1054—1070

Kam jsme se posunuli od zrušení směrnice o uchovávání údajů

Jaroslav Denemark*

Abstrakt: Evropská unie svou snahu chránit základní práva na soukromí a ochranu osobních údajů v době rychlého rozvoje nových komunikačních technologií zvládá vcelku obstojně. Ať už je to evropský normotvůrce nebo Soudní dvůr EU, přístup k unijnímu právu odráží modernitu dnešní doby. Nicméně na poli uchovávání osobních údajů provozovateli telekomunikačních sítí pro účely předání těchto údajů státním orgánům panovaly od dob zrušení směrnice o uchovávání údajů jisté rozpaky. Cílem příspěvku je tak nejen zhodnotit reakce Evropské unie na nové technologické výzvy s ohledem na ochranu soukromí a osobních údajů a zhodnotit jejich vhodnost či efektivitu, ale především odpovědět na otázku, zda dnes máme unijním acquis jasně stanovené mantinely pro vnitrostátní úpravu ochrany osobních údajů.

Klíčová slova: uchovávání osobních údajů, právo na soukromí, lokalizační údaje, právo a moderní technologie

Úvod

Moderní technologie jsou výzvou pro každého normotvůrce. Sledovat jejich vývoj a dostatečně svižně na něj reagovat úpravou legislativy je v případě procesů tvorby práva jednoznačně tématem na pořadu dne. Evropská unie má snahu na výzvy moderních technologií reagovat postupy, jež v sobě zahrnují jak nové právní předpisy, tak judikaturní činnost, která v důsledku nejen napomáhá překlenout období legislativního procesu, ale má též za cíl napomoci nabídnout řešení nových výkladových výzev.

Nejinak je tomu na poli ochrany soukromí a práva na ochranu osobních údajů. Vztah těchto dvou práv k moderním technologiím byl nejednou předmětem mnohých apelů ke změně právního rámce. Prvním aspektem problému k vyčlenění postoje Evropské unie je nutné zodpovězení otázky, zda jsou práva na soukromí a ochranu osobních údajů právy základními.

Teprve poté se lze ptát a odpovědět na otázku, jaký přístup Evropská unie zvolila směrem k těmto právům, a lze do určité míry porozumět tomu, jak se, ať už legislativně, či judikaturou, Evropská unie vypořádala se střetem práva na soukromí a ochranu osobních údajů s jinými právy ve světle moderních technologií. Právě tento unijní postup je totiž tím, co formuje rámec úpravy preventivního uchovávání provozních a lokalizačních údajů o elektronické komunikaci u poskytovatelů telekomunikačních služeb (známe pod anglickým výrazem *data retention*; dále v textu bude použito kratšího slovního spojení „uchovávání údajů“)[1] platné na území pevninské Evropy.

* JUDr. Jaroslav Denemark. Doktorand na katedře evropského práva PF UK. E-mail: jaroslav.denemark@gmail.com. ORCID: https://orcid.org/0000-0002-8304-1312.

1 Toliko po vzoru Ústavního soudu, který sice pro *„preventivní uchovávání provozních a lokalizačních údajů o elektronické komunikaci u poskytovatele telekomunikačních služeb“* používá zkrácené anglické *„data retention“* (nález Pl. ÚS 45/17), v překladu však a v porovnání s názvem dotčené směrnice lze užít české „uchovávání údajů“ (srov. např. bod odůvodnění č. 9 *in fine* směrnice o uchovávání údajů v české a anglické jazykové verzi).

1. Ochrana soukromí a osobních údajů středobodem zájmu

Evropská unie řadí ochranu soukromí a právo na ochranu osobních údajů mezi základní lidská práva. Nasvědčuje tomu nejen systematika předního lidskoprávního katalogu na úrovni Evropské unie, tj. Listiny základních práv Evropské unie, která řadí právo na soukromí a právo na ochranu osobních údajů již do Hlavy II, nadepsané Svobody,[2] ale též přístup institucí Evropské unie k těmto právům.

Soudní dvůr Evropské unie jednoznačně stanovil (a to ještě za hodnotového východiska s ohledem na lidská práva v podobě čl. 8 Evropské úmluvy o ochraně lidských práv),[3] že: *„Právo na respektování soukromého života […] je základním právem chráněným právním řádem Společenství.“*[4] Ochrana osobních údajů je pak vnímána jako právo inherentní právu na soukromí (je jeho integrální součástí) a zásah do osobních údajů je zásahem do soukromí (logicky zde ale neplatí *vice versa*, protože ne každý zásah do soukromí je zásahem do osobních údajů).[5]

Esencí výše uvedeného budiž čtenáři tohoto pojednání první věta prvního recitálu nařízení Evropské unie s populárním označením „GDPR“, a to konkrétně: *„Ochrana fyzických osob v souvislosti se zpracováním osobních údajů je základním právem.“*[6]

Je tedy bez dalších pochyb zřejmé, že nejen právo na soukromí, ale i právo na ochranu osobních údajů je v rámci unijního *acquis* považováno za základní lidské právo a jako takové musí být v případě střetu s dalšími lidskými právy považováno. Přesto je třeba mít na paměti, jak už to u základních práv bývá, že právo na ochranu soukromí, ani právo na ochranu osobních údajů není právem absolutním.[7, 8]

Evropská unie si uvědomuje extrémní důležitost sofistikované a komplexní ochrany osobních údajů nejen směrem k naplnění ochrany jednoho z moderních základních lidských práv, ale též k naplnění principu, na kterém je Evropská unie vystavena – volném pohybu osobních údajů.[9] Trh s osobními údaji nabývá na čím dál větší síle a důležitosti[10] a ne nadarmo se říká, že osobní údaje jsou již více cenné než ropa.[11] Je tedy nutné k osob-

---

2 Listina základních práv Evropské unie, konsolidované znění z roku 2012 (2012/C 326/02), Úř. věst. 326/391, 26. 10. 2012, Článek 7 „Respektování soukromého a rodinného života“ a článek 8 „Ochrana osobních údajů“.

3 Evropská úmluva o ochraně lidských práv ve znění Protokolů č. 11 a 14 s Protokoly č. 1, 4, 6, 7, 12, 13 a 16.

4 Rozhodnutí Soudního dvora Evropské unie ze dne 8. dubna 1992, C-62/90 *Komise v. Německo*, ECLI:EU:C:1992:169.

5 Např. rozhodnutí Soudního dvora Evropské unie ze dne 13. května 2014, C-131/12 *Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Coteja Gonzáles*, ECLI:EU:C:2014:317 (*Google v. Spain*), bod 80.

6 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), Úř. věst. l. 119/1, 4. 5. 2016, recitál č. 1. (dále jen jako „GDPR“).

7 Ibidem, recitál č. 4.

8 V judikatuře typicky obecně k tomu, že žádná základní práva, až na právo na život a zákaz mučení a nelidských či ponižujících trestů nebo zacházení, nejsou absolutní, uvádí autor tohoto pojednání rozhodnutí Soudního dvora Evropské unie ze dne 12. června 2003, C-112/00, *Eugen Schmidberger, Internationale Transporte und Planzüge proti Rakouské republice*, ECLI:EU:C:2003:333, bod 80, konkrétně k neabsolutní povaze práva na soukromí a ochranu osobních údajů pak např. rozhodnutí Soudního dvora Evropské unie ze dne 9. listopadu 2010, C-92/09 a C-93/09, *Volker und Markus Schecke GbR, Hartmut Eifert proti Land Hessen za přítomnosti Bundesanstalt für Landwirtschaft und Ernährung*, bod 48.

9 Sdělení Komise Evropskému parlamentu, Radě, evropskému hospodářskému a sociálnímu výboru a výboru regionů, Komplexní přístup k ochraně osobních údajů v Evropské unii, KOM(2010) 609 v konečném znění, 4. 11. 2020, s. 2.

10 JOUROVÁ, V. *EU Data Protection Reform – What benefits for businesses in Europe*? Leden 2016. PDF dostupné z: doi:10.2838/1782.

11 The world's most valuable resource is no longer oil, but data. *The Economist*. 2017. Dostupné z: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

ním údajům přistupovat s náležitou péčí a trhu s tímto artiklem stanovit jasné regule.[12] Evropská unie se na tento trend snaží reagovat a zároveň držet krok s novými výzvami, jež skýtají nové platformy přenosu a ukládání osobních údajů, i když ne vždy se jí to daří.

2. Prst na tepu doby

Již v roce 2000 předložila Komise návrh směrnice o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací,[13] která nabyla platnosti v roce 2002 (a dosud nepozbyla) a jejímž cílem bylo přizpůsobit ochranu osobních údajů tak, aby jim byla přiznána co největší ochrana na poli elektronických komunikací, a modernizovat tak principy a modely ochrany stanovené již směrnicí Evropského parlamentu a Rady 97/66/ES ze dne 15. prosince 1997 o zpracování osobních údajů a ochraně soukromí v odvětví telekomunikací.[14] Ostatně již v této směrnici bylo uvedeno, že: *„[…] internet převrací tradiční struktury trhu tím, že poskytuje společnou, obecnou infrastrukturu pro široký okruh služeb elektronických komunikací. Veřejně dostupné služby elektronických komunikací prostřednictvím internetu otevírají uživatelům nové možnosti, ale zároveň vytvářejí i nová rizika pro jejich osobní údaje a soukromí“* (sic!).[15]

Ona snaha postavit se novým výzvám, jež nové technologie bezpochyby přináší, je (alespoň) na poli ochrany osobních údajů Evropské unii imanentní. Potřebu aktualizace rámce ochrany osobních údajů pocítila Komise již v roce 2009, kdy začala s rozsáhlými debatami a se zadáváním vypracování studií relevantních k dané problematice.[16] V roce 2010 pak Komise prostřednictvím sdělení uvedla, že na základě již rok probíhajících diskusí a na základě závěrů z vypracovaných studií[17] předloží v roce 2011 legislativní návrh, jež bude mít za cíl nahradit doposud platnou směrnici o ochraně osobních údajů a postavit se tak výzvám souvisejícím s novými technologiemi.[18] Komise již v tomto sdělení vyjádřila největší obavu nad tím, že: *„Způsoby shromažďování osobních údajů jsou zároveň stále propracovanější a lze je hůře odhalit. Používání sofistikovaných nástrojů umožňuje hospodářským subjektům sledovat chování jednotlivců, a tak se lépe zaměřit na potenciální zákazníky. Rostoucí využívání postupů pro automatický sběr dat (například elektronický prodej jízdenek či výběr mýtného) nebo geolokačních zařízení umožňuje snadněji zjistit polohu určité osoby jednoduše díky jejímu mobilnímu zařízení. Veřejné orgány také stále více využívají osobních údajů za různým účelem, mimo jiné k vyhledávání osob v případě propuknutí přenosné choroby, pro předcházení terorismu a trestné činnosti a k účinnějšímu*

12 TRAKMAN, L. – WALTERS, R. – ZELLER, B. Trade in personal data: Extending international legal mechanisms to faciliate transnational trade in personal data? *European Data Protection Law Review*. 2020, roč. 6, č. 2, s. 243–258.

13 Proprosal 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, COM(2000) 385 final – 2000/0189(COD), Úř. věst. C 365 E/223 ze dne 19. 12. 2000.

14 Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích), Úř. věst. 13, sv. 29, respektive Úřední věstník evropských společenství L 201/37 ze dne 31. 7. 2002, bod odůvodnění č. 4.

15 Ibidem, bod odůvodnění č. 6.

16 Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů, Komplexní přístup k ochraně osobních údajů v Evropské unii, KOM(2010) 609 v konečném znění, 4. 11. 2020, s. 3.

17 Např. Comparative study on different approaches to new privacy challenges in particular in the light of technological developments, vypracovanou na základě smlouvy č. JLS/2008/C4/011 – 30-CE-0219363/00-28, ze dne 20. ledna 2010.

18 Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů, Komplexní přístup k ochraně osobních údajů v Evropské unii, KOM(2010) 609 v konečném znění, 4. 11. 2020, s. 2.

boji proti nim, pro správu systémů sociálního zabezpečení nebo pro daňové účely, a to v rámci svých aplikací elektronické veřejné správy nebo jinak.“[19]

Ve výše uvedené citaci lze sledovat dvojí dimenzi možných nástrah nových technologií. Zaprvé je dle Komise nutná ochrana před soukromoprávními aktéry, společnostmi, jež využívají nové technologie ke sběru osobních údajů zákazníka k co největší personalizaci reklamy. Druhou rovinou je pak sběr dat veřejnoprávními aktéry, kteří získávají přístup k lokalizačním údajům, ať už za účelem vyhledávání osob s ohledem na veřejné zdraví, či jako prostředek ochrany před terorismem. Výše uvedené obavy Komise se později ukázaly jako oprávněné.

3. Soudní dvůr Evropské unie a moderní technologie

V době, kdy byla ještě platná směrnice o ochraně osobních údajů, se na výzvy moderních technologií promptně snažil reagovat i Soudní dvůr Evropské unie. Ten tak například musel stanovit, že uvedení odkazu na osoby identifikovatelné jménem nebo jinak je automatizovaným zpracováním osobních údajů.[20] Uveřejnění osobních údajů na internetu prostřednictvím serveru usazeném v členském státě tak, že k těmto údajům má přístup kdokoli na světě, není předáním údajů do třetí země.[21]

Osobní údaje by neměly být ve veřejně přístupném online rozhraní zpracovávány po nekonečně dlouhou dobu a měly by být selektovány tak, aby bylo užito jen naprosté minimum, a to i v poměru zásady transparentnosti při poskytování unijních dotací.[22] Zpracováním osobních údajů je i tzv. automatizovaná indexace prováděná algoritmem internetového vyhledávače vedoucí k zobrazení výsledků vyhledávání v určitém pořadí.[23]

Subjekty údajů mají právo být zapomenuty (právo na výmaz výsledků vyhledávání na základě jména osoby při splnění kritérií stanovených Soudním dvorem Evropské unie).[24] Právo být zapomenut bylo dalšími rozhodnutími dále vykládáno ve vztahu k obchodnímu rejstříku dostupnému na internetu, kde Soudní dvůr Evropské unie zdůraznil neabsolutní povahu tohoto práva a obecně práva na ochranu osobních údajů v poměru převládajícího veřejného zájmu.[25] S globálním rozsahem internetové sítě se musel Soudní dvůr Evropské unie vypořádat při posuzování extrateritoriálního účinku práva být zapomenut, přičemž jeho závěry v této věci jsou platné i pro hranice působnosti jiných práv spojených s ochranou osobních údajů. Soudní dvůr Evropské unie dochází k závěru, že v případě aplikace práva být zapomenut na doméně v daném členském státě je třeba vymazat výsledky vyhledávání ze všech mutací vyhledávače pro všechny členské státy.[26] Bylo též stanoveno, že sice neexistuje povinnost na unijní úrovni *per se*, dle které musí vyhledávač vymazat

19 Ibidem.

20 Rozsudek Soudního dvora Evropské unie ze dne 6. listopadu 2003, C-101/01, *Bodil Linqvist*, ECLI:EU:C:2003:596, bod 27.

21 Ibidem, bod 71.

22 Rozsudek Soudního dvora Evropské unie ze dne 9. listopadu 2010, C-92/09 a C 93/09, *Volker und Markus Schecke HbR*, ECLI:EU:C:2010:662, bod 85.

23 Rozsudek Soudního dvora Evropské unie ze dne 13. května 2014, C-131/12, *Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja Gonzáles*, ECLI:EU:C:2014:317, bod 41.

24 Ibidem, bod 85.

25 Rozsudek Soudního dvora Evropské unie ze dne 9. března 2017, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce proti Salvatore Mannimu*, ECLI:EU:C:2017:197, bod 43.

26 Rozsudek Soudního dvora Evropské unie ze dne 24. září 2019, C-507/17, *Google LLC proti Commission nationale de l'informatique et des libertés (CNIL)*, ECLI:EU:C:2019:772, bod 66.

odkazy na výsledky pro uživatele i mimo Evropskou unii, zároveň ale není zakázáno, aby tuto povinnost po zohlednění všech podrobností daného případu stanovil dozorový orgán na poli ochrany osobních údajů nebo soud daného členského státu.[27]

Výše uvedené závěry jen dokládají, že s novými technologiemi přicházejí nové výzvy, na které je nutné reagovat jak normotvorbou, tak judikaturní činností, která typicky vyplňuje prázdná místa mezi již zastaralou právní úpravou, a ještě neplatnou novou, která má za cíl přinést změněnou a modernější podobou regulace.

Je nicméně možné, aby vůle normotvůrce nebyla ve výsledné regulaci podpořena testem proporcionality a v takovém případě je dokonce možné, aby Soudní dvůr Evropské unie takovou regulaci prohlásil za neplatnou.

4. Soukromí vs. bezpečí

Výše uvedené závěry Soudního dvora Evropské unie, jež reagovaly na technický pokrok, jsou více či méně zaměřeny na střet práva na ochranu osobních údajů, respektive práva na soukromí, a práva na svobodný přístup k informacím, respektive práva na svobodu slova. Problematika svobody slova ve střetu s právem na soukromí je imanentní rozvoji technologií.[28] Ostatně již v roce 1890 bylo v souvislosti s rozvojem „okamžitých fotografií", rychlého tisku a distribuce tištěných periodik přemítáno nad nutností mít právo na soukromí a nad střetem se svobodou slova a právem na informace.[29] Ve zdrcující většině výše uvedených případů se jedná o regulaci (respektive narušení) práva na soukromí soukromými aktéry, ať už společnostmi za účelem nějakého zisku, nebo fyzickými osobami omezujícími soukromí jiných osob ne nutně za ekonomickým účelem. Postupem času se ale v rámci evropského prostoru vyjevila otázka nutnosti ochrany bezpečnosti, a to především v souvislosti s terorismem.[30]

Státní orgány, jejichž cílem je právě zachování a obrana bezpečnosti, mají k dispozici více a více údajů z dříve nevídaných prostředků. Mezi takové údaje mimo jiné patří záznamy o telefonních hovorech, včetně mobilních čísel, polohy uživatele elektronických zařízení, jména a adresy, IP adresy[31] apod. Tyto údaje primárně zpracovávají poskytovatelé služeb, ať už je to internetové připojení nebo mobilní operátor, za účelem bezpečnosti je ale nutné, aby k těmto údajům měly za určitých okolností přístup právě příslušné státní složky.

S vlnou teroristických útoků počátkem milénia[32] začaly jednotlivé členské státy přijímat národní úpravy, jimiž operátorům (provozovatelům telekomunikačních služeb) stanovovaly povinnost uchovávat výše zmíněné údaje (lokalizační, tj. polohové a jiné provozní údaje – číslo volajícího či vytáčeného, jejich jména atd. – souhrnně nazývané provozní

27 Ibidem, bod 72.

28 Např. The New Internet World – A Global Perspective on Freedom of expression, Privacy, Trust and Security Online, *The Global Information Technology Report 2010–2011*, World Economic Forum ve spolupráci s INSEAD a Oxford University.

29 WARREN, S. D. – BRANDEIS, L. D. The Right to Privacy. *Harvard Law Review*. 1890, Vol. 4, No. 5.

30 BIGNAMI, F. Privacy and law enforcement in the European Union: The data retention directive. *Chicago Journal of International Law*. 2007, roč. 8, č. 1, s. 238.

31 IP adresa byla označena za osobní údaj Soudním dvorem Evropské unie v rozsudku ze dne 19. října 2016 ve věci C-582/14, *Patrick Breyer proti Bundesrepublik Deutschland*, ECLI:EU:C:2016:779, bod 49.

32 11. září 2001 v New Yorku, 11. března 2004 v Madridu a 7. července 2005 v Londýně, srov. např. C-301/16, *Irsko v. Evropský parlament a Rada*, bod 36.

metadata).[33] Evropská unie vycítila potřebu harmonizace, protože rozličné národní úpravy jednotlivých členských států nikterak nenapomáhaly jak vnitřnímu trhu, tak ani nepodporovaly efektivní justiční spolupráci.[34]

Reakcí na tyto výzvy ve smyslu uchovávání osobních údajů a předání těchto údajů vnitrostátním orgánům za účelem bezpečnosti (tj. předcházení, vyšetřování, odhalování a stíhání trestných činů) byla tzv. „směrnice o uchovávání údajů" (nebo též pod anglickým názvem *„Data Retention Directive"*).[35] Cíl směrnice o uchovávání údajů byl alespoň na první pohled jasný, rámcově sjednotit přístup jednotlivých členských států s ohledem na *„povinnosti poskytovatelů uchovávat určité údaje a zajistit jejich dostupnost pro účely vyšetřování, odhalování a stíhání závažných trestných činů, jak jsou vymezeny každým členským státem […]."*[36]

5. Legální základ směrnice o uchovávání údajů; Irsko v. parlament a Rada

Jednou z překážek zákonodárného procesu přijetí směrnice o uchovávání údajů byl nicméně fakt, že nebylo na první pohled zřejmé, zda se má vůbec přijímat směrnice v rámci prvního pilíře s ohledem na to, že harmonizuje i takové zacházení s osobními údaji, které posílí jednotný trh, nebo rámcové rozhodnutí v rámci pilíře třetího, protože směrnice měla (ve smyslu měla mít) za úkol posílit justiční spolupráci.[37]

Původně bylo navrženo Francií, Irskem, Švédskem a Spojeným královstvím přijmout Radou rámcové rozhodnutí jakožto návrh v mezích třetího pilíře. Právní služby Komise a Rady ale došly k závěru, že má být přijímána směrnice v intencích pilíře prvého, a to z důvodu, že předchozí úprava zabývající se uchováváním dat (a obecně osobními údaji) už byla přijata postupem předvídaným prvním pilířem a s ohledem na vliv připravované směrnice na vnitřní trh.[38, 39] S ohledem na to, že pro přijetí rámcového rozhodnutí postupem pro třetí pilíř byla nutná jednomyslnost v Radě, které nebylo dosaženo, byl návrh států stažen.[40]

V návaznosti na to byl Komisí předložen návrh směrnice o uchovávání údajů jako návrh v mezích prvého pilíře a takto byla směrnice nakonec i přijata (tj. spolurozhodovacím

---

33 Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 200/58/ES, Úř. věst. L 105/54 ze dne 13. 4. 2006 (v poznámkách pod čarou a při citaci dále jen *„Data Retention Directive"*), bod 9, bod 17 bod 22 odůvodnění.

34 BIGNAMI, F. Privacy and law enforcement in the European Union: The data retention directive. *Chicago Journal of International Law*. 2007, Vol. 8, No. 1, s. 239.

35 Směrnice Evropského parlamentu a Rady 2006/24/ES.

36 Ibidem, bod 21 odůvodnění.

37 FLYNN, C. Data retention, the separation of power in the EU and the right to privacy: a critical analysis of the legal validity of the 2006 directive on the retention of data. *University College Dublin Law Review*. 2008, roč. 8, s. 1–25.

38 Ibidem, s. 4.

39 Argumentace právních služeb byla založena na bývalém článku 47 (nynějším 40) Smlouvy o Evropské unii: „Provádění společné zahraniční a bezpečnostní politiky se nedotýká uplatňování postupů a rozsahu pravomocí *orgánů, které Smlouvy stanoví pro výkon pravomocí Unie uvedených v článcích 3 až 6 Smlouvy o fungování Evropské unie. Stejně tak se provádění politik uvedených v daných článcích nedotýká uplatňování postupů a rozsahu pravomocí orgánů, které Smlouvy stanoví pro výkon pravomocí Unie podle této kapitoly."* Bylo totiž řečeno, že plánovaná směrnice o uchovávání údajů rozvádí zmocnění již dané čl. 15 směrnice o soukromí a elektronických komunikacích, což by nebylo možné přijetím v mezích třetího pilíře právě s ohledem na tehdejší čl. 47 Smlouvy o Evropské unii.

40 FLYNN, C. Data retention, the separation of power in the EU and the right to privacy: a critical analysis of the legal validity of the 2006 directive on the retention of data. *University College Dublin Law Review*. 2008, roč. 8, s. 1–25.

postupem se stanoviskem Evropského parlamentu a kvalifikovanou většinou v Radě).[41] Takový postup měl ale nakonec i politické důsledky, když některé státy vnímaly s nevolí užití prvního pilíře, tedy komunitární úrovně tehdejšího společenství, k zásahu do politik zahrnutých to pilíře třetího (jehož „výsostným pánem" byly státy samotné).[42]

Přijetí směrnice o uchovávání údajů v režimu prvního pilíře tak každopádně vynechalo z působnosti směrnice dříve tak kýženou harmonizační úpravu justiční spolupráce na poli předávání dotčených údajů v trestních věcech a směrnice se omezila v podstatě jen na regulaci soukromých subjektů.[43]

Uvedený politický spor vyústil podáním žaloby na neplatnost přijaté směrnice o uchovávání údajů vládou Irska za podpory Slovenské republiky.[44] Nosným argumentem žaloby bylo, že směrnice byla přijata dle čl. 95 Smlouvy o Evropském společenství, na jehož základě lze přijímat opatření, jejichž cílem je: *„Sbližování vnitrostátních právních předpisů za účelem zlepšení fungování vnitřního trhu."* Přitom ale hlavním cílem směrnice o uchovávání údajů měl být boj proti trestné činnosti.[45]

Slovenská republika, za jejíž podpory byla žaloba Irskem podána, argumentovala, že směrnice o uchovávání údajů zasahuje do soukromí jednotlivých osob tak závažným způsobem (tj. flagrantně narušuje čl. 8 EÚLP), že nebylo možné tento zásah odůvodnit hospodářskými cíli, ale pouze bojem s trestnou činností a terorismem. Z tohoto důvodu bylo vhodné (ne-li nutné), aby taková úprava byla přijata jednomyslně a mimo rámec tehdejšího společenství (mimo rámec prvého pilíře).[46]

Soudní dvůr Evropské unie konstatoval, že dle odůvodnění přijaté směrnice o uchovávání údajů bylo jedním ze stěžejních cílů harmonizovat úpravy jednotlivých členských států právě na poli uchovávání a vyžádání si lokalizačních a provozních údajů. Dříve přijaté právní úpravy jednotlivými členskými státy na základě zmocnění v čl. 15 odst. 1 směrnice o soukromí a elektronické komunikaci se natolik lišily, že byly způsobilé narušit jednotný trh. K takové harmonizaci pak bylo vhodné přijmout opatření dle čl. 95 Smlouvy o Evropském společenství.[47]

Soudní dvůr se dále ztotožnil s argumentem právních služeb Komise a Rady založeném na čl. 47 (nyní čl. 40) Smlouvy o Evropské unii, o němž autor podrobněji psal v poznámce pod čarou 39 tohoto pojednání.[48] Na základě výše uvedeného pak Soudní dvůr Evropské unie uzavřel, že směrnice o uchovávání údajů byla přijata správným legislativním postupem založeným na jediném možném legislativním základu.[49]

Nutno podotknout, že Soudní dvůr Evropské unie se v předešlém rozhodnutí nezabýval slučitelností samotného obsahu směrnice o uchovávání údajů s unijním právem (respektive lidskými právy), což se mělo ale brzy změnit.

---

41 Dá se říci, že Komise vypracovala návrh směrnice už během projednávání rámcového rozhodnutí, načež státy v Radě se rozhodly nepokračovat v projednávání rámcového rozhodnutí (i na základě stanoviska právních služeb) a spíše přikročit k procesu projednávání návrhu směrnice předloženého Komisí.

42 Ibidem.

43 GALLI, F. Digital Rights Ireland as an opportunity to foster desirable approximation of data retention provisions. *Maastricht Journal of European and Comparative Law*. 2016, roč. 23, č. 3, s. 460–477.

44 Rozsudek Soudního dvora Evropské unie ze dne 10. února 2009, C-301/06, *Irsko v. Evropský parlament a Rada Evropské unie*, ECLI:EU:C:2009:68.

45 Ibidem, bod 30.

46 Ibidem, bod 34.

47 Ibidem, body 61–73.

48 Ibidem, body 75–83.

49 Ibidem, bod 93.

6. Směrnice o uchovávání údajů a test proporcionality; Digital Rights Ireland

Je nutné zmínit, že směrnice o uchovávání údajů stanovila přímo povinnost, na rozdíl od pouhého zmocnění ve směrnici o soukromí a elektronických komunikacích,[50] ukládat provozní a lokalizační údaje.[51] Naopak dokonce směrnice o soukromí a elektronických komunikacích obsahovala diametrálně odlišnou úpravu, když stanovovala *„důvěrný charakter sdělení a provozních údajů, jakož i povinnost vymazat nebo anonymizovat tyto údaje. Nejsou-li již potřebné pro přenos sdělení, s výjimkou případu, kdy jsou potřebné pro vyúčtování a pouze po dobu, kdy tato potřeba přetrvává.*"[52] Právě ona povinnost uchovávat provozní a lokalizační údaje po stanovenou dobu minimálního trvání šesti měsíců vyvolávala od samého počátku určité rozpaky.[53]

Stanovení takové povinnosti se nezamlouvalo mnoha organizacím zabývajícím se soukromím osob v digitálním světě. Jedna z těchto organizací – *Digital Rights Ireland* – se tak rozhodla vykonstruovat proces, jehož cílem bylo napadnout uchovávání lokalizačních a provozních údajů na základě směrnice o uchovávání údajů. *Digital Rights Ireland* tak podala žalobu k irským soudům, přičemž tvrdila, že vlastní mobilní telefon, který používá. Poskytovatel služeb telefonické komunikace musí na základě zákona, jímž byla provedena směrnice o uchovávání údajů, po dobu stanovenou zákonem uchovávat provozní a lokalizační údaje o komunikacích pro účely předcházení, odhalování, vyšetřování a stíhání trestných činů, jakož i pro účely zajišťování bezpečnosti státu.[54] Taková povinnost zasahuje *Digital Rigths Ireland* do práva na soukromí, a proto se organizace dožadovala zrušení prováděcího zákona, potažmo směrnice o uchovávání údajů jako takové.

Se stejným požadavkem se ve stejnou dobu obrátilo na rakouskou soudní soustavu 11 131 stěžovatelů, přičemž oba případy skončily jako předběžná otázka před Soudním dvorem Evropské unie, který dané věci spojil v jedno řízení,[55] jež vyústilo v rozsudek ve věci pod populárním zkráceným názvem *Digital Rights Ireland*.

Je nepochybné, že uchovávání údajů ve smyslu směrnice o uchovávání údajů zasahuje do soukromého života a zároveň je zpracováním osobních údajů.[56] S ohledem na to musí být tento zásah odůvodněný (tj. odpovídat cíli obecného zájmu), stanovený zákonem, musí respektovat podstatu omezených práv a být v souladu s testem proporcionality dle čl. 52 odst. 1 Listiny základních práv EU.[57]

Dle Soudního dvora Evropské unie nedochází k popření samotné podstaty práva na soukromí a ochranu osobních údajů, protože směrnice o uchovávání údajů neumožňuje nikomu seznámit se přímo s obsahem komunikace dotčených subjektů a zároveň stanovu-

50 Stanovisko Evropského inspektora ochrany osobních údajů k návrhu směrnice Evropského parlamentu a Rady o uchovávání údajů zpracovaných v souvislosti s poskytováním veřejných služeb elektronických komunikací, kterou se mění směrnice 200/58/ES (KOM(2005) 438 v konečném znění, Úř. věst. C 298/1 ze dne 29. 11. 2005 (dále jen jako „Stanovisko inspektora k Data Retention Directive").

51 Směrnice o uchovávání údajů, čl. 6 a 5.

52 Rozsudek soudního dvora Evropské unie ze dne 8. dubna 2014, C-293/12 a C-594/12, *Digital Rights Ireland Ltd*, ECLI:EU:C:2014:238, bod 32.

53 Např. Stanovisko inspektora k Data Retention Directive, bod 22; Article 29 Data Protection Working Party Opinion 9/2004 (11885/04/EN).

54 Rozsudek soudního dvora Evropské unie ze dne 8. dubna 2014, C-293/12 a C-594/12, *Digital Rights Ireland Ltd*, ECLI:EU:C:2014:238, bod 17.

55 Ibidem, bod 19.

56 Ibidem, bod 29, 34, 35 a 36.

57 Ibidem, bod 38.

je pro poskytovatele služeb povinnost dodržovat základní zásady ochrany osobních údajů (povinnost mít taková technická a organizační opatření, aby bylo zamezeno náhodnému nebo neoprávněnému zničení, ztrátě či pozměnění údajů).[58, 59]

Cíl obecného zájmu směrnice o uchovávání údajů taktéž naplňovala. Uchovávání údajů bylo stanoveno pro boj s mezinárodním terorismem, zachování mezinárodního míru a bezpečnosti, což samo o sobě je dle judikatury Soudního dvora Evropské unie obecným zájmem. Navíc takový obecný zájem spadá pod právo na osobní bezpečnost ve smyslu čl. 6 Listiny základních práv EU.[60]

Ve vztahu k výše uvedenému bylo nutné testem proporcionality poměřit přiměřenost a nezbytnost zásahu do základních práv na soukromí a ochranu osobních údajů vzhledem k výše uvedenému cíli směrnice o uchovávání údajů. Je konstatováno, že uchovávání daných údajů určených ve směrnici o uchovávání údajů je způsobilé k naplnění předeslaného cíle.[61]

První zádrhel nastává v případě posouzení nezbytnosti uchovávání daných údajů stanoveného počtu subjektů dle směrnice o uchovávání údajů. Ustálená judikatura Soudního dvora Evropské unie přitom praví, že při zásahu do soukromí a práva na ochranu osobních údajů musí být zásah (výjimka z práva na soukromí a ochranu osobních údajů) omezen na to, co je pro splnění určeného cíle naprosto nezbytné.[62] V daném případě je však stanovena povinnost uchovávat veškeré provozní údaje jakýmkoli způsobem související s pevnou, mobilní či internetovou telefonní sítí, připojením k internetu a internetové elektronické pošty.[63] Zároveň se uchovávání provozních údajů ze všech výše uvedených zdrojů elektronické komunikace vztahuje na všechny uživatele, a to bez jakéhokoli rozlišovacího klíče, přičemž rozlišovací klíč není stanoven ani pro uchovávání samotných provozních údajů. Jinými slovy je stanovena povinnost uchovávat většinu provozních údajů, z víceméně všech zdrojů elektronické komunikace, všech uživatelů bez jakéhokoli rozdílu.[64]

Velice vágní se zdá Soudnímu dvoru Evropské unie i stanovení pravidel pro přístup osob k uchovávaným údajům. Především směrnice o uchovávání údajů nestanovovala objektivní kritéria, komu a za jakým účelem je možné údaje poskytnout, natož aby byl stanoven mechanismus přezkumu oprávněnosti přístupu k takto uchovávaným údajům.[65]

V poslední řadě bylo Soudním dvorem Evropské unie předpisu vytčeno, že doba uchovávání je směrnicí o uchovávání údajů stanovena na minimálně 6 měsíců a maximálně 24 měsíců. Přitom ale není stanoveno žádné východisko pro určení doby uchovávání, není rozlišeno mezi jednotlivými uchovávanými údaji, a tak je doba uchovávání bez jakýchkoli vodítek plně na členských státech, respektive na samotných poskytovatelích služeb elektronických komunikací.[66]

---

58 Ibidem, bod 39–40.

59 Nutno nicméně podotknout, že v tomtéž rozsudku Soudní dvůr Evropské unie v posledních závěrečných bodech (66, 67 a 68) vytýká unijnímu normotvůrci, že ve směrnici o uchovávání údajů nejsou stanoveny dostatečné bezpečnostní záruky (ani nerozlišuje mezi citlivými a „regulérními" osobními údaji), když není zaručeno, že poskytovatelé služeb elektronických komunikací skutečně přijmou dostatečná technická a organizační opatření a navíc je umožněno při určení uplatňované úrovně bezpečnosti zohlednit poskytovatelům ekonomická hlediska.

60 Ibidem, bod 41–44.

61 Ibidem, bod 49.

62 Rozsudek soudního dvora Evropské unie ze dne 7. 11. 2013, C-473/12, *Institut professionnel des agents immobiliers (IPI), proti Geoffreyi Englebertovi, Immo 9 SPRL, Grégorymu Francotteovi*, ECLI:EU:C:2013:715, bod 39.

63 Rozsudek soudního dvora Evropské unie ze dne 8. dubna 2014, C-293/12 a C-594/12, ECLI:EU:C:2014:238, bod 56.

64 Ibidem, bod 56–60.

65 Ibidem, bod 60–62.

66 Ibidem, bod 63–63.

Shrnuto podtrženo, Soudní dvůr Evropské unie kvituje snahu evropského normotvůrce s ohledem na harmonizaci přístupu členských států k předcházení mezinárodnímu terorismu, či jiných trestných činů ohrožující veřejnou bezpečnost, jedná se o cíl obecného zájmu. Zároveň nebyla popřena samotná podstata práva na soukromí a ochranu osobních údajů, protože nebylo umožněno seznámit se s obsahem dotčené komunikace. Taktéž bylo konstatováno, že určená povinnost uchovávat provozní data může naplnit výše uvedený cíl obecného zájmu. Směrnice o uchovávání údajů ale nemohla projít testem proporcionality, protože stanovovala tak široké mantinely a natolik rozostřené (nebo dokonce žádné) ukazatele, že nenaplňovala požadavek nezbytně nutného (ve smyslu minimalizovaného) zásahu do dotčených základních práv.

Byť byla směrnice o uchovávání údajů Soudním dvorem Evropské unie prohlášena za neplatnou, nemělo to přímý dopad na transponovanou úpravu do legislativy jednotlivých členských států.[67] Členské státy nadto samy nebyly jednotné v otázce, jaký dosah rozsudek ve věci má na jednotlivé národní úpravy vůbec mít.[68]

7. Otázkou je jak?

Členské státy sice byly zmocněny (ve smyslu bylo jim unijním normotvůrcem *umožněno* – tj. oproti směrnici o uchovávání údajů, která k uchovávání osobních údajů stanovovala sama přímo povinnost) k národním úpravám omezujícím právo na soukromí a ochranu osobních údajů ve vztahu k elektronickým komunikacím článkem 15 odst. 1 směrnice o soukromí a elektronických komunikací, ale rozsah tohoto zmocnění byl více či méně nejasný a úprava stále musí reflektovat mantinely vytyčené Soudním dvorem Evropské unie.[69] Vnitrostátní úprava ve smyslu čl. 15 odst. 1 směrnice o soukromí a elektronických komunikacích může být odůvodněna pouze pro zajištění národní bezpečnosti, obrany, veřejné bezpečnosti a pro prevenci, vyšetřování, odhalování a stíhání trestných činů nebo neoprávněného použití elektronického komunikačního systému, a navíc musí být v demokratické společnosti nezbytná, přiměřená a úměrná výše uvedeným cílům.[70]

Státy si v podstatě s rozsudkem ve věci *Digital Rights Ireland* nebyly s to poradit.[71] Rozpaky z důsledků rozsudku *Digital Rights Ireland* lze demonstrovat dvěma případy, které následně vyústily v případ před Soudním dvorem Evropské unie známým pod populárním názvem *Tele2 Sverige*.

Po rozsudku ve věci *Digital Rights Ireland* odmítala švédská telekomunikační společnost Tele2 Sverige nadále uchovávat údaje elektronických komunikací a ta data, která uchovávala k danému datu, vymazala. Důsledkem bylo, že Tele2 Sverige přestala dodávat dané údaje švédské policii, což vyústilo ve správní stížnost švédského policejního

---

67 SMEJKAL, V. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, s. 324.

68 Rozsudek Soudního dvora Evropské unie ze dne 21. 12. 2016, C-203/15 a C-698/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:970, bod 63.

69 RAUHOFER, J. – SITHIGH, D. The Data Retention Directive Never Existed. *SCRIPTed: A Journal of Law, Technology and Society*. 2014, roč. 11, č. 1, s. 127.

70 Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. 7. 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací Úř. věst. 13, sv. 29, respektive Úřední věstník evropských společenství L 201/37 ze dne 31. 7. 2002, čl. 15 odst. 1.

71 GALLI, F. Digital Rights Ireland as an opportunity to foster desirable approximation of data retention provisions. *Maastricht Journal of European and Comparative Law*. 2016, roč. 23, č. 3, s. 460–477.

ředitelství, které rozsudek ve věci *Digital Rights Ireland* interpretovalo odlišně. Švédskou soudní soustavou se pak případ dostal před Soudní dvůr Evropské unie.[72]

Věc byla spojena společně s předběžnou otázkou položenou britskými vrcholnými soudy v případě, kdy se stěžovatelé domáhali zrušení ustanovení zákona, jež je dle nich po vynesení rozsudku ve věci *Digital Rights Ireland* v opozici vůči článku 8 EÚLP.[73]

V roce 2016 se tak Soudní dvůr Evropské unie zabýval poprvé po zrušení směrnice o uchovávání údajů souladem vnitrostátní úpravy s čl. 15 odst. 1 směrnice o soukromí a elektronických komunikacích ve světle podmínek stanovených rozsudkem ve věci *Digital Rights Ireland*.

V prvé řadě se Soudní dvůr Evropské unie musel vypořádat s otázkou, zda dotčená úprava členských států spadá pod rámec unijního práva s ohledem na úpravu v čl. 15 odst. 1 směrnice o soukromí a elektronických komunikacích. Tato otázka je více či méně odrazovým můstkem pro posouzení souladu vnitrostátních úprav s ohledem na možná porušení základních práv Evropské unie vzhledem k tomu, že Listina základních práv Evropské unie a základní práva v ní obsažená musí být naplněna orgány členských států pouze při uplatňování unijního práva.[74]

Soudní dvůr Evropské unie systematickým a teleologickým výkladem dochází k celkem jednoznačnému závěru, že úprava v právních řádech členských států, jež stanovuje povinnost uchovávat lokalizační údaje, spadá pod rámec směrnice o soukromí a elektronických komunikacích, protože při uchovávání lokalizačních a provozních údajů dochází ke zpracování osobních údajů. Stejně tak spadá pod právní rámec směrnice o soukromí a elektronických komunikacích *„legislativní rámec […] přístupu vnitrostátních orgánů k údajům uchovávaným poskytovateli služeb elektronických komunikací“*.[75] To s ohledem na fakt, že přístupem k uchovávaným údajům je zasaženo do soukromí a práva na ochranu osobních údajů subjektů.

S ohledem na výše vymezený závěr může Soudní dvůr Evropské unie přikročit k posouzení vnitrostátních úprav s ohledem na principy a rámec směrnice o soukromí a elektronické komunikaci, a především pak s ohledem na čl. 15 odst.1 předmětné směrnice. V rozsudku je potvrzeno, že čl. 15 odst. 1 směrnice o soukromí a elektronických komunikacích opravňuje členské státy k zavedení takových legislativních výjimek, které stanovují poskytovatelům služeb elektronických komunikací povinnost uchovávat provozní a lokalizační údaje a umožnit k nim přístup státním orgánům s ohledem na předcházení či vyšetřování trestné činnosti. Nicméně takové výjimky musí být s ohledem na smysl unijní úpravy omezeny na *„v demokratické společnosti nezbytné, vhodné a přiměřené“*.[76] Takové požadavky odpovídají požadavkům testu proporcionality,[77] který byl použit i v rozsudku ve věci *Digital Rights Ireland*.

S ohledem na to, že Soudním dvorem Evropské unie v předmětném případě projednávané úpravy členských států stanovovaly plošnou a nerozlišovací povinnost pro uchová-

---

72 Rozsudek Soudního dvora Evropské unie ze dne 21. 12. 2016, C-203/15 a C-698/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:970, body 44–51.

73 Ibidem, body 52–59.

74 Listina základních práv Evropské unie, konsolidované znění z roku 2012 (2012/C 326/02), Úř. věst. 326/391, 26. 10. 2012, Článek 51 odst. 1 „Oblast použití“.

75 Rozsudek Soudního dvora Evropské unie ze dne 21. 12. 2016, C-203/15 a C-698/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:970, bod 75 a 76.

76 Ibidem, bod 95.

77 Ibidem.

vání veškerých lokalizačních a provozních údajů všech účastníků a registrovaných uživatelů, jež se vztahovala na veškeré prostředky elektronické komunikace,[78] postupoval dále Soudní dvůr Evropské unie v podstatě stejně, jako při výkladu směrnice o uchovávání údajů. Dochází tedy k dílčímu závěru, že byť podle čl. 15 odst. 1 směrnice o soukromí a elektronických komunikacích povoluje stanovit členským státům výjimku z předmětné úpravy dotčené směrnice, projednávanou vnitrostátní úpravou je spíše stanoveno pravidlo, které popírá smysl a význam výjimky uvedené v čl. 15 odst. 1 (tj. čl. 15 odst. 1 stanovuje výjimku z pravidla, přičemž členské státy z této výjimky stanovují pravidlo sobě vlastní, které v důsledku charakter výjimky popírá).[79]

Z výše uvedeného Soudní dvůr Evropské unie dovozuje, že taková vnitrostátní úprava, která za účelem boje proti trestné činnosti stanovuje plošné a nerozlišující uchovávání veškerých provozních a lokalizačních údajů všech účastníků a registrovaných uživatelů, které se vztahuje na veškeré prostředky elektronické komunikace, není v souladu s čl. 15 odst. 1 směrnice o soukromí a elektronických komunikacích, ani s čl. 7, 8, 11 a čl. 52 odst. 1 Listiny základních práv Evropské unie.[80]

Soudní dvůr Evropské unie dále stanovuje, že je nutné, aby přístup příslušných vnitrostátních orgánů k uchovávaným údajům byl řádně odůvodněn, podléhal předchozímu přezkumu ze strany soudů nebo nezávislých správních orgánů a aby takové orgány rozhodovaly na základě odůvodněné žádosti příslušných orgánů, které mají umožněn přístup k uchovávaným údajům.[81] Příslušné orgány navíc musejí vždy upozornit dotčené osoby, že mají přístup k jejich uchovávaným údajům, a to ve chvíli, kdy toto sdělení nemůže již ohrozit probíhající vyšetřování.[82] Závěrem Soudní dvůr Evropské unie podotýká, že přístup k uchovávaným údajům může být pouze za účelem v limitech čl. 15 odst. 1 směrnice o soukromí a elektronických komunikacích, tj. za účelem boje proti závažné trestné činnosti a s ohledem na bezpečnost uchovávání údajů, včetně organizačních a technických opatření. Zároveň musí být zajištěno uchovávání dotčených údajů na území Evropské unie tak, aby bylo možné nad nimi efektivně vykonávat dohled ze strany nezávislých orgánů členských států.[83]

Necelý rok po vydání rozsudku ve věci *Tele2 Sverige* provedl Eurojust šetření ohledně opatření jednotlivých členských států přijatých ve světle výše uvedeného. Na základě šetření vydal Eurojust report, z kterého je patrné, že většina členských států výše uvedená rozhodnutí Soudního dvora Evropské unie reflektovala pouze minimálně.[84]

Především většina členských států při šetření uvedla, že dotčená vnitrostátní právní úprava neobsahuje cílené požadavky na uchovávání dat uživatelů nebo prostředků komunikace, ergo je stále požadováno nerozlišující, celoplošné uchovávání všech lokalizačních a provozních údajů všech uživatelů veškerých komunikačních prostředků.[85] Žádný

78 Ibidem, bod 97.
79 Ibidem, bod 104.
80 Ibidem, bod 112.
81 Ibidem, bod 120.
82 Ibidem, bod 121.
83 Ibidem, bod 125.
84 EU: Member State data retention regimes – what's changed? The answer is very little, publikováno dne 20. 11. 2017 [cit. 2021-03-14]. Dostupné z: <https://www.statewatch.org/news/2017/november/eu-member-state-data-retention-regimes-what-s-changed-the-answer-is-very-little/>.
85 Report of Eurojust on data retention regimes in Europe in light of the CJEU ruling of 21 December 2016 in Joined Cases C-203/15 and C-698/15, dokument č. 10098/17, ze dne 6. listopadu 2017, s. 7.

ze členských států, které v daném šetření odpovídaly, nicméně nemá takovou národní legislativu, která by stanovovala povinnost uchovávání lokalizačních a provozních údajů pouze cíleně s ohledem na konkrétní osoby a určitou lokalitu.[86, 87]

Některé státy uvedly (Rakousko, Holandsko, Rumunsko, Slovinsko a Slovensko), že již v souladu s rozsudkem ve věci *Digital Rights Ireland* jejich ústavní soudy zrušily národní úpravy stanovující nerozlišující povinnost uchovávání osobních údajů pro předcházení závažné trestné činnosti. V této souvislosti pak přijaly národní úpravu, která umožňovala příslušným orgánům vyžádat taková data od provozovatelů služeb elektronických komunikací, která tito provozovatelé uchovávali pro soukromé účely v souladu s platnou právní úpravou.[88] Slovensko nadto do legislativy zavedlo tzv. *data freezing*, to je uchovávání údajů o určité osobě do budoucna s ohledem na důvodné podezření příslušného orgánu s ohledem na (možnost) páchání trestné činnosti dotčeným subjektem.[89]

Zpráva Eurojustu uzavírá, že jednotlivé úpravy v členských státech jsou v režimu přezkoumávání, nebo již byly v návaznosti na judikaturu Soudního dvora Evropské unie určitým způsobem změněny (byť ne tak, aby byly plně kompatibilní; viz výše) nebo jsou předmětem probíhajícího soudního přezkumu vrcholných soudů jednotlivých členských států.[90]

8. Další upřesnění přípustnosti uchovávání údajů ve věci Ministerio fiscal a ve věci Privacy International

Své závěry Soudní dvůr Evropské unie znovu potvrdil v roce 2018 (ve věci zkráceně *Ministerio fiscal*)[91] a zároveň svůj výklad čl. 15 odst. 1 směrnice o soukromí a elektronických komunikacích upřesnil v tom smyslu, že orgán činný v trestním řízení může požádat soud, aby stanovil provozovatelům služeb elektronické komunikace povinnost vydat takové provozní údaje, které mohou identifikovat držitele karty SIM v kradeném mobilu.[92] Dle Soudního dvora Evropské unie není v takovém případě nutné, aby byl trestný čin kvalifikován jako „závažný", protože za „závažný" nelze ani považovat takový zásah do soukromí a práva na ochranu osobních údajů.[93]

Přes všechno výše uvedené (především s ohledem na rozsudek ve věci *Tele2 Sverige*) se nicméně Soudní dvůr Evropské unie opět musel vyslovit k posouzení úpravy členských států ukládající plošné nerozlišující ukládání provozních a lokalizačních osobních údajů a zda vůbec taková úprava, s ohledem na účel národní bezpečnosti, spadá pod čl. 15 odst. 1 směrnice o soukromí a elektronických komunikacích.

Ve věci C-623/17 (zkráceně *Privacy International*) některé členské státy (Švédsko, Spojené království, Česká republika, Irsko, Estonsko, Francie, Kypr, Maďarsko a Polsko) tvrdily, že národní úprava umožňující bezpečnostním a zpravodajským službám vyžádat si provozní a lokalizační údaje od provozovatelů služeb elektronických komunikací za účelem

86 Ibidem.

87 Slovensko se nicméně k danému přiblížilo svou úpravu tzv. *data freezing*, srov. níže.

88 Report of Eurojust on data retention regimes in Europe in light of the CJEU ruling of 21 December 2016 in Joined Cases C-203/15 and C-698/15, dokument č. 10098/17, ze dne 6. listopadu 2017, s. 7.

89 SMEJKAL, V. *Kybernetická kriminalita*, s. 326.

90 Ibidem, s. 13.

91 Rozsudek Soudního dvora Evropské unie ze dne 2. 10. 2018, C-207/16, ve věci *Ministerio Fiscal*, ECLI:EU:C:2018:788, bod 37.

92 Ibidem, bod 63.

93 Ibidem, bod 62.

národní bezpečnosti nespadá do oblasti působnosti evropského práva s ohledem na čl. 4 odst. 2 Smlouvy o Evropské unii.[94]

Soudní dvůr Evropské unie v prvé řadě připomíná, že dle ustálené judikatury pouhá skutečnost, že je určité opatření členského státu přijato za účelem zajištění vnitřní a vnější bezpečnosti tohoto členského státu, nezbavuje členské státy povinnosti dodržovat mantinely dané právem Evropské unie a zprostit se tak eurokonformní odpovědnosti.[95] Soudní dvůr Evropské unie pak s odkazem na své předchozí závěry ve spojených věcech C-203/15 a C-698/15 (*Tele2 Sverige* a *Watson*) ve spojení s čl. 23 odst. 1 písm. d) a h) GDPR uzavírá, že *„vnitrostátní právní úprava, která státnímu orgánu umožňuje uložit poskytovatelům služeb elektronických komunikací povinnost předávat bezpečnostním a zpravodajským službám – pro účely zajištění národní bezpečnosti – provozní a lokalizační údaje, spadá do oblasti působnosti této směrnice"* (směrnice o soukromí a elektronických komunikacích).[96]

V předmětném případě pak nebylo posuzováno, zda je v souladu s čl. 15 odst. 1 směrnice o soukromí a elektronických komunikacích taková národní úprava, která přímo ukládá povinnost plošného a nerozlišujícího ukládání provozních a lokalizačních údajů, ale úprava, která umožňuje orgánům členských států uložit *ad hoc* povinnost k takovému ukládání (plošnému a nerozlišujícímu s cílem národní bezpečnosti).[97]

Soudní dvůr Evropské unie v podstatě jen opakuje ustálené závěry z rozsudků ve věcech *Digital Rights Ireland*, *Tele2 Sverige* a *Watson*. Posuzovaná pravomoc orgánů členských států je výjimkou ze zásady důvěrnosti a jako taková musí splňovat požadavky nezbytné nutnosti, legitimního cíle a testu proporcionality. Pokud může orgán vyžádat od provozovatele služeb elektronických komunikací jakékoli provozní či lokalizační údaje od všech uživatelů těchto služeb, a to bez jakéhokoli rozlišovacího hlediska, je tento zásah do základních práv na soukromí a práva na ochranu osobních údajů příliš extenzivní. Ergo kladívko taková národní úprava není v souladu s čl. 15 odst. 1 směrnice o soukromí a elektronických komunikacích.[98]

9. Poslední v řadě – La Quadrature du Net

V den vynesení rozsudku ve věci *Privacy International* byl vynesen rozsudek ve spojených věcech C-511/18, C-512/18 a C-520/18 (zkráceně ve věci *La Quadrature du Net*), který opět potvrdil ustálené závěry Soudního dvora Evropské unie a poskytl další vodítka pro výklad národních úprav s ohledem na ukládání provozních a lokalizačních údajů a přístupu k nim.[99]

V rozsudku ve věci *La Quadrature du Net* Soudní dvůr Evropské unie velice extenzivně posoudil (v celých 229 bodech rozsudku) možná prolomení zákazu plošného a nerozlišujícího uchovávání lokalizačních a provozních údajů a poskytl tak dle autora tohoto příspěvku již velmi komplexní návod pro možné úpravy vnitrostátních právních řádů

94 Rozsudek Soudního dvora Evropské unie ze dne 6. 10. 2020, C-623/17, *Privacy International proti Secretary of State for Foreign and Commonwealth Affairs a dalším*, ECLI:EU:C:2020:790, bod 32 a 33.

95 Ibidem, bod 44.

96 Ibidem, bod 48 a 49.

97 Ibidem, bod 50.

98 Ibidem, body 66–82.

99 Rozsudek Soudního dvora Evropské unie ze dne 6. 10. 2020, C-511/18, C-512/18 a C-520/18, *La Quadrature du Net (C-511/18 a C-512/18) a další)*, ECLI:EU:C:2020:791.

jednotlivými členskými státy. Bylo sice opět zopakováno, že opatření členských států stanovující plošné a nerozlišující uchovávání provozních a lokalizačních údajů není možné, nicméně lze taková opatření zavést v poměrně jasně vymezených mutacích.[100] Autor tohoto příspěvku si neklade za cíl předložit čtenáři úplný a vyčerpávající seznam možných výjimek, přesto je pro demonstraci vhodné uvést některé národní úpravy považované Soudním dvorem Evropské unie za přípustné.

V souladu s čl. 15 odst. 1 směrnice o soukromí a elektronických komunikacích je tak přípustná úprava členského státu, která umožňuje přikázat s cílem národní bezpečnosti plošné a nerozlišující uchovávání provozních a lokalizačních údajů v případě, kdy členský stát čelí „závažnému ohrožení národní bezpečnosti, které se jeví jako skutečné a aktuální nebo předvídatelné."[101] Výše uvedený příkaz musí být zároveň možné podrobit soudnímu přezkumu (nebo přezkumu nezávislého správního orgánu), jehož rozhodnutí je závazné a takový příkaz lze vydat pouze na dobu nezbytně nutnou.[102]

I v souladu s předchozí judikaturou je závěr, že je možná taková úprava, která stanoví s cílem národní bezpečnosti a dále s cílem boje proti závažné trestné činnosti a předcházení závažnému ohrožení veřejné bezpečnosti cílené uchovávání údajů (tj. na základě objektivních a nediskriminačních kritérií kategorií dotčených osob) nebo uchovávání údajů prostřednictvím zeměpisného kritéria, a to vždy na dobu nezbytně nutnou.[103]

Soudní dvůr Evropské unie také připouští takovou národní úpravu, která za účelem zajištění národní bezpečnosti, boje proti trestné činnosti a veřejné bezpečnosti, stanoví plošné a nerozlišující uchovávání údajů o totožnosti (sic!) uživatelů prostředků elektronické komunikace.[104] Důvodem pro umožnění této úpravy je dle Soudního dvora Evropské unie především fakt, že údaje o totožnosti provozovatelé služeb elektronických komunikací v každém jednotlivém případě stejně uchovávají[105] a navíc pouze na základě totožnosti uživatele nelze zjistit datum, čas, dobu trvání ani adresáta uskutečněné komunikace, místo, kde se tato komunikace uskutečnila a ani četnost komunikace s určitými osobami v určitém období. Ergo kontaktní údaje, včetně údajů o totožnosti, nepředstavují dle Soudního dvora Evropské unie závažný zásah do soukromí uživatelů, protože v zásadě tyto údaje o soukromí uživatelů nic neříkají.[106, 107]

Veškeré výše uvedené mechanismy v právních řádech členských států musí být vymezeny natolik jasně a konkrétně, aby představovaly „jasná a přesná pravidla", která jsou nicméně obhajitelná pouze potud, pokud *„zajišťují při uchovávání dotčených údajů dodržení souvisejících hmotněprávních a procesních podmínek a pokud subjekty údajů mají k dispozici účinné záruky proti riziku zneužití"*.[108]

Pravdou nicméně zůstává, že rozsudek ve věci *La Quadrature du Net* do určité míry změkčil velice přísná pravidla pro uchovávání lokalizačních a provozních údajů.[109]

---

100 Ibidem, výrok rozsudku.
101 Ibidem, bod 168 a 177.
102 Ibidem.
103 Ibidem.
104 Ibidem, bod 168.
105 Ibidem, bod 159.
106 Ibidem, bod 157.
107 Nutno podotknout, že tímto závěrem Soudní dvůr Evropské unie spíše než vyjasnění přípustnosti a nepřípustnosti uchovávání údajů vnesl do dané problematiky o něco větší nejistotu. Viz srov. např. SERDULA, N. Plošné uchovávání komunikačních metadat v EU ve světle rozsudku La Quadrature du Net. *Jurisprudence*. 2021, č. 3, s. 39–46.
108 Ibidem, bod 168.
109 SERDULA, N. *Plošné uchovávání komunikačních metadat v EU ve světle rozsudku La Quadrature du Net*, s. 39–46.

Závěrem

Byť dnes již bohatá judikatura Soudního dvora Evropské unie stanovuje určitá kritéria, jak do právních řádů členských států včlenit uchovávání lokalizačních a provozních údajů poskytovateli služeb elektronických komunikací (posledním citovaným rozsudkem dosti komplexní), bylo by jistě vhodné reagovat na judikaturní vývoj unijní normou.

V dohledné době je taková úprava přinejmenším nejistá a její zakotvení dokonce *expressis verbis* vylučuje i návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích) předložený Komisí začátkem roku 2017.[110] *„Tento návrh nezahrnuje žádná zvláštní ustanovení v oblasti uchovávání údajů. Zachovává hlavní myšlenku článku 15 směrnice o soukromí a elektronických komunikacích a přizpůsobuje ji konkrétnímu znění článku 23 obecného nařízení o ochraně osobních údajů, který členským státům poskytuje důvody pro omezení rozsahu povinností a práv uvedených v konkrétních článcích směrnice o soukromí a elektronických komunikacích. Členské státy tak mohou zachovat nebo vytvořit vnitrostátní rámce pro uchovávání údajů, které mimo jiné stanoví cílená opatření pro uchovávání údajů, pokud jsou tyto rámce v souladu s právem Unie a zohledňují judikaturu Soudního dvora týkající se výkladu směrnice o soukromí a elektronických komunikacích a Listiny základních práv.“*[111]

Čl. 15 směrnice o soukromí a elektronické komunikaci je tak v podstatě překopírován do čl. 11 návrhu výše uvedeného nařízení, přičemž ve zbytku se dle odůvodnění návrhu nařízení unijní legislativec spokojil s odkazem na ustálenou judikaturu (což bylo v návrhu uvedeno již v roce 2017, kdy vodítka byla nastavena velmi vágně).[112]

Nutno přesto dodat, že unijní zástupci uchovávání lokalizačních a provozních údajů nespouštějí ze svého hledáčku. Například v roce 2017 Evropská rada vyslovila nutnost spolupráce mezi členskými státy na poli obrany proti teroristickými útoky s důrazem na komunikační kanály teroristy užívanými.[113] V roce 2018 pak Evropská rada vyzvala k přijetí takových prostředků, které umožní Europolu, Eurojustu a příslušným orgánům členských států vzájemnou spolupráci mezi těmito orgány, ale i spolupráci se soukromým sektorem.[114] Též v roce 2018 předložilo Rakousko, tehdy předsedající Radě, zprávu o nutnosti uchovávání údajů harmonizovat (za doprovodu výzvy ministrů spravedlnosti členských států), na jejímž základě pak Rada přijala výzvu k přijetí harmonizační úpravy uchovávání údajů.[115] Rada v tomtéž dokumentu konstatovala, že právě uchovávání údajů je fundamentálním nástrojem pro boj se závažnou kriminalitou, jmenovitě s terorismem

110 Návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích) ze dne 10. 1. 2017, COM(2017) 10 final, 2017/0003 (COD).

111 Ibidem, s. 3.

112 Nicméně zákonodárný proces může podobu nařízení ještě změnit. Rada v dokumentu č. 6078/21 ze dne 10. 2. 2021, kterým se ujímá mandátu pro vyjednávání o nařízení s Evropským parlamentem, nastiňuje možnou podobu ustanovení o uchovávání údajů, které je sice vcelku vágní (čl. 7 odst. 4 návrhu znění nařízení v dokumentu Rady č. 6078/21), je nicméně o něco specifičtější ustanovení než výše uvedený návrh čl. 11 návrhu nařízení předloženého Komisí (které ale návrh Rady ponechává beze změny).

113 Dokument Evropské rady EUCO 8/17 ze dne 23. 6. 2017.

114 Dokument Evropské rady EUCO 13/18 ze dne 18. 10. 2018.

115 Dokument Rady Evropské unie č. 9663/19 ze dne 27. 5. 2019.

a s kyberkriminalitou.[116, 117] V březnu roku 2021 pak Rada během portugalského prezidenství vydala dokument, kterým reflektuje dosavadní soudní vývoj v otázce uchovávání údajů, včetně analýzy posledního rozsudku Soudního dvora Evropské unie ve věci *La Quadrature du Net*, a vyslovila opětovný apel na nutnou harmonizační úpravu této problematiky, při kterézto příležitosti položila ministrům otázky ohledně jejich představy o podobě takové normy.[118]

Byť původní směrnice o uchovávání údajů zohledňuje uchovávání údajů v souvislosti s terorismem a jinou závažnou trestnou činností, je třeba tuto problematiku adresovat i s ohledem na velmi recentní téma. Nutnost uceleného právního rámce s ohledem na uchovávání údajů se projevil i během pandemie COVID-19. Členské státy řešily problematiku trasování nakažených osob, přičemž jediným legálním základem v prostoru Evropské unie pro vyžádání lokalizačních údajů o osobách a jejich následné použití pro trasování těchto osob se zdál být (a stále je) představován čl. 15 směrnice o soukromí a elektronické komunikaci.[119]

Možnost využít údaje uchovávané provozovateli telekomunikačních služeb byla členskými státy podřazena pod v čl. 15 odst. 1 směrnice o soukromí a elektronické komunikaci uvedené *„zajištění národní bezpečnosti a veřejné bezpečnosti“*.[120] Vágnost a relativní přísnost tohoto zmocnění však měly za následek rozlišný přístup jednotlivých členských států. Ostatně výjimečnost užití uchovávání údajů dle čl. 15 odst. 1 potvrzuje i vyjádření evropského inspektora pro ochranu osobních údajů Wojciecha Wiewiórowského, který napsal, že takto uchovaná a získaná data užitá k trasování musí být anonymizována, chráněna sofistikovanými technickými a personálními opatřeními, a především uchovávána po co nejkratší možnou dobu.[121]

Zatímco u nás nebo v Bulharsku bylo trasování pomocí lokalizačních údajů dobrovolné (u nás za pomoci aplikace eRouška), například v Polsku bylo užití aplikace pro trasování povinné. Německo a Rakousko pak zvolily cestu anonymizovaných lokalizačních údajů (pro vytváření map zasažených území) získaných od telekomunikačních operátorů.[122] Podobně anonymně postupovaly i Francie a Itálie, když v souladu se stanovisky svých dozorových úřadů sbíraly přes aplikace pouze anonymní data (respektive pseudonymizované seznamy kontaktů).[123]

Nelze tak než konstatovat, že úprava jednotná pro členské státy EU je nutná. Ať už je to boj s terorismem, kybernetickou kriminalitou nebo sběr a uchovávání údajů pro trasování občanů s ohledem na veřejné zdraví, uchovávání údajů je potřebným nástrojem nabízejícím efektivní řešení.

---

116 Ibidem.

117 Ostatně boj s kyberkriminalitou se svou závažností dostal do apelu již Evropské rady – je tak vidno, že jak Rada, tak Evropská rada si uvědomují závažnost kybernetických útoků a jsou připraveni jim čelit i prostřednictvím *data retention*.

118 Dokument Rady č. 6455/21 ze dne 2. 3. 2021.

119 ETTELDORF, C. EU member state data protection authorities deal with Covid-19: An overview. *European Data Protection Law Review*. 2020, roč. 6, č. 2, s. 268.

120 Ibidem, s. 266.

121 Odpověď evropského inspektora pro ochranu osobních údajů na dotaz ohledně možnosti trasování. Dokument č. C2020-0337.

122 Ibidem, s. 266.

123 Ibidem, s. 268.

Where have we shifted since Declaring Data Retention Directive Invalid

Jaroslav Denemark (https://orcid.org/0000-0002-8304-1312)

Abstract: The European Union is quite efficient in its efforts to protect fundamental rights to privacy and to personal data protection, even during the time of rapid development of communication technologies. Whether it is the European legislator or the EU Court of Justice, the overall approach reflects the todays' modernity. Nonetheless, there have been certain confusion regarding the data retention of personal data by telecommunication services providers for the purpose of transferring the data to the public authorities since the declaration of Data Retention Directive invalid. The aim of this paper is not only to evaluate the effectiveness of European Union's practice within the evolution of new technologies regarding the challenges towards the right to privacy and personal data protection, but also to answer the question of whether we now have clear guidelines for data retention legislation on the national level.

Keywords: data retention, right to privacy, localization data, law and modern technology