Blanketní uchovávání komunikačních údajů v judikatuře evropských soudů

Daniel Novák*

1. Zásady směrnice o uchovávání údajů

Podstatu směrnice o uchovávání údajů (plným názvem směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. 3. 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES, dále též „Data Retention Directive", „DRD") představuje vymezení povinnosti poskytovatelů veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí uchovávat provozní a lokalizační údaje, resp. související údaje nezbytné k identifikaci účastníka nebo uživatele.[1] Uchovávání obsahu sdělení nepředepisuje, ale v některých případech svými důsledky zaručuje. Směrnice deklarovala záměr zajistit dostupnost údajů pro účely vyšetřování, odhalování a stíhání závažných trestných činů, a to po dobu 6 až 24 měsíců. V případě žádosti příslušných vnitrostátních orgánů jsou správci těchto údajů povinni k jejich poskytnutí.[2] DRD znamenala komplexnější zásah do právní regulace elektronických komunikací, jak vyplývá již z jejího názvu předznačujícího změnu směrnice 2002/58/ES.[3] K dalším přesahům náleží povinnost Evropské komise podávat zprávy týkající se používání souvisejících směrnic.[4] DRD nabyla účinnosti dne 3. 5. 2006.

Úsilí bezpečnostních složek o uplatnění důslednějších metod kontroly nad elektronickou komunikací se vyznačuje stejně dlouhou historií jako informační technologie samotné, avšak zásadní impuls získalo teroristickými útoky z 11. 9. 2001. Vliv této události se projevil i ve státech, které k omezování svobod legitimizovanému bezpečnostními hrozbami tradičně přistupovaly zdrženlivě.[5] Kromě terorismu a organizovaného zločinu předmětnou regulaci odůvodňovaly zkušenosti se šířením počítačových virů jako „Melissa" nebo „I Love You", resp. jejich variant.[6] Téma záhy nabylo evropskoprávní rozměr. Na kriminalistický význam komunikačních údajů upozornila Rada EU ve složení ministrů spravedlnosti a vnitra dne 19. 12. 2002.[7] De-

* Mgr. et Mgr. Daniel Novák, asistent soudce Ústavního soudu ČR

[1] Za zaznamenání stojí, že základními okruhy uchovávaných údajů (srov. čl. 1 odst. 2 a čl. 5) jsou údaje potřebné k: dohledání a identifikaci zdroje sdělení, identifikaci adresáta sdělení, zjištění data, času a doby trvání komunikace, určení typu sdělení, identifikaci komunikačního vybavení uživatelů nebo jejich údajného komunikačního vybavení a zjištění polohy mobilního komunikačního zařízení.

[2] Tito poskytovatelé zásadně nebudou (v souvislosti s uchováváním údajů) považováni za nositele veřejné moci, což je významné z hlediska aplikace Úmluvy o ochraně lidských práv a základních svobod. Stát je ovšem povinen vytvořit odpovídající právní záruky pro zachování ochrany soukromí. Lze tudíž předpokládat, že subjekty údajů budou případnou procesní pozornost obracet zejména ke státu, a nikoli poskytovatelům.

[3] VANÍČEK, Zdeněk. Předpisový rámec elektronických komunikací EU čeká revize. *Právní zpravodaj*. 2006, č. 4, s. 15–16.

[4] Čl. 14 DRD, čl. 18 DPEC a čl. 25 Směrnice Evropského parlamentu a Rady 2002/21/ES ze dne 7. 3. 2002 o společném předpisovém rámci pro sítě a služby elektronických komunikací (rámcová směrnice).

[5] Ve Spojeném království byla problematika diskutována na parlamentní úrovni již v prosinci 2001. Srov. Comments of the Information Commissioner on the provisions of the Anti-Terrorism, Crime and Security Bill relating to the retention of communications data. Dostupné z http://www.publications.parliament.uk/pa/jt200102/jtselect/jtrights/51/51ap02.htm. Srov. též diskusi o Regulation of Investigatory Powers Act (RIPA), ActAnti-terror laws raise net privacy fears, on line http://news.bbc.co.uk/2/hi/science/nature/1647309.stm. Dále též Andy McCue: Government rethinks data policy. Dostupné z http://www.computing.co.uk/ctg/news/1842253/government-rethinks-policy. Secret plan to spy on all British phone calls. Dostupné z http://www.observer.co.uk/uk_news/story/0,6903,406191,00.html. EDITORIAL: Spied on from cradle to grave. Dostupné z http://www.observer.co.uk/leaders/story/0,6903,406160,00.html.

[6] Zásady boje proti počítačové kriminalitě formuluje americká studie z března 2000 The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet. A Report of the President's Working Group on Unlawful Conduct on the Internet. Dostupné z http://www.justice.gov/criminal/cybercrime/unlawful.htm.

[7] Council Conclusions of 19 December 2002 on information technology and the investigation and prosecution of organised crime. Dostupné z http://www.consilium.europa.eu/ueDocs/cms_Data/docs/polju/en/EJN288.pdf Dále též Rozhodnutí

klarace o boji proti terorismu, kterou Evropská rada přijala dne 25. 3. 2004, pověřila Radu EU přezkoumáním návrhů opatření směřujících k uchovávání těchto údajů poskytovateli služeb.[8]

Ačkoli DRD ve 22. odstavci preambule oznamuje, že dodržuje základní práva a ctí zásady uznávané zejména Listinou základních práv Evropské unie“ (dále též „Listinou“), patří k nejkontroverznějším tématům práva EU, a to se zřetelem k jí založenému průlomu do ochrany soukromí v informačním smyslu.[9] Že DRD trpí z lidskoprávního hlediska nedostatky, zejména ve vztahu k vymezení podmínek přístupu orgánů k uchovávaným údajům a výmazu předmětných údajů, varoval již ve fázi předcházející jejímu schválení Evropský inspektor ochrany údajů a Evropský hospodářský a sociální výbor.[10] Není tudíž překvapivé, že implementaci směrnice – příslušná lhůta skončila dne 15. 9. 2007 – provázely spory, které nalezly konkrétní výraz v soudních řízeních před Evropským soudním dvorem (dále též „ESD“) a posléze i ústavními či správními soudy členských států.

2. Kritika směrnice o uchovávání údajů

Kritiku právního rámce blanketního uchovávání údajů lze nejobecněji rozčlenit podle toho, zda obrací pozornost k DRD nebo vnitrostátní transpoziční úpravě. V prvním případě jsou uplatňovány výhrady formální nebo obsahové. *Formální* rovina se stala předmětem přezkumu ESD z iniciativy Irska (podporovaného Slovenskou republikou), které zpochybnilo adekvátnost poukazu směrnice na čl. 95 Smlouvy o ES týkající se sbližování právních předpisů o vnitřním trhu, v řízení vedeném pod C-301/06.[11] Irsko navázalo na svůj předchozí návrh, kterým se spolu s Francií, Spojeným královstvím a Švédskem dne 28. 4. 2004 vyslovilo, aby předmětná problematika byla upravena rámcovým rozhodnutím založeným na čl. 30, čl. 31 odst. 1 bod c)

Rady 2003/48/SVV ze dne 19. 12. 2002 o uplatnění zvláštních opatření v oblasti policejní a soudní spolupráce v boji proti terorismu v souladu s článkem 4 společného postoje 2001/931/SZBP. Dostupné z http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003D0048:CS:HTML

[8] Declaration on Combating Terrorism. Dostupné z http://ue.eu.int/ueDocs/cms_Data/docs/pressData/en/ec/79637.pdf.

[9] Ohledně ochrany provozních údajů lze poukázat na řadu doporučení a stanovisek:

Article 29 Working Party. Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6. (10750/02/EN/Final, WP 58, 30. 5. 2002). Dostupné z http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp58_en.pdf.

Article 29 Working Party. Opinion 7/2000 On the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 COM (2000) 385 (5042/00/EN/FINAL, WP36, 2. 11. 2000). Dostupné z http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp36en.pdf.

Article 29 Working Party. Opinion 4/2001 On the Council of Europe's Draft Convention on Cyber-crime. (5001/01/EN/Final WP 41, 22. 3. 2001). Dostupné z http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp41en.pdf.

Article 29 Working Party. Opinion 10/2001 on the need for a balanced approach in the fight against terrorism. (0901/02/EN/Final, WP 53, 14. 12. 2001). Dostupné z http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp53en.pdf.

Article 29 Working Party. Opinion 5/2002 on the Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 September 2002) on mandatory systematic retention of telecommunication traffic data. (11818/02/EN/Final, WP 64, 11. 10. 2002). Dostupné z http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp64_en.pdf.

Article 29 Working Party. Opinion 1/2003 on the storage of traffic data for billing purposes. (12054/02/EN, WP 69, 29. 1. 2003). Dostupné z http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp69_en.pdf.

Article 29 Working Party. Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism. [Proposal presented by France, Ireland, Sweden and Great Britain (Document of the Council 8958/04 of 28 April 2004)] (11885/04/EN, WP 99, 9. 11. 2004). Dostupné z http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp99_en.pdf.

[10] Stanovisko Evropského inspektora ochrany údajů k návrhu rámcového rozhodnutí Rady o ochraně osobních údajů zpracovávaných v rámci policejní a soudní spolupráce v trestních věcech (KOM(2005) 475 v konečném znění) (2006/C 47/12). Dostupné z http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:047:0027:0047:CS:PDF.

Stanovisko Evropského hospodářského a sociálního výboru k Návrhu směrnice Evropského parlamentu a Rady o uchovávání údajů zpracovávaných v souvislosti s poskytováním veřejných služeb v odvětví elektronických komunikací, kterou se mění směrnice 2002/58/ES KOM(2005) 438 v konečném znění – 2005/0126 (COD) (2006/C 69/04). s. 16. Dostupné z http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:069:0016:0021:CS:PDF.

[11] Rozsudek ESD ze dne 10. 2. 2009, C-301/06, Irsko v. Evropský parlament a Rada Evropské unie. Dostupné z http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006J0301:CS:HTML.

a čl. 34 Smlouvy o Evropské unii.[12] Pracovní skupina Rady EU v jeho intencích vypracovala dokument, který obsahoval předlohu rámcového rozhodnutí o uchovávání údajů. Z jejího textu však nevyplývá vyšší úroveň ochrany lidských práv oproti úpravě přijaté posléze formou směrnice.[13] Odmítnutí „irského" normativního řešení odůvodnila Právní služba Rady EU, která dospěla k závěru, že harmonizace blanketního uchovávání údajů spadá do pravomoci Společenství.[14] Uplatněný názor je slučitelný s vnitřní logikou směrnice 2002/58/ES, kterou DRD mění.[15] DRD navazuje na modifikaci zásady minimality v čl. 15 odst. 1 uvedené směrnice, který zahrnuje právní podklad pro její omezení odůvodnitelné konstatováním, že jde o opatření v demokratické společnosti nezbytné, přiměřené a úměrné pro zajištění národní bezpečnosti (tj. bezpečnosti státu), obrany, veřejné bezpečnosti a pro prevenci, vyšetřování, odhalování a stíhání trestných činů nebo neoprávněného použití elektronického komunikačního systému, jak je uvedeno v čl. 13 odst. 1 směrnice 95/64/ES.[16] Obsah těchto opatření – spočívajících v časově omezeném zadržení údajů – podléhá korektivu obecných zásad práva Společenství, včetně zásad uvedených v čl. 6 odst. 1 a 2 Smlouvy o EU.

Právě odtud se odvíjela legislativní hlediska pro zařazení uchovávání provozních a lokalizačních údajů do směrnicového práva. Řečené potvrdilo stanovisko vzešlé z administrativy Evropské komise, které přisvědčilo úzké souvislosti DRD s čl. 95 Smlouvy o ES.[17] Vydaný dokument spatřoval v DRD jistou konkretizaci či upřesnění čl. 15 odst. 1 směrnice 2002/58/ES. Současně DRD omezila dosah „výchozího" článku tím, že z něj vyňala údaje podle vlastního čl. 1 odst. 1. Ve svých faktických dopadech došlo transpozicí DRD v převážné většině členských států k posílení bezpečnostních složek. Z hlediska práva EU nebyl tento výsledek nevyhnutelný. Jak Ústavní soud České republiky v nálezu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10, odst. 41, konstatoval, napadenou (vnitrostátní) právní úpravou regulovaný rozsah uchovávaných údajů se zcela zřetelně pohybuje nad rámcem předvídaným v DRD.[18] Naopak do vnitrostátní úpravy nebyly zahrnuty konkretizované právní záruky slučitelné s DRD. K této převažující tendenci lze konstatovat, že čl. 15 odst. 1 směrnice 2002/58/ES ve znění před účinností DRD poskytoval širší uvážení národnímu zákonodárci, avšak poukaz na nutnost implementovat „dobře viditelnou" evropskou legislativu umožní bez bližší argumentace přejít fakt, že zákon omezuje soukromí výrazněji, než ve skutečnosti DRD požaduje. Právě z této perspektivy je možné nahlížet na část kritiky DRD. Tím ovšem nejsou výtky vůči DRD vyvráceny. Za zaznamenání stojí paradox, že v Irsku, které požadovalo zrušení DRD, byla vydána úprava odkazující na čl. 15 směrnice 2002/58/ES, která zakotvila uchovávání údajů po dobu čtyř let, tj. v nejdelší lhůtě v EU.[19]

ESD v rozsudku ze dne 10. 2. 2009, C-301/06, konstatoval, že DRD v čl. 95 Smlouvy o ES nalézá právně regulérní oporu. Dovodil, že uvedená směrnice se svým věcným obsahem týká převážně fungování vnitřního trhu, resp. odstranění překážek na vnitřním trhu elektronických komunikací. Že podstatné rozdíly existovaly, zůstává nezpochybnitelné. ESD neshledal potřebným podrobnější odůvodnění, zda tato situace vytvářela problémy, jejichž řešení nemohlo být ponecháno na členských státech a dispozicích čl. 15 směrnice 2002/58/ES. DRD podle soudu upravuje operace, které jsou nezávislé na provedení jakéhokoli případného úkonu v oblasti policejní a justiční spolupráce

[12] Nejskeptičtěji se k blanketnímu uchovávání údajů stavělo Německo a Finsko.

[13] Text je datován dnem 24. 2. 2005. Working Party on cooperation in criminal matters Article 36 Committee, 15098/04 COPEN 142 TELECOM 172. Dostupné z http://www.statewatch.org/news/2005/apr/draft-data-retention-proposal.pdf.

[14] Avis du service juridique. Conseil de l´Union Européenne. 5. 4. 2005. No. 7688/05. Dostupné z http://www.statewatch.org/news/2005/apr/Council-legal-opinion-data-retention.pdf.

[15] Jmenované stanovisko připomíná recitál 9 preambule směrnice 2002/58/ES, který předepisuje, že členské státy, dotčení poskytovatelé a uživatelé, jakož i příslušné orgány Společenství, by měli spolupracovat při zavádění a rozvoji odpovídajících technologií, pokud je to nezbytné pro uplatňování ochranných opatření stanovených touto směrnicí, a měli by především mít na zřeteli minimalizaci zpracování osobních údajů a používání anonymních nebo pseudoanonymních údajů tam, kde je to možné. Zásadu minimality dále rozvíjí čl. 6 citované směrnice.

[16] K zásadě minimality srov. čl. 6 odst. 1 písm. c) a e) a potažmo v čl. 7 a 8 Směrnice Evropského parlamentu a Rady 95/46/ES a čl. 6 odst. 1 písm. c) a e) a potažmo v čl. 7 a 8 Úmluvy č. 108 o ochraně osob se zřetelem na automatizované zpracování osobních údajů.

[17] Projet de décision-cadre sur la conservation des données – Analyse juridique. Document de travail des services de la Commission. Bruxelles, le 22. 3. 2005, SEC(2005) 420.

[18] Ústavní soud konstatoval, že nad rámec předmětné Směrnice o data retention se u internetového připojení a služeb a e-mailové komunikace sleduje a uchovává množství přenesených dat, informace o použití šifrování, metoda a status požadavků na službu a její realizace a rovněž i informace o posílání SMS z internetových bran a další „zájmové identifikátory". U telefonie nad rámec Směrnice o data retention napadená právní úprava vyžaduje uchovávat údaje o identifikaci předplacené telefonní karty, veřejného telefonního automatu, čísla dobíjecích kuponů a jejich přiražení k dobíjenému číslu, vazbu mezi mobilním přístrojem a vloženými SIM kartami.

[19] Komplexní přehled legislativních úprav před implementací DRD poskytuje text Council of the European Union. Answers to questionnaire on traffic data retention. 14107/02 LIMITE. CRIMORG 100. TELECOM 42. Dostupné z http://www.effi.org/sananvapaus/eu-2002-11-20.html.

v trestních věcech, a neharmonizuje otázku přístupu vnitrostátních orgánů příslušných v trestněprávní oblasti k údajům, ani jejich využívání či výměnu mezi uvedenými orgány. Právě vzdálenější vztah ke státním orgánům vyvolal rozdílný výsledek řízení oproti rozsudku ESD ze dne 30. 5. 2006, C-317/04 a C-318/04, který se týkal předávání osobních údajů cestujících letadly. ESD tudíž odmítl argumentaci, že směrnice byla vydána na nesprávném smluvním základě, neboť ve skutečnosti dopadá na oblast vnitřní bezpečnosti.[20] Jinak řečeno, položil důraz na okolnost, že adresátem povinností jsou účastníci trhu („poskytovatelé služeb"), a nevyvodil důsledky z účelu uchovávání těchto údajů, a sice zajištění jejich dostupnosti státu.[21] To je však z hlediska ustálené systematiky právní úpravy překvapivé, neboť odposlechy a záznamy telekomunikačního provozu představují instituty trestního práva procesního, a nikoli veřejného hospodářského práva, kterým je v rámci práva telekomunikačních systémů upravena technická (detailnější) stránka věci (srov. český zákon č. 141/1961 Sb., trestní řád, v § 88 a § 88a).[22] Poskytovatelé se k harmonizaci úprav stavěli zdrženlivě; pokud působí ve více členských státech, odlišné vnitrostátní úpravy na ně dopadají zvýšenými administrativními náklady, avšak prodloužení (či nové založení) povinnosti uchovávat údaje znamená navýšení výdajů přinejmenším srovnatelné.[23]

Obsahová udržitelnost DRD samotné – tj. její lidskoprávní dimenze – prozatím ESD, resp. Soudním dvorem Evropské unie (dále též „SDEU") prověřena nebyla. Ani výše uvedené irské podání předmětnou otázku nepředestřelo. Zde se projevuje určitý nedostatek účinných procesních nástrojů přezkumu aktů práva EU při současné existenci záruk v oblasti „hmotného" práva lidských práv, kdy za účinnosti Lisabonské smlouvy je referenčním rámcem především Listina a Úmluva o ochraně lidských práv a základních svobod (dále též „Úmluva").

Příležitost k otevření této argumentační roviny neposkytly ani ústavní či správní soudy členských států, které v rámci svých řízení týkajících se dané problematiky lucemburskému soudu předběžnou otázku nepředložily. Neučinil tak ani Spolkový ústavní soud v řízení vedeném pod sp. zn. 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, neboť vyšel z konstatování, že DRD zakládá povinnost údaje ve vymezeném rozsahu uchovávat, nestanoví však podmínky přístupu k údajům a jejich použití orgány členských států. V samotné otázce uchovávání údajů určených směrnicí, tj. pramenem komunitárního práva (vyznačujícím se aplikační předností), neshledal kolizi se základními právy a svobodami podle Základního zákona.[24] Toto ostré rozlišení mezi „uchováváním" a „přístupem", které formuloval ESD v rozsudku C-301/06, však není samozřejmé, a to též ve světle (byť poměrně obecného) čl. 4 DRD, nadepsaného „přístup k údajům".

---

[20] Ve shodě s ESD právní služba Rady již dříve (viz čl. 25 stanoviska) nezpochybnila úsudek, že poté, co jsou příslušnými státními orgány uchovávané údaje vyžádány pro účely trestněprávní, nacházejí se mimo materii komunitárního práva.

[21] Srov. ANDENAS, Mads; ZLEPTNIG, Stefan. Surveillance and Data Protection: Regulatory Approaches in the EU and Member States. European Business Law Review. 2003, no. 14, s. 765–813. Konzistentně rozhodl ESD rozsudkem ze dne 29. 1. 2008, C-275/06, Promusicae, a usnesením ze dne 19. 2. 2009, C-557/07, LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v. Tele2 Telecommunication GmbH, kdy dospěl k závěru, že předávání komunikačních údajů státním orgánům je neharmonizovanou problematikou práva členských států.

[22] Připodobitelnou ediční povinnost, která obecně stíhá každého, kdo má věc důležitou pro trestní řízení u sebe, řadíme do trestního řádu rovněž, a nikoli např. do obchodního zákoníku pod úpravu společenstevního práva, má-li danou věc vydat obchodní společnost.

[23] Poskytovatelé služeb vyjadřovali obavy z nákladů spojených s implementací předpisů týkajících se retence údajů. Loney, Matt. 12. 2. 2002. ISPs spell out true cost of data retention. Dostupné z http://www.zdnet.co.uk/news/regulation/2002/12/12/isps-spell-out-true-cost-of-data-retention-2127408/ Poskytovatelé v některých státech ovšem posléze využili příležitosti a získané údaje jim slouží k vymáhání pohledávek, resp. k marketingu, což oprávněně kritizoval Ústavní soud v nálezu sp. zn. Pl. ÚS 24/10, odst. 57. K tomu srov. snahy nositelů práv duševního vlastnictví o zpřístupnění těchto údajů pro vlastní právní postupy. Problematiku uchovávání údajů z hlediska neziskového sektoru rozebírá text DANEZIS, George. Traffic Data Retention. Impact on civil society organization. University of Cambridge, Computer Laboratory. Dostupné z http://www.worldcivilsociety.org/onlinenews/docs/18.09_danezis_george_wcsf-position.pdf. Potřebnost harmonizace kvůli úsporám nákladů poskytovatelů služeb působících ve více jurisdikcích oproti tomu potvrzuje zpráva Common Industry Statement on Storage of Traffic Data for Law Enforcement Purposes, s. 5, kterou společně vydaly významné zájmové organizace ICC, UNICE, EICTA a INTUG.. Dostupné z www.statewatch.org/news/2003/jun/CommonIndustryPositiondataretention.pdf. Z dalších dokumentů srov. *G8* Government-Industry Workshop on Safety and Security in Cyberspace: Report of Workshop 1: Data Retention, Tokyo, květen 2001, www.mofa.go.jp/policy/i_crime/high_tec/conf0105-4.html. ECTA, European Competitive Telecommunications Association: ECTA position on data retention in the EU, srpen 2002, https://www.ectaportal.com/uploads/-1412ECTAdataretentionstatement.DOC. ECTA, European Competitive Telecommunications Association: ECTA attacks EU Government plans to undermine internet users privacy and increase costs, ECTA News release, 11. 9. 2002, https://www.ectaportal.com/uploads/413Data_retention_110902.doc.

EuroISPA, Internet Service Providers' Association (Europe) / US ISPA, Internet Service Providers' Association (U.S.A.): Position on the Impact of Data Retention Laws on the Fight against Cybercrime, 30. 9. 2002, Dostupné z www.euroispa.org/docs/020930eurousispa_dretent.pdf.

[24] Jak je uvedeno níže, specifickou výjimkou je komunikace s institucemi plnícími některé služby sociální pomoci.

Ústavní soud České republiky ve věci sp. zn. Pl. ÚS 24/10 nevyhověl požadavku na předložení předběžné otázky uplatněnému navrhovateli – skupinou poslanců, kteří dali přednost soudnímu řízení (oproti změně úpravy ve „standardním" zákonodárném procesu) též se zřetelem k možnosti zpochybnit – v pomyslném dalším „instančním stupni" – přímo obsah směrnice.

Předběžnou otázku nevznesl ani rumunský Ústavní soud, jehož rozhodnutí ze dne 8. 10. 2009, no. 1258, při srovnání se svými evropskými protějšky vyznívá coby doposud nejkategoričtější kritika blanketního uchovávání údajů.[25] Označené – poměrně stručné rozhodnutí – zrušuje zákon č. 298/2008. Napadené úpravě vytýká nejasné vymezení kategorií uchovávaných údajů, osobního dosahu a státních orgánů s přístupem k údajům. Zákon je kladen do kontrastu s trestním řádem, který zakotvuje přísnější pravidla ohledně obsahu komunikace. Rozhodnutí Ústavního soudu se nevyslovuje k závazkům Rumunska vyplývajícím z práva EU, resp. povinností implementovat DRD. Potud jde o „běžnou" argumentaci. Dále však konstatuje, že „povinnost uchovávat údaje, založená zákonem č. 298/2008 jako výjimka nebo derogace zásady ochrany osobních údajů a jejich důvěrnosti činí prázdným – skrze svoji povahu, délku a oblast použití – obsah této zásady". Rozhodnutí též brojí proti dopadům úpravy na všechny osoby, bez ohledu na to, zda spáchaly trestný čin nebo nikoli, resp. zda jsou vyšetřovány. Tím je podle rumunského Ústavního soudu popřena presumpce neviny, přičemž a priori jsou všichni uživatelé elektronických komunikačních prostředků považováni za osoby, podezřelé nebo vinné z terorismu nebo jiné závažné trestné činnosti.

Do „radikálnějšího" směru kritiky blanketního uchovávání údajů lze zařadit též rozhodnutí Správního soudu ve Wiesbadenu ze dne 27. 2. 2009, sp. zn. 6 K 1045/08, v němž se vyslovuje přesvědčení, že uchovávání údajů porušuje základní právo na ochranu soukromí. Retenci soud shledal nikoli potřebnou v demokratické společnosti a směrnici samotnou stojící v rozporu se zásadou proporcionality chráněnou též čl. 8 Úmluvy. Obsahové těžiště kritiky vtělené do tohoto rozhodnutí lze spatřovat v otázce „preventivní" povahy dohledu i nad těmi, kdo se nezákonného jednání nedopustili.[26] Pozdější rozsudek Spolkového ústavního soudu ovšem zde uplatněná hlediska zčásti překonal.

Uvedená rozhodnutí představují radikálnější směr kritiky, avšak nejsou způsobilá otřást legislativním rámcem Evropské unie. Určitý vývoj na tomto poli by mohl přinést irský Vysoký soud, který dne 5. 5. 2010 v řízení o žalobě nevládní organizace Digital Rights Ireland Limited deklaroval, že předběžnou otázku předloží; prozatím ji však neformuloval. Tento procesní postup již uplatnil švédský Nejvyšší soud, přičemž řízení o předběžné otázce je vedeno pod C-461/10. Zde je ovšem otevřena specifická problematika vztahu mezi DRD a směrnicí Evropského parlamentu a Rady 2004/48/ES ze dne 29. 4. 2004 o dodržování práv duševního vlastnictví, zejména jejím čl. 8, který předvídá kompetenci soudních orgánů nařídit zpřístupnění informace o původu a distribučních sítích zboží či služeb, kterými je porušováno právo duševního vlastnictví. Posuzovaná věc vychází z civilního sporu, zatímco DRD se týká oblasti trestněprávní. Nejvyšší soud posléze obrátil pozornost k vlivu okolnosti, že DRD nebyla doposud do švédského právního řádu implementována.[27] Indikátorem může být rozsudek Soudního dvora EU (velkého senátu) ze dne 9. 11. 2010 ve spojených věcech C-92/09 a C-93/09 (Volker und Markus Schecke GbR a Hartmut Eifert v. Land Hessen), který zdůrazňuje nezbytnost vytvoření záruk ochrany základních práv jednotlivců při nakládání s osobními údaji pocházejícími z elektronické komunikace.

„Radikální" oponenti DRD dovozují její neslučitelnost s Úmluvou, a to argumentací, že členské státy transpozičními úpravami nedostojí (resp. nemohou dostát) již samotnému kritériu zákonnosti omezení čl. 8 Úmluvy, neboť šíře osobního dosahu retence (předepsaná DRD) je postavitelná naroveň s neurčitou zákonnou úpravou, proti níž se Evropský soud pro lidská práva (dále též „ESLP") vyslovil rozsudky Kruslin v. Francie či Amann v. Švýcarsko.[28] Harmonizované uchovávání údajů tak má porušovat Úmluvu *per se*.[29] Odpůrci DRD

[25] Rozhodnutí rumunského Ústavního soudu ze dne 8. 10. 2009, no. 1258. Dostupné z http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html.

[26] Rozhodnutí Správního soudu ve Wiesbadenu ze dne 27. 2. 2009, sp. zn. 6 K 1045/08. Dostupné z http://wiki.vorratsdatenspeicherung,de/Uneil_VG_Wiesbaden_2009-02.

[27] Jisté vodítko představují rozsudek ESD ze dne 29. 1. 2008, C-275/06, Promusicae a usnesení ze dne 19. 2. 2009, C-557/07, LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v. Tele2 Telecommunication GmbH; obě rozhodnutí se týkají vztahu mezi retencí údajů a ochranou práv duševního vlastnictví. Text předběžných otázek ve věci C-461/10 je dostupný z http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:317:0024:0024:EN:PDF

[28] Rozsudek ESLP ze dne 24. 4. 1990 ve věci Kruslin v. Francie, stížnost č. 11801/85, resp. rozsudek ESLP ze dne 16. 2. 2000 ve věci Amann v. Švýcarsko, stížnost č. 27798/95. Již z principu odmítá blanketní uchovávání údajů text Privacy International. Covington & Burling, Memorandum of laws concerning the legality of data retention with regard to the rights guaranteed by the European Convention on Human Rights, ze dne 10. 10. 2003, s. 9. Dostupné z http://www.statewatch.org/news/2003/oct/Data_Retention_Memo.pdf.

[29] Že blanketní uchovávání údajů v daném rozsahu nemůže být shledáno slučitelným s Úmluvou, předvídá dokument Privacy International. Covington & Burling, Memorandum of laws concerning the legality of data retention with regard to

čerpají též z rozsudku ve věci S. a Marper v. Spojené království, směřujícímu proti blanketním a nediskriminačním opatřením, které se uplatňují bez ohledu na individuální dopady a charakteristiky.[30] Odlišností mezi uvedeným judikátem a pravidly DRD je konkrétně omezená doba uchovávání údajů, pročež nelze zde uplatněné výhrady přenášet bez dalšího na evropské směrnicové právo. ESLP se k právním aktům Evropské unie vyslovuje zdrženlivě, nicméně jeho případná kritika postupů orgánů členských států vycházejících z DRD by v první řadě postavila tyto členské státy před volbu mezi porušením povinností daných směrnicí a Úmluvou.[31]

Že přinejmenším dočasné nerespektování DRD není pro některé státy nemyslitelné, dokládá jejich prodlení s implementací (v této souvislosti se hovoří o Irsku, Nizozemsku, Polsku, Rakousku, Řecku a Švédsku).[32] Prostor pro uplatnění námitek z nedostatečné ochrany lidských práv tak může být vytvořen případnými právními postupy Evropské komise a SDEU. Průtahy jsou v případě Švédska paradoxní, neboť novela telekomunikačního zákona (FRA-lagen) – schválená přes protesty veřejnosti – ukládá místním operátorům a poskytovatelům internetového připojení předávat komunikační údaje, a to včetně obsahové složky, zpravodajské službě (FRA) k využití nepředpokládajícímu povolení soudu.[33] Jde tedy nad rámec DRD.

3. Kritika vnitrostátních úprav implementujících směrnici o uchovávání údajů

Kromě výše uvedených principiálních námitek je v judikatuře evropských soudů zastoupena umírněnější názorová pozice. Její podstatou je přesvědčení, že lze harmonizovat transpoziční úpravu s normami (vnitrostátního) ústavního práva, resp. že samotná zásada preventivního uchovávání údajů nekoliduje s ústavněprávními požadavky. Do této kategorie spadají rozhodnutí německého a českého Ústavního soudu, dále bulharského Nejvyššího správního soudu a kyperského Nejvyššího soudu.

Nejširší publicitu získal rozsudek, jímž německý Spolkový ústavní soud dospěl k závěru, že zákonodárce příslušné – v kolizi stojící právní hodnoty – neharmonizoval tak, aby výsledek dostál normám ústavního práva. Jmenovaný orgán ochrany ústavnosti svým prvním senátem rozsudkem ze dne 2. 3. 2010, sp. zn. 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, konstatoval, že uchovávání dat (stanovené preventivně a na dobu šesti měsíců) ve smyslu §§ 113a, 113b telekomunikačního zákona a použití těchto dat podle § 100g odst. 1 trestního řádu – implementující DRD – stojí v rozporu s čl. 10 odst. 1 Základního zákona (který stanoví, že listovní tajemství, jakož i poštovní a telekomunikační tajemství jsou nedotknutelná), v důsledku čehož uvedená ustanovení zrušil.[34]

Pokud jde o údaje týkající se připojení k internetu, internetové telefonie a elektronické pošty, Česká republika jako jeden z šestnácti členských států využila možnosti prodloužit lhůtu pro implementaci DRD do 15. 3. 2009.[35] Přesto byl očekávaný obsah – doposud neschválené – směrnice do právního řádu promítnut již s účinností ke dni 1. 5. 2005 zákonem č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, resp. v rovině podzákonného práva vyhláškou č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání.

---

the rights guaranteed by the European Convention on Human Rights, ze dne 10. 10. 2003. Dostupné z http://www.statewatch.org/news/2003/oct/Data_Retention_Memo.pdf. Text (předpokládající, že úprava bude obsažena v rámcovém rozhodnutí) připouští, že ESLP se prozatím k problematice nevyslovil, ovšem zákaz „nediskriminačního" uchovávání údajů považuje za nepřípustný konsekventně zejména k judikátu ESLP ve věci Klass v. Spolková republika Německo.

[30] Rozsudek velkého senátu ESLP ze dne 4. 12. 2008 ve věci S. a Marper v. Spojené království, stížnosti č. 30562/04; 30566/04.

[31] Rozsudek velkého senátu ESLP ze dne 30. 6. 2005 ve věci Bosphorus Hava Yollari Turizm ve Ticaret Anonim Sirketi v. Irsko, stížnost č. 45036/98.

[32] RICKNÄS, Mikael. Sweden challenges EU data retention directive. *Computerworld*. Vydáno 27. 5. 2009. Dostupné z http://www.computerworld.com/s/article/9133566/Sweden_challenges_EU_data_retention_directive

[33] ENDitorial: Sweden is listening to all internet and phone conversations. Dostupné z http://www.edri.org/edrigram/number6.13/sweden-fra-adoption

[34] Rozsudek Spolkového ústavního soudu ze dne 2. 3. 2010 ve věci sp. zn. 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08. Dostupné z http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011en.html. Že téma uchovávání údajů vyvolalo značný ohlas veřejnosti dokládá i počet navrhovatelů – 34 000 – kteří adresovali Spolkovému ústavnímu soudu ústavní žalobu proti předmětné právní úpravě.

[35] Prohlášení České republiky podle čl. 15 odst. 3 DRD zní: V souladu s čl. 15 odst. 3 Česká republika prohlašuje, že odkládá uplatňování této směrnice na uchovávání komunikačních údajů týkajících se připojení k internetu, internetové telefonie a internetové elektronické pošty o období 36 měsíců od data přijetí této směrnice.

Zákonem č. 247/2008 Sb., byl zákon o elektronických komunikacích – nyní již s poukazem na platnou DRD – s účinností ode dne 1. 9. 2008 změněn ve svém § 97 odst. 3 a 4 tak, že zahrnul uchovávání též neúspěšných pokusů o volání, upřesnil povinnosti poskytovat údaje příslušným orgánům a dobu uchování předmětných údajů. Součástí procesu implementace předvídaného v čl. 13 DRD je též stanovení sankčního mechanismu.[36] Orgánem dozoru nad dodržováním předpisů přijatých na podkladě čl. 7 DRD, předvídaným v čl. 9 DRD, je v České republice Úřad pro ochranu osobních údajů (§ 87 odst. 3 zákona č. 127/2005 Sb.). Z hlediska právního řádu České republiky znamená mezník nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10, zrušující – k návrhu skupiny poslanců Poslanecké sněmovny Parlamentu České republiky – její obsahové těžiště transpoziční úpravy, které představuje ustanovení § 97 odst. 3 a 4 zákona č. 127/2005 Sb., a vyhlášku č. 485/2005 Sb.

Ústavní soud České republiky zdůraznil, že jednotlivá ustanovení DRD vymezují v podstatě pouze povinnost data uchovávat. Tím však problematiku nebagatelizoval, neboť současně připomenul, že z rozsudku ESLP ve věci Malone v. Spojené království (a jím inspirované vnitrostátní judikatury) vyplývá, že i provozní a lokalizační údaje jsou součástí komunikace, a tedy spadají pod dosah ochrany soukromí ve smyslu čl. 8 odst. 1 Úmluvy.[37] Odtud se podává argumentační instrumentarium pro zpochybnění přípustnosti použití takto získaných údajů coby důkazů.[38]

Ke zrušení úpravy implementující DRD přistoupil bulharský Nejvyšší správní soud a Nejvyšší soud Kypru.[39] V současné době probíhá obdobné řízení před polským a maďarským Ústavním soudem.[40] Bulharský Nejvyšší správní soud napadenému ustanovení vytkl nedostatečné vymezení účelu, za kterým je umožněn přístup k údajům, dále absenci soudního dohledu a nerespektování ústavněprávního požadavku na „srozumitelný a dobře formulovaný základ jak pro přístup k osobním údajům, tak i jejich uchovávání“. Sporné zůstalo, zda protiústavní úprava přístupu k údajům diskvalifikuje též samotnou povinnost údaje uchovávat.

Ústavněprávní kritiku transpozičních úprav lze rozdělit do dvou základních okruhů. První předestírá výtky z nedostatečné *kvality právní úpravy*, resp. neodpovídajícího stupně její určitosti, jasnosti a předvídatelnosti. Zde by mohlo být dosažení nápravy snazší, vyjdeme-li z úvahy, že se jedná spíše o „technické“ nedopatření, a nikoli výslednici politických faktorů. Jak bylo očekávatelné, německý zákonodárce v tomto směru nepochybil. Ústavní soud České republiky konstatoval (v odst. 46–47 nálezu), že požadavkům na právní jistotu nedostála formulace § 97 odst. 3 zákona č. 127/2005 Sb., ze které nevyplývá zřetelně, jaké státní orgány jsou oprávněny vyžadovat uchovávané údaje a na základě kterého zvláštního právního předpisu; předmětná právní úprava podle Ústavního soudu neposkytuje spolehlivou oporu pro závěr, že okruh těchto subjektů je shodný s § 88a tr. řádu. Nižší standard ochrany lidských práv poskytuje předmětná úprava oproti DRD též potud, že nevymezuje konkrétní účel, pro který mohou být provozní a lokalizační údaje oprávněným orgánům poskytovány. Další ústavněprávní deficit zahrnuje nejasná lhůta uchovávání údajů (období ne kratší než 6 měsíců a ne delší než 12 měsíců, odst. 51), zákaz uchovávání obsahu zpráv (což je formulace blízká DRD, nicméně ve vnitrostátním právu by si zasloužila podrobnější vymezení) a výmaz údajů po uplynutí příslušné lhůty.

Druhá součást kritiky se týká lidskoprávních standardů – obsahově vyjasněné – úpravy. K posouzení jejich ústavněprávního významu je nutné přistoupit k testu *proporcionality* sestávajícího typicky z kritérií vhodnosti, potřebnosti a závažnosti v kolizi stojících práv. Spolkový ústavní soud vymezil – v návaznosti na uvedený test – striktní podmínky ústavněprávně konformní implementace DRD, týkající se zejména 1/ úpra-

[36] Podle čl. 13 odst. 2 DRD platí, že každý členský stát zejména přijme nezbytná opatření pro zajištění toho, aby úmyslný přístup k údajům uchovávaným v souladu s touto směrnicí nebo úmyslné předání takových údajů, jež nejsou povoleny podle vnitrostátních právních předpisů přijatých na základě této směrnice, bylo trestáno sankcemi, včetně správních nebo trestních sankcí, které jsou účinné, přiměřené a odrazující.

[37] Srov. rozsudek ESLP ze dne 2. 8. 1984 ve věci Malone v. Spojené království, stížnost č. 8691/79, resp. nálezy Ústavního soudu sp. zn. II. ÚS 502/2000 a IV. ÚS 536/2000.

[38] Jedná se o v pořadí druhou významnou ingerenci Ústavního soudu České republiky v nedávné době do problematiky dokazování v trestním řízení. Prvním byl nález ze dne 8. 6. 2010, sp. zn. Pl. ÚS 3/09, 219/2010 Sb., kterým jmenovaný soud zasáhl do otázky prohlídek jiných prostor a pozemků dle § 83a odst. 1 trestního řádu. Na tento nález navázalo stanovisko pléna Ústavního soudu ze dne 14. 12. 2010, sp. zn. Pl. ÚS-st 31/10, 426/2010 Sb., řešící jeho intertemporální účinky. Soudkyní zpravodajkou byla v obou právních věcech vyúsťujících nálezem místopředsedkyně Ústavního soudu Eliška Wagnerová.

[39] Srov. rozhodnutí bulharského Nejvyššího správního soudu ze dne 11. 12. 2008, no. 13627. Dostupné z http://blog.veni.com/wp-content/uploads/2008/12/reshenievas-naredba40.pdf. Rozhodnutí kyperského Nejvyššího soudu ze dne 1. 2. 2011, no. 65/2009, 78/2009, 82/2009 και 15/2010-22/2010. Dostupné z http://www.supremecourt.gov.cy/Judicial/SC.nsf/All/5B67A764B86AA78EC225782F004F6D28/$file/65-09.pdf

[40] Hungarian Data Retention Law – challenged at the Constitutional Court. EDRi. Vydáno 4. 6. 2008. Dostupné z http://www.edri.org/edrigram/number6.11/hungary-data-retention-constitutional. Hungary – Privacy Profile. Dostupné z https://www.privacyinternational.org/article/hungary-privacy-profile. Poland – Privacy Profile. Dostupné z https://www.privacyinternational.org/article/poland-privacy-profile#_ftnref.

vy zabezpečení uchovávání údajů, 2/ účelové vázanosti zpřístupnění a použití údajů, 3/ transparentnosti procesu zpřístupnění a použití údajů (dané informováním subjektu údajů) a 4/ právní (soudní) ochrany subjektů údajů. Na sporná místa z hlediska testu proporcionality poukázal Jiří Herczeg, který úpravě hlásící se k DRD vytkl, že 1/ slouží k odhalování „běžné" kriminality (čímž jde nad rámec DRD), 2/ je neefektivní, 3/ opomíjí hledisko subsidiarity, 4/ nezakotvuje informační povinnost a následnou soudní kontrolu, 5/ porušuje zásadu presumpce neviny a 6/ nezajišťuje ochranu důvěrné komunikace.[41] Jak posléze vyšlo najevo, uvedené doktrinární stanovisko není vzdáleno kritériím, která shledal za podstatná Ústavní soud České republiky.

4. Transpoziční úpravy v testu proporcionality

4.1 Hodnoty, k jejichž ochraně vnitrostátní úpravy směřují, vhodnost a potřebnost předmětných úprav

DRD i transpoziční úpravy odkazují na *hodnoty* uznané primárním právem EU, resp. vnitrostátními ústavněprávními normami, a sice veřejný pořádek a bezpečnost. Podle judikatury ESD v oblasti základních svobod lze veřejný pořádek a bezpečnost uplatnit jen při existenci skutečné a dostatečně závažné hrozby, kterou je dotčen základní zájem společnosti. Existenci takto kvalifikovaného zájmu požadují například rozsudky ze dne 29. 4. 2004, Orfanopoulos a Oliveri (C-482/01 a C-493/01, Recueil, s. I-5257, bod 66), k volnému pohybu osob, resp. ze dne 14. 3. 2000, Eglise de scientologie (C-54/99, Recueil, s. I-1335, bod 17), k volnému pohybu kapitálu.[42] Uvedené hledisko se promítá do DRD, která – na rozdíl od některých transpozičních vnitrostátních úprav – uvažuje pouze o závažných trestných činech.[43]

Úpravu lze – ve smyslu testu proporcionality – pokládat za *vhodnou*, pokud její cíl ztotožníme s bojem proti trestné činnosti páchané za využití „standardních" elektronických komunikačních prostředků.[44] Účinné retenci se ovšem lze vyhnout, a to s využitím běžných technologií, přičemž s výjimkou kriminality „neplánovité" či jinak „nekvalifikované" bude jejich využití typické.[45] Peter Fairbrother popisuje některé metody, jak ztížit elektronické sledování.[46] Upozorňuje například, že „obezřetní" drogoví dealeři zákazníkům nevolají ze svého mobilního telefonu, ale z veřejných telefonních automatů, a naopak.[47] Samozřejmostí je též časté obměňování mobilních telefonů a předplacených SIM karet. E-mailová komunikace může být uskutečněna např. s pomocí remailerů nebo onion routingu. Do úvahy přichází použití kryptografických metod, včetně steganografie. Fairbrother též připomíná selhání elektronického sledování při úsilí dopadnout Usámu bin Ládina (paradoxně jeho úkryt vyvolal podezření zřejmě též absencí připojení k elektronickým komunikačním sítím), resp. některé případy z Blízkého východu nebo atentát v severoirském městu Omagh, kdy telekomunikační údaje nepostačovaly k odsouzení jeho strůjce.[48] Je tedy otáz-

[41] HERCZEG, Jiří: Ústavněprávní limity monitoringu telekomunikačního provozu: konflikt mezi bezpečností a svobodou. *Bulletin advokacie.* 2010, č. 5, s. 31.

[42] Rozsudek ESD ze dne 29. 4. 2004 ve spojených věcech C-482/01 a C-493/01 Georgios Orfanopoulos and Others a Raffaele Oliveri v Land Baden-Württemberg. Dostupné z http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62001J0482:EN:HTML. Rozsudek ESD ze dne 14. 3. 2000, C-54/99, Association Eglise de scientologie de Paris and Scientology International Reserves Trust v The Prime Minister. Dostupné z http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:61999J0054:EN:HTML.

[43] Rovněž hledisko obsažené v DRD bylo předmětem kritiky ze strany WP29. European Data Protection Authorities find current implementation of data retention directive unlawful. Dostupné z http://ec.europa.eu/justice/policies/privacy/news/docs/pr_14_07_10_en.pdf Je ovšem diskutabilní, nakolik může DRD tuto problematiku spadající do sféry trestního práva blíže harmonizovat.

[44] Není pochyb, že tyto komunikace jsou způsobilým nástrojem páchání trestné činnosti – podobně jako např. dopravní prostředky a mnoho dalších lehce dostupných a každodenně používaných předmětů.

[45] Snadno „dohledatelná" komunikace bude používána zejména k vytváření „falešných" stop.

[46] FAIRBROTHER, Peter: Defeating traffic analysis. Dostupné z http://www.apcomms.org.uk/apig/archive/activities-2002/data-retention-inquiry/written-evidence-for-the-data-retention-inquiry/fairbrother.pdf.

[47] V české právní praxi drogové delikty představují nejpočetnější skupinu případů (v roce 2009 šlo o 32,8%), kde se úkony podle § 88 tr. řádu uplatňují. Efektivita odposlechů a sledování telekomunikačního provozu je vysoká, statistiky uvádějí souhrnný údaj 74%.V podrobnostech srov. Centrála informatiky a analytických procesů SKPV. Odbor analytických procesů. Analýza odposlechů a sledování osob a věcí dle trestního řádu za rok 2009. Příloha k č. j. PPR-1006-36/ČJ-2010-0099TA. s. 56, s. 69 a násl. Údaj o účinnosti těchto metod je značně odlišný od informace pocházející ze Spolkové republiky Německo, kde jde o cca 17% případů, ALBRECHT, Hans-Jörg, ARNOLD, Harald; DEMKO, Daniela; BRAUN, Elisabeth et al.: Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen, Freiburg 2003, s. 455 a násl. Dostupné z http://www.beck.de/rsw/upload/Beck_Aktuell/Abschlussbericht_1_1.pdf

[48] Ovšem i tito „profesionálové" mohou učinit chybu, která je využitelná bezpečnostními složkami. Zkušenosti s útoky v Madridu dne 11. 3. 2004 ukazují na odlišný problém, kdy

ka, zda kritérium vhodnosti není splněno jen proto, že DRD – resp. některé vnitrostátní úpravy včetně derogované české – se vyznačují poměrně širokým záběrem trestné činnosti, na kterou je lze aplikovat. Pokud by se normy zaměřily jen na mezinárodní organizovaný zločin a terorismus, výsledná bilance navazujících úkonů by byla ještě spornější. Tím se ovšem závěr o vhodnosti úpravy dle DRD značně oslabuje.[49] Diskutabilní však zůstává, nakolik je výběr těchto extrémních případů reprezentativní z hlediska hodnocení legitimity DRD. Pokud by byly „sledovací" aktivity na bázi DRD (označované též coby soft surveillance – „měkký dohled", neboť údajně nikdo není k elektronické komunikaci nucen) zakázány, není vyloučeno jejich částečné přesunutí do většího „přítmí", kde by se jejich výsledky staly procesně nepoužitelné, ale zpravodajsky vytěžitelné.[50]

Úprava postrádá *potřebnost*, pokud lze zákonodárcem sledovaného účelu dosáhnout alternativními normativními prostředky. Existuje-li prostor pro výběr, je ústavně konformní ten z regulačních mechanismů, který danou ústavně chráněnou hodnotu omezuje v míře nejmenší (jde o subsidiaritu). Hledisko potřebnosti obstojí, pokud jde o povinnost uchovávat údaje podle DRD, neboť bez uchovávání údajů nesporně je vyloučeno jejich pozdější vyžádání. Jistou náhradu znamená tzv. data freezing, kdy dochází k rozhodnutí o zahájení sledování údajů konkrétní osoby do budoucna.[51] Tento prospektivní a adresný postup je ovšem variantou dosti vzdálenou, s odlišným potenciálem ohrožovat lidská práva, ale též napomáhat boji proti trestné činnosti.

Potřebnost je nutné hodnotit i co do vymezení trestné činnosti, k jejíž eliminaci má úprava směřovat, a přístupu státních orgánů k údajům. Tato problematika nicméně dopadá spíše do oblasti proporcionality v užším slova smyslu. Subsidiarita se projevuje i kritériem použití úpravy jen v situaci, kdy nelze sledovaného účelu dosáhnout jinak nebo bylo-li by jinak jeho dosažení podstatně ztížené (srov. § 88 odst. 1 českého trestního řádu); klade – nemá-li být jen formální zárukou – nezanedbatelné nároky na předvídavost rozhodujícího soudce, který může nanejvýše spekulovat, jaké poznatky budou z uchovávaných údajů zjištěny, resp. jaké důkazy budou získány orgány činnými v trestním řízení z jiných pramenů.

4.2 Proporcionalita v užším smyslu

a) Časová rovina uchovávání údajů

Ohledně proporcionality v užším smyslu (z argumentačního instrumentaria Spolkového ústavního soudu se nabízí též pojem příkaz k optimalizaci) stojí za zaznamenání propočty relativní četnosti využití blanketně uchovávaných údajů. Již v období před schválením DRD stoupenci i kritici úpravy předestírali vlastní bilance. Uveřejněný odhad předpokládá, že během dvouletého období bude využito jen asi 0,2% z těchto dat pro důkazní účely a z nich 90% bude vyžádáno během prvního měsíce po vzniku údajů. Je tedy patrné, že 99,98% údajů bude zbylých 23 měsíců uchováváno zbytečně a s rizikem zneužití.[52] Další dostupná kalkulace vycházející z britských bezpečnostních složek (a formulující odlišný závěr) udává, že 95% žádostí bude v případě méně závažné kriminality vzneseno během prvních tří měsíců a ostatních 5% zpravidla do 12 měsíců, u závažné nebo organizované trestné činnosti bude asi 85% žádostí uplatněno v období do 24 měsíců po vzniku údajů, v důsledku čehož se doporučuje uchovávat údaje po dobu 5 let.[53] Dříve se uvádělo, že

bezpečnostní složky měly k dispozici zpravodajské informace, zčásti pocházející z odposlechů, nicméně k odvrácení nebezpečí nepostačovaly, neboť jim nebyla věnována náležitá pozornost. Ve zmiňovaném případě šlo o problém související s jazykovou bariérou.

[49] Výše učiněná poznámka o dopravních prostředcích je uplatnitelná též k námitce, že DRD je nesystémová, neboť všeobecné sledování pohybu vozidel, vytvoření databáze DNA zahrnující vzorky celé populace či označení osob, u nichž lze předpokládat zvýšené riziko, že se stanou obětí trestné činnosti, RFID chipy by k prevenci nebo objasňování trestné činnosti přispělo zřejmě ve větší míře; vzniku těchto druhů „stop" lze totiž obtížněji předcházet. Naznačované rozšíření databází dostupných státním orgánům by však znamenalo postupnou orwellizaci společnosti.

[50] Nelze přehlédnout ani americké monitorovací systémy, jakými jsou Carnivore, Echelon, Terrorism Information Awareness, Novel Intelligence from Massive Data či Glass Box (a případně další, veřejnosti neznámé) nebo britský Interception Modernisation Programme. Kontrola elektronické komunikace je ovšem charakteristická i pro řadu dalších významných států.

[51] Srov. Úmluvu o počítačové kriminalitě z roku 2001, který v čl. 16 a 17 pojednává o urychleném uchování (conservation) provozních údajů po dobu nejvýše 90 dnů (čl. 16 odst. 2), a to na základě příkazu příslušného státního orgánu.

[52] Srov. článek vycházející z předpokladu, že doba uchování údajů bude dokonce 3 roky. Invasive, Illusory, Illegal, and Illegitimate: Privacy International and EDRi Response to the Consultation on a Framework Decision on Data Retention. Vydáno 15. 9. 2004. Dostupné z www.privacyinternational.org/issues/terrorism/rpt/responsetoretention.html K dispozici je ovšem číslo ještě nižší, podle kterého jen 1 z 250.000 údajů je posléze vyžadován bezpečnostními složkami UHE, Bianca, HERRMANN, Jens: Überwachung im Internet – Speicherung von personenbezogenen Daten auf Vorrat durch Internet Service Provider, 18. 08. 2003, Dostupné z www.ig.cs.tu-berlin.de/oldstatic/da/2003-08/UheHerrmann-Diplomarbeit-082003.pdf, s. 161.

[53] NCIS Submission on Communications Data Retention Law. Roger Gaspar. Looking to the Future. Charity on Communications Data Retention Law. Submission to the Home Office for Legislation on Data Retention. Bod 6. 1. 1. Dostupné z

pro obchodní účely je jen výjimečně zapotřebí uchovávat provozní údaje po dobu delší než 3 měsíce.[54] Nyní je tato „potřebnost" dále relativizována tím, že internetové připojení není hrazeno podle jeho skutečné délky, nýbrž paušálně.[55]

Vedení odpovídajících statistik předepisuje čl. 10 DRD. Čl. 14 DRD ukládá Komisi předložit Evropskému parlamentu a Radě do 15. 9. 2010 hodnocení používání této směrnice a jejího dopadu na hospodářské subjekty a spotřebitele. K dané problematice byla dne 3. 12. 2010 v Bruselu pořádána konference, kde ovšem nedošlo ke zveřejnění bližších statistických údajů, a to s vysvětlením, že členské státy nepředaly odpovídající podklady.[56] Výsledky setkání představovaly pro kritiky DRD zklamání též proto, že její opodstatněnost uznali někteří z dosavadních odpůrců úpravy v Evropské komisi.

Zjištění, že se procentuelní podíl využitelných údajů limitně blíží nule, by samozřejmě nasvědčoval tomu, že test proporcionality není splněn. Bylo by proto vhodné zvážit zkrácení období uchovávání údajů.[57] Z těchto odhadů ovšem vybočuje praxe, kdy v České republice počet žádostí o poskytnutí provozních a lokalizačních údajů výrazně překračuje hranici sto tisíc ročně.[58] Jde přibližně o desetinásobek případů oproti Spolkové republice Německo.[59] Toto zjištění by mělo směřovat k omezení uplatňování uvedeného procesního nástroje. Statistiky dokládající nízkou relativní četnost údajů využitelných v trestním řízení ovšem nevyzní většině veřejnosti coby přesvědčivé, pokud se vyskytují dlouhodobě neobjasněné případy závažné kriminality. Na druhou stranu, jiné zúžení uchovávání než časové by nebylo uskutečnitelné, pakliže setrváme na požadavku (byť nikoli absolutizovatelného) zákazu hodnocení obsahu komunikace. S dobou uchovávání údajů souvisí též otázka nákladů těchto opatření.[60] Ty ponesou buď daňoví poplatníci (pakliže státní orgány budou poskytovatelům zvýšené výdaje nahrazovat), nebo klienti (a to nejen přímo v ceně služeb, ale i dalším omezením soukromí, neboť jejich poskytovatelé budou shromážděné údaje zpracovávat, kupř. ke zmapování zákaznického chování). Prozatím nejsou k dispozici důkazy, že nová legislativa má dopady do tržní struktury vyvolané tím, že ne všichni poskytovatelé služeb jsou schopni se s jejími ekonomickými důsledky vyrovnat ve stejné míře.[61] Patří se dodat, že z časového ohraničení uchovávání údajů vyplývá nutnost odpovídajících záruk jejich následného nevratného výmazu.

b) Obsah komunikace

Konstatování vtělené do DRD v čl. 1 odst. 2 nelze považovat za záruku, že obsahová stránka komunikace zůstane nepřístupná. Z některých provozních údajů (typicky z URL) je možné obsah komunikace „rekon-

http://www.cryptome.org/ncis-carnivore.htm. Citovaný dokument vydala britská National Crime Intelligence Service, do sdělovacích prostředků „unikl" v prosinci 2000 a byl považován za kontroverzní. Tímto materiálem se přímo inspirovala legislativa přijímaná po 11. 9. 2001. Srov. A new blow to our privacy. Dostupné z http://www.guardian.co.uk/technology/2002/jun/06/onlinesupplement.privacy. Obdobná problematika byla nicméně ještě před zmiňovaným teroristickým útokem projednávána v rámci G-8. G8 Government-Private Sector Hihg-Level Meeting on High-Tech Crime Tokyo, May, 22-24, 2001, Report for Workshop 1: Data Retention Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers. Dostupné z http://www.mofa.go.jp/policy/i_crime/high_tec/conf0105-4.html.

[54] NCIS Submission on Communications Data Retention Law. Roger Gaspar. Looking to the future. Charity on Communications Data Retention Law. Submission to the Home Office for Legislation on Data Retention. Bod 3. 1. 1. Dostupné z http://www.cryptome.org/ncis-carnivore.htm

[55] Služba označovaná jako neomezené připojení k internetu.

[56] Srov. Taking on the Data Retention Directive. Data Retention Conference, 3 December 2010, Brussels. Dostupné z http://www.dataretention2010.net/files/discussion_paper_for_the_DRD_Conference_of_3_December_2010.pdf

[57] Zkrácení období považuje za vhodnou možnost WP 29. European Data Protection Authorities find current implementation of data retention directive unlawful. Dostupné z http://ec.europa.eu/justice/policies/privacy/news/docs/pr_14_07_10_en.pdf.

[58] Nález Ústavního soudu cituje následující prameny: The Evaluation of Directive 2006/24/EC and National Measures to Combat criminal Misuse and Anonymous Use of Electronic Data",. Dostupné z http://www.dataretention2010.net/docs.jsp. HERCZEG, Jiří: Ústavněprávní limity monitoringu telekomunikačního provozu: konflikt mezi bezpečností a svobodou. *Bulletin advokacie.* 2010, č. 5, s. 29.

[59] Report of the Data Retention Conference, 'Towards the Evaluation of the Data Retention Directive', Brussels, 14 May 2009. Brussels, 6 July 2009 JLS F3/JV D(2009) 9330 – rev 2., s. 10.

[60] Technologie uchovávání velkého objemu dat (příkladem může být sortiment společnosti Teradata) se ovšem postupně stávají cenově dostupnějšími (srov. Moorův zákon).

[61] Pokud by byly údaje uchovávány centrálně, byly by provozní náklady srovnatelné s národní databází DNA. NCIS Submission on Communications Data Retention Law. Roger GASPAR. Looking to the future. Charity on Communications Data Retention Law. Submission to the Home Office for Legislation on Data Retention. Bod 6. 6. Dostupné z http://www.cryptome.org/ncis-carnivore.htm. Rozbor ekonomických dopadů blanketního uchování údajů obsahuje článek DANEZIS, Georgie; WITTNEBEN, Bettina: The Economics of Mass Surveillance and the Questionable Value of Anonymous Communications. (2006) Proceedings of the 5th Workshop on The Economics of Information Security, Springer. Tento text dochází ke kritickým závěrům, podle nichž dohled omezí soukromí osob, které se protiprávního jednání nedopustily, zatímco nalezení delikventů bude přinejmenším nákladné.

struovat“. Odborník v oblasti práva informačních technologií Ian Walden se vyslovil, že lokalizační a provozní údaje odhalují o osobním životě jednotlivce tolik, co samotný obsah komunikace.[62] V případě zpřístupnění obsahu sdělení jde přitom o závažný zásah do soukromí. Udržitelnost citovaného výroku je závislá na souvislostech komunikace. Význam čl. 1 odst. 2 DRD není namístě přeceňovat, neboť platí, že pokud vyžadující orgán činný v trestním řízení obsah procesně regulérním způsobem zachytil a z těchto údajů byly zjištěny další skutečnosti, nebude čl. 1 odst. 2 DRD mít před soudem praktické důsledky.[63] Spolkový ústavní soud rozlišil mezi použitím uchovávaných údajů přímým a nepřímým (např. ztotožnění osoby, které byla přidělena určitá IP adresa), u kterého postačují slabší právní záruky.

I kdyby orgány s pravomocí získat uchovávané údaje neměly přístup k obsahu sdělení, kterého se tyto údaje týkají, bez dopadů do oblasti soukromí nemusí být ani zjištění samotné komunikace.[64] Závažnější důsledky bývají spojovány se sledováním delšího časového úseku, z nějž lze vytvořit celkový profil jednotlivce, zahrnující řadu citlivých údajů a umožňující v nezanedbatelné míře předvídat jeho chování.[65] Odpovídající argument uznal Spolkový ústavní soud konstatováním, že lze takto sestavit detailní údaje o společenské nebo politické příslušnosti, jakož i osobních zálibách, sklonech nebo slabostech jednotlivých osob.

Z hlediska věcného dosahu sledování komunikace není bez významu, že Pracovní skupina zřízená podle čl. 29 směrnice 95/46/ES přijala extenzívní výklad pojmu osobní údaj, který zahrnuje – mimo jiné – dynamické IP adresy.[66] Lze zdůraznit, že do dosahu DRD nespadají bez dalšího údaje ze sociálních sítí; je nutné konkrétní posouzení aplikovatelnosti úpravy.[67]

c) Osobní dosah uchovávání údajů

Spolkový ústavní soud se negativně vyslovil k ústavnosti uchovávání údajů bez rozlišení účastníků komunikace. Konstatoval, že je třeba vymezit „velmi úzký okruh telekomunikačních spojení“, který by obecnému režimu uchovávání údajů nepodléhal; mělo by se jednat o komunikaci osob, úřadů nebo organizací působících v sociální nebo církevní oblasti, které poskytují osobám zůstávajícím v anonymitě převážně nebo výhradně telefonické poradenství a pomoc v psychické nebo sociální nouzi, a které jsou vázány mlčenlivostí. Odůvodnění Spolkového ústavního soudu lze pokládat za přesvědčivé, přesto stojí za zaznamenání, že v případě nábožensky motivovaného terorismu nalézajícího zázemí v síti institucí provozujících hlavní činnost v sociální oblasti může být tento ústavněprávní požadavek snadno zneužit k obejití DRD. Není přitom pochyb, že síla tohoto systému odpovídá parametrům jeho nejslabšího článku. Současně nelze přehlédnout, že možností, jak DRD obejít, je řada (viz shora), a námitkou „zneužitelnosti“ lze zpochybnit praktické jakékoliv normativní řešení.

---

[62] Dr Ian Walden Evidence. APIG Communications Data Inquiry Oral Evidence 11. 12. 2002. Dostupné z http://www.apcomms.org.uk/apig/archive/activities-2002/data-retention-inquiry/oral-evidence-for-the-data-retention-inquiry/dr-ian-walden-evidence.html

[63] Srov. technické problémy Policie ČR se zjišťováním obsahu internetové telefonie prostřednictvím sítě Skype. Lze doplnit, že další technologií, která vyvolala zájem bezpečnostních složek kvůli ztíženému přístupu ke komunikaci, je smartphone BlackBerry, který byl v některých státech Blízkého východu z tohoto důvodu zakázán. Stejnou hrozbu opakovaně uplatňuje Indie. Za připomenutí stojí též causa, kdy se BIS snažila „přimět“ ke spolupráci společnost CircleTech, která vyvíjí šifrovací software pro mobilní telefony (jde o volání přes internet, a nikoli „standardní“ hovor přes síť GSM). Zde ovšem byl ve hře obsah komunikace, a nikoli „jen“ provozní a lokalizační údaje. Celkově však lze konstatovat, že Česká republika patří mezi státy s liberálním přístupem k šifrovacím technologiím (srov. omezení používání programu PGP).

[64] Resp. jejího místa, srov. např. software Google Latitude nebo celou řadu dalších aplikací a služeb mobilních operátorů pro lokalizaci mobilních telefonů.

[65] EAGLE, Nathan; PENTLAND, Alex Sandy. Eigenbehaviors: Identifying Structure in Routine. *Behavioral Ecology and Sociobiology*. 2009, no. 63, s. 1057–1066. Dostupné z http://reality.media.mit.edu/pdfs/eigenbehaviors.pdf.
K uvedenému srov. http://reality.media.mit.edu/user.php nebo http://reality.media.mit.edu/dyads.php. Předmětné studie se týkaly typového určení sociálních vazeb na základě sledování pohybu osob s mobilními telefony s funkcí bluetooth. Dosažená úspěšnost se pohybovala v rozpětí 90-95 %. Studie je analyzována též v článku EAGLE, Nathan; PENTLAND, Alex Sandy; LAZER, David. Inferring friendship network structure by using mobile phone data. Proceedings of the National Academy of Sciences, Vol. 106, No. 36. (8 August 2009), pp. 15274–15278. Dostupné z http://www.pnas.org/content/early/2009/08/14/0900282106.full.pdf+html. Za bližší pozornost nepochybně stojí studie EAGLE, Nathan. Machine Perception and Learning of Complex Social Systems. 2005. Dostupné z reality.media.mit.edu/pdfs/thesis.pdf. K uvedenému srov. pojem reality mining, který znamená shromažďování a analýzu elektronických dat získávaných z prostředí a vztahujících se k sociálnímu chování, a to s cílem identifikovat předvídatelné vzorce chování. Jde o druh analýzy elektronických stop. K ekonomickému využití srov. HESSEILDAHL, Arik. There's Gold in 'Reality Mining'. Dostupné z http://www.businessweek.com/technology/content/mar2008/tc20080323_387127.htm.

[66] Article 29, Data Protection Working Party (2007). *Opinion 4/2007 on the concept of personal data*. Brussels. Dostupné z http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

[67] Report of the Data Retention Conference, ‘Towards the Evaluation of the Data Retention Directive’, Brussels, 14 May 2009.Brussels, 6 July 2009 JLS F3/JV D(2009) 9330 – rev 2., s. 2.

Německý Spolkový ústavní soud a Ústavní soud České republiky se nezabývaly detailněji otázkou profesního tajemství lékaře, advokáta apod.[68] Lze však mít za to, že v případě komunikace mezi obhájcem a obviněným by měl platit nejen zákaz odposlechu a záznamu telekomunikačního provozu (výslovně uznaný v § 88 odst. 1 tr. řádu), ale též přístupu k blanketně uchovávaným údajům. Obdobná hlediska by se měla uplatnit i v případě komunikace mezi lékařem a pacientem.

Složitější situace nastane v souvislosti s právem novináře na ochranu zdroje již proto, že nelze jednoznačně zodpovědět otázku, kdo je novinář. Určité řešení se podává z konstatování, že svoboda projevu náleží každému, pročež by se nemělo přihlížet k „formálnímu" profesnímu zařazení konkrétní osoby.[69] Toto pojetí by ovšem zásadně zúžilo prostor pro aplikaci DRD a navazujících úprav. Měl by mít zaručeno preferenční zacházení např. přispěvatel extrémistického blogu? Příklad podezření z neoprávněného použití blanketně uchovávaných údajů nalezneme v Polsku, kde v období let 2005–2007 tajná služba sledovala mobilní telefony desítky novinářů ve snaze odhalit informátory investigativních reportáží, které se týkaly místní politické scény.[70] Paradoxní rozměr získává kauza okolností, že DRD byla do polského právního řádu implementována až v roce 2009.

d) Místo uchovávání údajů

Podle DRD údaje uchovávají poskytovatelé veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí, od nichž si je vyžádají oprávněné státní orgány. Britský ministerský předseda Gordon Brown prosazoval změněnou národní úpravu počítající s uchováváním předmětných údajů v centralizované státem spravované databázi.[71] Vytvoření této databáze by znamenalo, že případný únik dat bude mít větší rozsah než tehdy, děje-li se z databází poskytovatelů. Byť zajisté není technicky nemožné kontrolovat, které údaje byly použity, české zkušenosti s úniky informací z vyšetřovacích spisů, které prakticky bez výjimky zůstaly neobjasněny, podporují kritiku tohoto řešení.

Z hlediska lokalizace údajů je podstatné, že prozatím vyvolává výkladové pochybnosti otázka aplikovatelného práva, kdy DRD považuje za určující, ve kterém státě byly údaje vytvořeny, zatímco směrnice 95/46/ES obsahuje pravidla složitější a ne vždy s DRD kompatibilní. Výkladové problémy by mohla vytvářet kupř. situace, kdy jsou údaje uchovávány v jiném státě než v tom, ve kterém vznikly, a to zejména tehdy, pokud jsou v obou státech zakotveny rozdílné lhůty uchovávání údajů.

e) Závažnost trestného činu

Jak bylo předznačeno, DRD – ve shodě s vnitřní logikou judikatury ESD – spojuje přístup státních orgánů k uchovávaným údajům s trestněprávní ochranou společenských zájmů zvláštního významu. V tomto směru pochybil jak zákonodárce německý, tak i český.

Spolkový ústavní soud shledal – s poukazem na princip proporcionality – ústavněprávní deficit v ustanovení § 100g StPO, neboť připouští použití údajů tehdy, je-li závažnost trestného činu značná nebo v případě jeho spáchání prostřednictvím telekomunikací. Materiální hledisko „závažnosti" trestného činu není blíže vymezeno, zákon neobsahuje taxativní výčet předvídaných trestných činů a nenaznačuje se ani, zda je třeba hodnotit závažnost obecně nebo v návaznosti na jednotlivé případy. Trestné činy páchané prostřednictvím telekomunikací zákon nerozlišoval. Spolkový ústavní soud poskytl zákonodárci vodítko, že státní orgány mohou být oprávněny k využívání předmětných údajů jen na podkladě důvodného podezření ze spáchání závažného trestného činu, a to pouze při dostatečném doložení rozhodných skutečností, kterými jsou existence konkrétního ohrožení fyzické integrity, života nebo svobody určité osoby, celistvosti nebo bezpečnosti spolku nebo spolkové země nebo odvrácení obecného ohrožení. Bližší vymezení skutkových podstat ponechal Spolkový ústavní soud na zákonodárci.

Ústavní soud České republiky zákonodárci vytkl, že ústavněprávně nepřípustně umožnil zpřístupnění uchovávaných údajů bez rozlišení závažnosti trestného činu (odst. 47–49 nálezu). V českém trestním řádu je pro „starší" institut odposlechu a záznamu telekomunikačního provozu (§ 88 tr. řádu) zaručen vyšší stupeň ochrany lidských práv než v souvislosti se zpřístupněním uchovávaných údajů podle § 88a téhož zákona. § 88 trestního řádu se totiž vztahuje na zvlášť závažný zločin nebo jiný úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva. Vzhledem k petitu návrhu Ústavní soud nepřistoupil k derogaci § 88a tr. řádu, nýbrž k apelu na zákonodárce, aby jeho text upra-

[68] K otázce předvídatelnosti obsahu zákonné normy a odposlechu hovoru mezi advokátem a jeho klientem (tj. „privilegované komunikace") srov. rozsudek ESLP ze dne 25. 3. 1998 ve věci Kopp v. Švýcarsko, stížnost č. 23224/94, resp. ze dne 20. 6. 2000 ve věci Foxley v. Spojené království, stížnost č. 33274/96.

[69] K nedořešené problematice vztahu mezi ochranou soukromí a svobodou projevu lze poukázat na rozsudek ESD ze dne 16. 12. 2008, C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy a Satamedia Oy.

[70] Journalists' Phones Monitored in Politically Inspired investigation? Thenews.pl, 8 October 2010,. Dostupné z http://www.thenews.pl/national/artykul141157_journalists-phones-monitored-in-politically-inspired-investigation.html.

[71] UK Government will store all phone, Internet traffic data. EDRi. Vydáno 21. 5. 2008. Dostupné z http://www.edri.org/edrigram/number6.IO/uk-isp-trafficdata

vil ve smyslu nosných důvodů nálezu. Vhodným vzorem je právě ustanovení § 88 tr. řádu.

f) Informační povinnost oprávněných orgánů[72]

Povinnost státního orgánu informovat monitorovanou osobu o vyžádání jejích blanketně uchovávaných údajů nemohla být harmonizována na podkladě čl. 95 Smlouvy o ES, a tedy úprava DRD neřeší otázku, jak se účastník komunikace dozví, že údaje byly předány. Z DRD však nevyplývá ani povinnost zákonodárce omezit právo na přístup k informaci o provedeném šetření. Pokud vnitrostátní úprava tyto limity „aktivisticky" stanoví, nemůže se zaštiťovat právem EU a hrozí kolize s judikaturou ESLP, který ve věci Klass v. Spolková republika Německo v souvislosti s problematiku odposlechů konstatoval obecnou – byť nikoli bezvýjimečnou – informační povinnost.[73] Judikatura evropských soudů ovšem samotné odposlechy telefonů nediskvalifikuje pouhým poukazem na skutečnost, že jimi monitorovaná osoba očekávala, že komunikace zůstane utajena.[74] V této souvislosti stojí za zmínku diskuse v americkém právním prostředí týkající se legality důkazů získaných odposlouchávacími zařízeními, které byly v soukromých prostorách rozmístěny utajeně.[75]

Spolkový ústavní soud dal najevo, že režim DRD je srovnatelný se situací předvídanou ve zmiňovaném rozsudku Klass v. Spolková republika Německo tím, že zákonodárci uložil, aby zakotvil pravidlo dodatečného vyrozumění subjektu údajů o předání údajů (s přípustnými – avšak restriktivně vykládanými – omezeními). Předem bude o poskytnutí údajů jejich subjekt zpraven jen tehdy, nedošlo-li by tímto postupem ke zmaření účelu vyšetřování. Obdobná hlediska ústavněprávního přezkumu uplatnil též Ústavní soud České republiky. Informování zájmové osoby představovalo chronický problém v souvislosti s odposlechy a záznamy telekomunikačního provozu; k jeho vyřešení došlo až vtělením odpovídající právní úpravy do § 88 odst. 8 a 9 tr. řádu, a to s účinností ode dne 1. 7. 2008 (zákon č. 177/2008 Sb.).

Informování subjektu údajů představuje podle Spolkového ústavního soudu prostředek, jak umožnit jednotlivci rozvoj jeho osobnosti a ochránit ho tak před zásahem třetích osob do jeho osobnostních práv, resp. pocitem „difúzní ohroženosti". Prozaičtěji vyjádřeno, příslušné sdělení může být důkazní oporou pro případný soudní přezkum postupu při zprostředkování a použití uchovávaných údajů. Slabou stránkou tohoto systému je kromě vnitřní logiky následné kontroly, která neumožňuje dispozicím s údaji předejít, též okolnost, že nesplní-li státní orgán informační povinnost „dobrovolně", má subjekt údajů jen omezené možnosti skutečný stav si ověřit. Nedostatečný prostor pro soukromoprávní iniciativu § 88 českého tr. řádu usiluje vyrovnat v první řadě dohledem ze strany soudu, který sdělení údajů nařídil.

5. Závěr

Dosavadní bilance evropských zákonodárců na poli ústavněprávního přezkumu jejich transpozičních úprav prima facie není příznivá. Nejde se však o vývoj překvapivý, neboť se jedná o legislativu poměrně netradiční, resp. dopadající do složitého a rychle proměnlivého terénu, který bývá formován značnými bezpečnostními riziky. Ačkoli nepřevažuje „antisystémová" kritika zásad DRD, zákonodárci bývají výsledky těchto soudních řízení uváděni do nikoli snadné pozice, a to tím spíše, pokud se předmětná úprava ruší již uveřejněním rozhodnutí ústavního soudu, přičemž následuje výmaz údajů. V tomto směru je patrný ustálený rozdílný přístup oproti judikatuře dopadající do oblasti soukromoprávní, vedený požadavkem na zajištění právní jistoty.[76] Žádný z členských států prozatím legislativní proces reagující na nosné důvody soudních rozhodnutí, která zpochybnila ústavněprávní udržitelnost transpozičních úprav, nedokončil; „výjimku" představuje bulharský zákonodárce, jenž Nejvyšším správním soudem zrušenou právní úpravu začátkem roku 2010 opětovně

[72] Pojem oprávněný orgán je převzat z české implementační úpravy. Není však přesný, neboť státní orgán nevykonává v případě zpřístupnění uchovávaných údajů právo, nýbrž pravomoc.

[73] Viz rozsudek ESLP ze dne 6. 9. 1978 ve věci Klass a ostatní v. Spolková republika Německo, stížnost č. 5029/71. Soud v odstavci 36 připomíná, že tam, kde státní instituce provádějí tajné sledování, jehož existence zůstává kontrolované osobě neznáma, s tím důsledkem, že toto sledování zůstává nezpochybnitelné (pozn. není proti němu k dispozici opravný prostředek), článek 8 Úmluvy by mohl být (co do svého významu) snížen k nicotnosti. Je možné, že by v takovém případě bylo s jednotlivcem zacházeno v rozporu s čl. 8 Úmluvy nebo by dokonce byl práva poskytnutého ve zmíněném článku zbaven, aniž by se o tom dozvěděl, a tedy aniž by mohl dosáhnout nápravy ať již na úrovni národní nebo před orgány Úmluvy. Srovnatelné závěry byly uplatněny v rozsudku ESLP ze dne 7. 7. 1989 ve věci Gaskin v. Spojené království, stížnost č. 10454/83, odst. 38.

[74] K legitimnímu očekávání utajení komunikace srov. rozsudek ESLP ze dne 25. 6. 1997 ve věci Halford v. Spojené království, stížnost č. 20605/92.

[75] DIFFIE, Whitfield; LANDAU, Susan. The politics of wiretapping and encryption Book Excerpt: Privacy on the Line. Dostupné z http://www.computerworld.com/s/article/9023907/The_politics_of_wiretapping_and_encryption?taxonomyId=17&pageNumber=6 BURNHAM, David. Above the Law: Secret Deals, Political Fixes, and Other Misadventures of the U.S. Department of Justice. Scribner, 1996.

[76] Srov. nález Ústavního soudu České republiky ze dne 1. 7. 2010, sp. zn. Pl. ÚS 14/10.

přijal a omezení lidských práv dále prohloubil. Zajímavé bude též sledovat, nakolik se zájem veřejnosti obrátí k uchovávání – mnohdy přesnějších a rozsáhlejších – souborů údajů soukromými subjekty.[77] Lze uvítat, že ESD/SDEU doposud nevychází vstříc snahám zejména zástupců nositelů práv duševního vlastnictví o zajištění si přístupu k údajům uchovávaných pro účely trestněprávní v jejich civilních sporech, nýbrž rozhodování ponechává na členských státech. Další oslabení ochrany soukromí by mohlo přinést – v některých členských státech uvažované – vytváření centrálních státních databází komunikačních údajů.

Summary

The article deals with one of the most controversial European directives – Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC – and its judicial reflections. DRD aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. The first chapter focuses on the principles of DRD. It explains arguments legitimizing this act. The second chapter is entitled "criticism against DRD". The formal criticism concerns the adequacy of the reference to Article 95 EC Treaty. The European Court of Justice did not recognize this opposition in case C-301/06. Polemics against the content of DRD are directed against the weakening of the presumption of innocence. The Court of Justice of the European Union has not so far dealt with this problem. The Romanian Constitutional Court accepted that argument. The third chapter concerns the criticism against the implementation of the DRD by the Member States, represented by the decision of the German Federal Constitutional Court, the Czech Constitutional Court, the Bulgarian Supreme Administrative Court and the Supreme Court of Cyprus. These decisions oppose against the laws of Member States which unreasonably or disproportionately restrict the protection of privacy. The fourth chapter focuses on the proportionality test, respectively the values which the legislation of the Member States protects, its suitability or usefulness and the proportionality in the strict sense. The article highlights the conclusion that these decisions have not been so far implemented in the laws of the Member States. In some cases it can be a difficult task.

[77] Online Focus. Bundesdatenschutzbeauftragter: Google, Facebook & Co. Reglementieren. Online Focus. Dostupné z http://www.focus.de/digital/internet/bundesdatenschutzbeauftragtergoogle-facebook-und-co-reglementieren_aid_487099.html.