cz/eklep/getAttachment?id=zd_rack8rveqpl.doc.

trestnými činy, na které trestní zákoník stanoví trest odnětí svobody s horní hranicí nejméně tři roky a patří tedy do tzv. 1. skupiny trestných činů, u kterých je pro účely trestního řízení možné telekomunikační data podle § 88a TŘ žádat. U počítačových trestných činů pod § 230 a 231 TZ je sice horní hranice trestní sazby nižší než požadované tři roky, avšak ty patří do taxativního výčtu trestných činů v § 88a TŘ. Drogové delikty přechovávání omamné a psychotropní látky a jedu (§ 284 TZ), nedovolené pěstování rostlin obsahujících omamnou nebo psychotropní látku (§ 285 TZ) či výroba a jiné nakládání s látkami s hormonálním účinkem (§ 288 TZ) nelze zařadit ani do první či druhé vymezené skupiny, avšak v tomto případě zavazují Českou republiku ke stíhání mezinárodní smlouvy,⁵⁴ a proto i zde je možné telekomunikační data získat. Z výše uvedeného výčtu úmyslných trestných činů, k nimž byly podle důvodové zprávy provozní a lokalizační údaje žádány nejčastěji, tak nově není možné získat záznam o proběhnuvší telefonické či internetové komunikaci zásadně pouze u trestného činu krádeže.

Byly proto porovnány policejní statistické údaje týkající se nápadu počtu trestných činů krádeže a krádeže vloupáním za účelem zjištění, zda a jaký vliv měla novela § 88a TŘ na objasněnost tohoto druhu kriminality. Právě u drobné majetkové kriminality byl z důvodu novelizace predikován výrazný pokles objasněnosti. Srovnání nápadu a objasněnosti těchto trestných činů bylo provedeno za období 1. 1. 2012 – 1. 8. 2012⁵⁵ a ve stejném období v roce 2010.⁵⁶ Ze srovnání statistických dat překvapivě vyplynulo procentuální zvýšení objasněnosti, a to jak u krádeže vloupáním, tak i krádeže prosté, ač bych sama očekávala opačný výsledek.⁵⁷

Můžeme proto dojít k závěru, že novela zpříšňující podmínky pro získání telekomunikačních dat se výraznějším způsobem nedotkne objasněnosti kriminality, neboť u většiny trestných činů je možné získat příkaz podle § 88a TŘ i nadále a ani u drobné majetkové kriminality negativní vliv *prozatím* prokázán nebyl.

6. K OPRÁVNĚNÝM ORGÁNŮM

Avšak které orgány jsou těmi orgány oprávněnými získat provozní a lokalizační údaje? Zrušené ustanovení § 97 odst. 3 zákona o elektronických komunikacích ukládalo povinnost operátorům poskytovat dané údaje orgánům oprávněným k jejich vyžádání dle zvláštního předpisu. Takováto formulace však v aplikační praxi vzbuzovala pochybnost, zda mezi tyto orgány patří i zpravodajské služby, konkrétně Bezpečnostní informační služba (dále jen BIS) a Vojenské zpravodajství, a to přestože zvláštní předpisy⁵⁸ toto oprávnění ustanovovaly. Paragraf 8 odst. 1 písm. b) zákona

⁵⁴ Např. Úmluva OSN proti nedovolenému obchodu s omamnými a psychotropními látkami ze dne 20. 12. 1988; Mezinárodní antidopingová Úmluva č. 57/2005 Sb. m. s.

⁵⁵ Aktuálnější statistická data nebyla v době uzavření rukopisu k dispozici.

⁵⁶ Porovnání proběhlo na základě kriminalistických statistik PČR zveřejňovaných na webových stránkách Policie České republiky. Policie České republiky. *Statistické přehledy kriminality za rok 2010, 2012*. Dostupné z: <http://www.policie.cz/statistiky-kriminalita.aspx>.

⁵⁷ V roce 2010 objasněnost trestného činu krádeže vloupáním činila 22,6 %, v roce 2012 pak 23,8 %. U tzv. krádeže prosté se míra objasněnosti zvýšila z 18,4 % (2010) na 22 % (2012). Není však vyloučeno, že výsledek byl ovlivněn zkreslením statistických dat.

⁵⁸ Zákon č. 154/1994 Sb., o Bezpečnostní informační službě, ve znění pozdějších předpisů, a zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění zákona č. 274/2008 Sb.

o Bezpečnostní a informační službě opravňuje BIS nejen k odposlouchávání a zaznamenávání telekomunikačního, radiokomunikačního a jiného podobného provozu, ale i k jeho zjišťování. V praxi tak docházelo k paradoxní situaci, kdy příslušníci BIS mohli na základě předchozího písemného povolení předsedy senátu Vrchního soudu⁵⁹ přímo odposlouchávat telekomunikační provoz nebo jej sami zaznamenávat, avšak získat údaje o skutečném provozu od operátorů bylo zhora nemožné, neboť ti odmítali zpravodajským službám vyhovět s ohledem na nedostatečně vymezené oprávnění.⁶⁰ Předkládaný návrh zákona učinil taxativním výčtem oprávněných orgánů takovým pochybám přítrž. Právnická nebo fyzická osoba, která provozní a lokalizační údaje uchovává, je na požádání povinna je bezodkladně poskytnout orgánům činným v trestním řízení,⁶¹ Policii České republiky,⁶² Bezpečnostní informační službě a Vojenskému zpravodajství i České národní bance pro účely dohledu nad kapitálovým trhem.

Naopak Úřad pro zahraniční styky a informace jako jediná zpravodajská služba obdobné oprávnění nemá a změnu nepřinesl ani novelizující zákon č. 273/2012 Sb. A to přestože v připomínkovém řízení k návrhu zákona Úřad pro zahraniční styky a informace požadoval vložit do § 97 odst. 3 ZEK nové písmeno a současně zapracovat do zákona č. 153/1994 Sb., o zpravodajských službách nové ustanovení, které by zakotvovalo oprávnění „pro ochranu činností, které koná na území České republiky, a jestliže je to nezbytné pro plnění úkolů v jeho působnosti zjišťovat údaje o telekomunikačním, radiokomunikačním a jiném obdobném provozu“.⁶³ Tento požadavek byl odůvodňován získáním poznatků důležitých pro ochranu zájmů a bezpečnosti České republiky, zejména v oblasti boje proti terorismu.⁶⁴ Některé členské státy navíc svěřují toto oprávnění daňové a celní správě nebo pohraničním orgánům.⁶⁵

Přitom v původním návrhu zákona č. 247/2008 Sb., kterým se novelizoval zákon č. 127/2005 Sb., byl navrhován taxativní výčet oprávněných orgánů jejich pojmenováním – v prvním návrhu stálo pouze Policie České republiky, pozměňovací návrhy vkládaly vedle PČR i státního zástupce a soud. Přijatý zákon však se od tohoto výčtu oprostil a vložil na místo toho širší pojem „oprávněným orgánům“.⁶⁶

⁵⁹ Srov. § 9 zákona č. 154/1994 Sb., o Bezpečnostní informační službě.

⁶⁰ Stejně je tato situace upravena v zákoně č. 289/2005 Sb., o Vojenském zpravodajství.

⁶¹ Jsou-li splněny podmínky stanovené zákonem č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů. Podmínky vymezuje § 88a TR. Co se rozumí pojmem policejní orgán, vymezuje § 12 odst. 2 TR.

⁶² Pro účely zahájení pátrání po konkrétní hledané nebo pohřešované osobě, zjištění totožnosti osoby neznámé nebo totožnosti nalezené mrtvoly, předcházení nebo odhalování konkrétních hrozeb v oblasti terorismu nebo prověřování chráněné osoby a při splnění podmínek stanovených zákonem č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

⁶³ Vypořádání připomínek k materiálu s názvem: návrh zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, a některé další zákony.

⁶⁴ Průběh vypořádání připomínek k návrhu zákona říká, že zásadní připomínka Úřadu pro zahraniční styky a informace byla akceptována, avšak v návrhu zákona se neobjevila.

⁶⁵ Důvodová zpráva k návrhu zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), a některé další zákony, 22. únor 2012, s. 20. Dostupná z: <http://eklep.vlada.cz/eklep/getAttachment?id=zdrack8rveq1pl.doc>.

⁶⁶ Pozměňovací návrhy ke Sněmovnímu tisku 398; Sněmovní tisk 398/4. Poslanecká sněmovna, 2008, 5. volební období, 2006–2010. Dostupné z: <http://www.psp.cz/sqw/text/tiskt.sqw?o=5&ct=398&ct1=4>.

Pro účely výkonu dohledu nad kapitálovým trhem je tento nástroj svěřen i České národní bance.⁶⁷ Byť se někteří domnívají, že Česká národní banka by měla být z okruhu oprávněných orgánů vyškrtuta.⁶⁸ Svěřit tento nástroj správnímu orgánu je velice neobvyklé i v porovnání s ostatními členskými státy.⁶⁹ Je možné pochybovat i o souladu s účelem uchovávání telekomunikačních dat dle Směrnice o data retention.⁷⁰ Tento nástroj má sloužit především k prevenci, odhalování a objasňování závažné trestné činnosti. Přesto do taxativního výčtu orgánů oprávněných získat provozní a lokalizační údaje ČNB v rámci novely § 97 odst. 3 zákona č. 127/2005 Sb. zařazena byla.

Policejní orgán má oprávnění získávat provozní a lokalizační údaje nejen pro účely trestního řízení, ale i v jiných případech. Zmocnění k vyžádání těchto dat obsahuje vedle § 88a TR i § 68 odst. 2 a § 71 písm. a) zákona o Policii ČR, a to k zahájení pátrání po konkrétní hledané či pohřešované osobě, za účelem identifikace osoby neznámé totožnosti, popř. nalezené mrtvoly a pro boj s terorismem. Další zmocnění policejního orgánu je obsaženo v zákoně č. 137/2001 Sb., o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízením a o změně zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů. Za takových okolností je policejní orgán oprávněn žádat provozní a lokalizační údaje bez jakéhokoli soudního či jiného povolení. Úřad pro ochranu osobních údajů v souvislosti s novelizací institutu zjišťování telekomunikačních údajů navrhoval vrátit se ke starší úpravě a podmínit poskytnutí těchto dat souhlasem soudce krajského soudu, aby došlo ke sjednocení praxe při vydávání povolení a bylo ochráně soukromí učiněno za dost.⁷¹ Jeho připomínka však akceptována nebyla.

Přestože povinnost uchovávání provozních a lokalizačních dat byla nálezem Ústavního soudu Pl. ÚS 24/10 zrušena, operátoři těmito údaji disponovali i po tomto datu. Ovšem jen v rozsahu nezbytném pro potřeby účtování, řízení provozu, zákaznické dotazy, odhalování podvodů apod. V souvislosti s tím jim i v době po vydání nálezů Pl. ÚS 24/10 a Pl. ÚS 24/11 zůstala povinnost na žádost oprávněných orgánů provozní a lokalizační údaje poskytovat. Pokud tedy poskytovatelé telekomunikačního provozu takové údaje měli, byli povinni je na základě soudního příkazu poskytnout. Až vydáním

⁶⁷ Své oprávnění s největší pravděpodobností čerpá z čl. 12 odst. 2 písm. d) Směrnice Evropského parlamentu a Rady 2003/6/ES o zneužívání trhu, které stanoví, že orgán dohledu má mít pravomoc požadovat existující záznamy telefonní i o datovém provozu. Viz Vypořádání připomínek k materiálu s názvem: Návrh zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, a některé další zákony. Praha, leden 2012, s. 61.

⁶⁸ Legislativní rada vlády. Zmocněnkyně pro lidská práva. Vypořádání připomínek k materiálu s názvem: Návrh zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, a některé další zákony. Praha, leden 2012, s. 62, 64.

⁶⁹ Srovn. s Hodnoticí zprávou Evropské komise o Směrnici o data retention. Evropská komise. Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES) z 18. dubna 2011, Brusel. Dostupná z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:CS:PDF>.

⁷⁰ Srov. čl. 1 odst. 1 Směrnice Evropského parlamentu a Rady 2006/24/ES.

⁷¹ Vypořádání připomínek k materiálu s názvem: Návrh zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, a některé další zákony. Praha, leden 2012, s. 34, 35.

onoho druhého zmiňovaného nálezu Ústavního soudu, který dnem 30. září roku 2012 zrušil ustanovení § 88a TŘ, přestaly soudu příkazy v bagatelních věcech vydávat.⁷²

Za zamyšlení stojí otázka, jak soud naloží s údaji, které byly získány ještě před tím, než došlo k derogaci § 97 odst. 3 a 4 ZEK. Mohou být před soudem použity jako důkaz? Ústavní soud správně nechává řešení tohoto problému na obecných soudech, aby v jednotlivých případech zvážily, zda došlo k porušení základních práv dotčeného uživatele elektronických komunikací. Vydaný nálezn automaticky nevylučuje využití získaných důkazů v již probíhajícím soudním řízení. Podle mého názoru by tak soud měl v každém jednotlivém případě posoudit, zda vyžádání telekomunikačních dat vyhovuje testu proporcionality tak, jak jej definoval Ústavní soud ve svém rozhodnutí pod sp. zn. Pl. ÚS 24/10 ze dne 22. března 2011. Především by měl vzít v úvahu, zda nebylo možné sledovaného účelu dosáhnout jiným způsobem a zda zjištění, která ze získaných údajů vyplynula, dokázala převážit negativní důsledky spojené se zásahem do základních lidských práv a svobod.

7. ZÁVĚR

Hovoříme-li o uchovávání telekomunikačních údajů, hledáme rovnováhu mezi dvěma hodnotami – důslednou ochranou základních lidských práv a svobod na jedné straně a neméně důležitou činností orgánů spočívající v ochraně společnosti před trestnými činy na straně druhé. Právo na informační sebeurčení má jedinci garantovat kontrolu nad údaji o sobě samém a ponechat na jeho rozhodnutí, jaké informace prozradí svému sociálnímu okolí.

Soukromé subjekty poskytující telekomunikační služby tato data uchovávají v první řadě pro vlastní potřeby týkající se účtování, vyřizování zákaznických dotazů, odhalování podvodů apod. Směrnice o data retention providerům stanovuje povinnost činit tak i nadále, neboť v souvislosti s vývojovými trendy (nárůst paušálních tarifů, předplacené služby e-komunikace) přestávala být tato data ukládána a stala se tím nedostupná i pro účely odhalování, vyšetřování a stíhání trestné činnosti.⁷³ Otázka, kterou bychom si měli položit, proto nezní, zda provozní a lokalizační údaje uchovávat, nýbrž po jakou dobu a v jakých případech je oprávněným orgánům pro účely trestního řízení poskytnout.

Ačkoli je směrnice o data retention v některých ohledech nedokonalá – zmiňme kupříkladu chybějící definici pojmu „závažný trestný čin“, poměrně velký rozptyl lhůty pro uchovávání telekomunikačních dat či rozlišně vymezený okruh oprávněných orgánů v jednotlivých právních úpravách – představuje důležitý prostředek, na jehož základě má dojít ke sjednocení národních právních úprav za účelem usnadnění odhalování, vyšetřování a stíhání závažných trestných činů.

⁷² Nález pléna Ústavního soudu sp. zn. Pl. ÚS 24/11 byl vydán dne 20. prosince 2011.

⁷³ Evropská komise. Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES) z 18. dubna 2011, Brusel, s. 5. Dostupná z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:CS:PDF>.

Evropská Unie prostřednictvím dotčené směrnice stanovila určitý cíl a členské státy se měly postarat o to, aby byl naplněn ústavně konformním způsobem. Nevyhovující znění ustanovení § 88a TR však existovalo ještě před vznikem samotné směrnice, a tímto se pouze dostalo do středu pozornosti Ústavního soudu, který jej shledal neproporcionálním ve vztahu k zásahu do práva na informační sebeurčení. Díky rozumně stanovené horní hranici trestní sazby, která vymezuje okruh trestných činů, u kterých je možné údaje o telekomunikačním provozu získat, doplněné o taxativní výčet trestných činů a závazek ke stíhání trestné činnosti vyplývající z mezinárodních smluv, je i po novele možné telekomunikační údaje získat u většiny z trestných činů, u nichž byl tento prostředek využíván nejčastěji. Data o proběhnuvší telekomunikaci tak již není možné využít zpravidla jen pro bagatelní trestnou činnost, jakou je např. trestný čin krádeže. A i přesto statistické údaje prozatím neukazují na pokles objasněnosti tohoto druhu kriminality. Můžeme proto říci, že se zákonodárci podařilo najít schůdné řešení a rovnováhu mezi oběma hodnotami – zachovat tento vyšetřovací nástroj pro potřeby orgánů činných v trestním řízení a omezit zásah do práv na ochranu osobnosti na případy, kdy veřejný zájem oprávněně převažuje nad zájmy jednotlivce. Snad bych jen novelizované úpravě vytknula příliš široký výčet orgánů oprávněných nakládat s telekomunikačními daty a na druhou stranu krátkou lhůtu k jejich uchovávání, jež je stanovena na nejnížší možné hranici.

Jaký je skutečný význam přístupu k provozním a lokalizačním údajům pro vyšetřování trestných činů, je těžké hodnotit. Například shrnující zpráva týkající se směrnice o data retention ve Velké Británii uvádí, že až 85 % žádostí se týká dat nikoli starších než 6 měsíců.⁷⁴ Dále se v literatuře můžeme setkat s odkazem na výzkum, podle kterého pouze ve 2–4 % vyšetřovaných případů již nebyla požadovaná data dostupná.⁷⁵ Na druhou stranu však stejná zpráva zmiňuje, že údaje starší jsou využívány právě k objasnění závažné trestné činnosti. Více než polovina žádostí o poskytnutí telekomunikačních dat za účelem vyšetřování teroristických hrozeb se týká dat starších 6 měsíců.⁷⁶

Pro futuro si tedy dovoluji navrhnout znovu zvážit délku uchovávání telekomunikačních dat pro účely trestního řízení za stávajícího omezení na závažnou trestnou činnost. Doporučila bych prodloužení lhůty na 1 rok. Naopak delší retenční období než 1 rok již podle některých zdrojů orgánům činným v trestním řízení neposkytuje žádnou nebo jen malou přidanou hodnotu,⁷⁷ a je proto shledáno jako nepřiměřené ve vztahu k osobnostním právům, mezi něž patří i právo na informační sebeurčení. Jak již bylo výše zmíněno, Česká republika patří mezi několik málo členských států Evropské Unie, které délku uchovávání provozních a lokalizačních údajů stanovily na nejnížší možné hranici 6 měsíců. Prodloužením lhůty by se oprávněné orgány dostaly ke starším datům, jež

⁷⁴ *Liberty and security: Striking the balance*. UK Presidency Paper. 2005, s. 1–5. Dostupné z: <http://www.edri.org/docs/UKpresidencypaper.pdf>.

⁷⁵ Max-Planck Institut für ausländisches und internationales Strafrecht. Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach § 100g, 100h StPO. Forschungsbericht im Auftrag des Bundesministeriums der Justiz. Freiburg. 2008.

⁷⁶ *Liberty and security: Striking the balance*. UK Presidency Paper. 2005, s. 1–5. Dostupné z: <http://www.edri.org/docs/UKpresidencypaper.pdf>.

⁷⁷ MARAS, M.-H. The economic costs and consequences of mass communications data retention: is the data retention directive a proportionate measure? *European Journal of Law and Economics*, 2012, roč. 33, č. 2, s. 458.

by mohly významným způsobem pomoci při odhalování a vyšetřování organizované trestné činnosti. Soukromé subjekty tato data pro své účely uchovávají i ve lhůtách několikrát delších, tak proč je současně neposkytnout i oprávněným orgánům pro boj s kriminalitou?

OBTAINING TELECOMMUNICATION DATA AS AN INSTRUMENT FOR INVESTIGATION OF INTERNET CRIME

Summary

The paper deals with the legislation of obtaining telecommunication data as an important instrument for investigation of crime and changes that have occurred as a result of finding the existing legislation unconstitutional. The main point is the necessity of transposition of the data retention directive 2006/24/ES which has produced many contradictory reactions and has been the subject of review constitutional courts of several EU Member States. The main conflict is between two values – protection of intimate personal data, on the one hand and the investigation of criminal activity on the other. The paper deals with development of legislation, highlights the amendments and also offers a comparison of issues in the legislation of other EU Member States. The author also tries to infer whether and what influence did amendment § 88a TR have on solving of criminality.

Key words: data retention, telecommunications, cyber crime, criminal procedure

Klíčová slova: uchovávání dat, telekomunikace, kybernetická kriminalita, trestní řízení