Plošné uchovávání komunikačních metadat v EU ve světle rozsudku *La Quadrature du Net*

Ondřej Serdula*

Blanket data retention in the light of the La Quadrature du Net judgement

Summary: *The issue of data retention has attracted significant attention in the past, especially with regards to the Digital Rights Ireland judgement, in which the CJEU invalidated the controversial Data Retention Directive. However, in many aspects, this judgment was just the beginning of the data retention saga, as it was followed by the crucial Tele2 Sverige judgement, in which the CJEU ruled that the blanket data retention of communications metadata is disproportionate per se, no matter the additional safeguards against abuse. Still, many member states, the Commission and even a few of the national courts did not accept these conclusions of the CJEU. That led to several new proceedings, including the recently decided case La Quadrature du Net. The purpose of this article is to consider whether the critique of the Tele2 Sverige judgment was justified, and if so, whether it was sufficiently reflected in the La Quadrature du Net judgment.*

Keywords: *Data retention; communications metadata; traffic and location data; privacy; personal data protection*

Teroristické útoky, ke kterým došlo počátkem 21. století v New Yorku, Londýně a Madridu, společně s rapidním rozvojem technologií, ke kterému došlo v téže době, představovaly úrodnou půdu pro rozšiřování pravomocí státních orgánů působících v oblasti trestního práva a národní bezpečnosti. Jedním z nových nástrojů, který se v tomto období dostal do popředí zájmu, byla *data retention*, tedy – zjednodušeně řečeno – povinné uchovávání komunikačních metadat[1] poskytovateli telekomunikačních služeb za účelem případného pozdějšího adresného přístupu k těmto údajům ze strany příslušných orgánů státu.

Do unijního práva se data retention dostala nejprve prostřednictvím čl. 15 odst. 1 směrnice 2002/58,[2] dle kterého členské státy mohou mj. za účelem prevence, vyšetřování, odhalování a stíhání trestných činů a za účelem zajišťování národní bezpečnosti přiměřeným způsobem omezit zásadu důvěrnosti sdělení, kterou čl. 5 této směrnice obecně stanovuje. Jako příklad takového omezení bylo výslovně zmíněno i opatření umožňující zadržení komunikačních metadat na omezenou dobu. Přijetím směrnice 2006/24[3] se pak z možnosti zavést data retention stala povinnost pro všechny členské státy.

Směrnice 2006/24 byla od svého počátku bezesporu jedním z nejkontroverznějších nástrojů sekundárního práva, a zavádění jejích pravidel do praxe se tak potýkalo se značnými problémy. V některých státech se směrnici vůbec nepodařilo včas provést,[4] zatímco v jiných došlo ke zrušení transpozičních předpisů ústavními soudy pro jejich rozpor s právem na soukromí.[5] Konec směrnice pak přinesl rozsudek Soudního dvora ve věci

* Autor působí v Kanceláři vládního zmocněnce pro zastupování České republiky před Soudním dvorem EU a je externím doktorandem na katedře evropského práva PF UK. Veškeré názory vyjádřené v tomto článku jsou výhradně jeho vlastní. E-mail: oserdula@gmail.com.

1 Tj. údajů souvisejících se sdělením odlišných od obsahu komunikace. Jde např. o údaje o účastnících komunikace, způsobu komunikace, čase komunikace, místě komunikace apod. Tyto údaje bývají někdy členěny na údaje provozní (nezbytné zejména k přenosu sdělení), lokalizační (nezbytné k lokalizaci zařízení) a údaje o totožnosti uživatelů, nazývané také údaje o předplatitelích (nezbytné zejména k vyúčtování služeb).

2 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).

3 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 2002/58/ES.

4 Směrnice nebyla včas transponována v Řecku, Irsku, Nizozemsku, Lucembursku, Švédsku a Rakousku. Za neprovedení směrnice ve stanovené lhůtě byly Švédsko, Rakousko, Irsko a Řecko později dokonce odsouzeny Soudním dvorem. Švédsko bylo následně dokonce odsouzeno znovu a byla mu v této souvislosti uložena finanční sankce, která mu však byla po zrušení směrnice 2006/24 Komisí navrácena. Srov. FIODOROVA, A. *Information Exchange and EU Law Enforcement*. Routledge 2018, nestránkováno.

5 Pro přehlednou analýzu rozhodnutí vnitrostátních ústavních soudů v oblasti data retention viz KOSTA, E. The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection. *SCRIPTed-A Journal*

Digital Rights Ireland,[6] ve kterém SDEU směrnici zrušil pro její rozpor s čl. 7, 8 a 52 odst. 1 Listiny.

Rozsudek Digital Rights Ireland ovšem neznamenal konec data retention v unijním právu. Vnitrostátní předpisy transponující směrnici 2006/24 zůstaly samozřejmě nadále v platnosti, přičemž čl. 15 odst. 1 směrnice 2002/58 zavedení data retention ve vnitrostátním právu nadále výslovně umožňoval. Co je však důležitější – ani Soudní dvůr ve věci Digital Rights Ireland, ani předtím ústavní soudy členských států neodmítly koncept data retention jako takový. Jejich závěry se totiž týkaly především absence dodatečných záruk proti zneužití v oblasti uchovávání údajů a přístupu k nim. Jinými slovy – nebyla řešena otázka *jestli*, ale spíše otázka *jak*.

V tomto ohledu představoval zásadní obrat rozsudek Tele2 Sverige,[7] ve kterém Soudní dvůr rozhodl, že čl. 15 odst. 1 směrnice 2002/58 vykládaný ve světle čl. 7, 8 a 11 Listiny brání plošnému a nerozlišujícímu uchovávání komunikačních metadat *jako takovému*, bez ohledu na dodatečné záruky, čímž došlo ke zpochybnění základního stavebního kamene data retention. Přesto ani rozsudek Tele2 Sverige nevedl ke konci diskuze o data retention v unijním právu. Bylo tomu tak z důvodu, že závěry Soudního dvora nebyly v praxi přijaty řadou klíčových aktérů. Krom vlád členských států se striktním přístupem Soudního dvora nesouhlasila ani Evropská komise, a co je důležitější, ani řada vnitrostátních soudů, dle kterých přístup Soudního dvora nepřikládal dostatečnou váhu bezpečnostním zájmům členských států.[8] Byla tak zahájena další řízení, jejichž předmětem se stala právě polemika se striktním přístupem Soudního dvora zastávaným ve věci Tele2 Sverige. Jedním z těchto případů byla věc La Quadrature du Net, v níž byl rozsudek Velkého senátu Soudního dvora vynesen 6. října 2020.[9]

Cílem tohoto článku je především shrnutí, analýza a kritické zhodnocení judikatury SDEU týkající se (ne)přípustnosti plošného uchovávání komunikačních metadat. Za tímto účelem je článek rozdělen do třech částí. V první části bude vysvětleno, z jakých důvodů představuje plošnost uchovávání komunikačních metadat nejen hlavní problém z hlediska slučitelnosti data retention s čl. 7, 8 a 11 Listiny, ale zároveň nezbytný předpoklad účinnosti tohoto nástroje. V další části práce bude přiblížen rozsudek Soudního dvora ve věci Tele2 Sverige a některé jeho problémy. Na závěr se text bude věnovat tomu, jak Soudní dvůr tento přístup změnil ve věci La Quadrature du Net, jakož i otázce, zda tento nový přístup Soudního dvora dostatečným způsobem reaguje na nedostatky předchozí judikatury.[10]

Plošné uchovávání údajů jakožto základní stavební kámen data retention

Díky plošnému charakteru uchovávání údajů bývá data retention označována za nástroj spočívající v preventivním plošném sledování komunikace.[11] S ohledem na to, jak právní úpravy data retention v členských státech EU v praxi fungují, se však jedná o poněkud zavádějící tvrzení. Ačkoliv totiž data retention spočívá v plošném *uchovávání* komunikačních metadat, k *přístupu* k těmto údajům může docházet pouze v individuálních případech. Data retention tak v žádném případě nevede k vytvoření jakési databáze komunikačních metadat, v níž by mohly příslušné orgány členských států volně vyhledávat. Tyto údaje jsou uloženy u poskytovatelů služeb až do doby, než se objeví souvislost s konkrétním trestným činem či hrozbou pro národní bezpečnost a – s výjimkou naléhavých případů – než je přístup k nim povolen ze strany soudu. Pokud v určité, zpravidla několikaměsíční lhůtě od vzniku údajů tato souvislost nalezena není, dojde k jejich automatickému smazání. Podstata typické právní

of Law, Technology and Society, 2013, roč. 10, č. 3, str. 339363. Srov. také MYŠKA, M. Aktuální otázky data retention. *Revue pro právo a technologie*, 2010, roč. 1, č. 1, str. 13–16.

6 Rozsudek Soudního dvora ze dne 8. dubna 2014, *Digital Rights Ireland a Seitlinger a další*, C-293/12, EU:C:2014:238.

7 Rozsudek Soudního dvora ze dne 21. prosince 2016, *Tele2 Sverige a Watson a další*, spojené věci C-203/15 a C698/15, EU:C:2016:970.

8 Srov. předkládací rozhodnutí v řízení před Soudním dvorem ve věci C-140/20 *Commissioner of the Garda Síochána*, body 5–8; ve věci C-793/19 *Spacenet*, body 17–31; ve věci C-623/17 *Privacy International*, body 3–6 či ve věci C-511/18 *La Quadrature du Net*, bod 23. Všechna předkládající rozhodnutí jsou dostupná na http://curia.europa.eu/. Pro další polemiku se závěry Soudního dvora srov. také nález Ústavního soudu ČR ze dne 14. května 2019, Pl. ÚS 45/17, body 76–82.

9 Rozsudek Soudního dvora ze dne 6. října 2020, *La Quadrature du Net a další*, spojené věci C-511/18, C 512/18 a C-520/18, EU:C:2020:791. Po vynesení rozsudku ve věci *La Quadrature du Net* se Soudní dvůr zabýval problematikou data retention také v rozsudku *Prokuratuur*. Ten se však týkal téměř výhradně problematiky přístupu k uchovávaným údajům, přičemž co se týče problematiky samotného plošného uchovávání, Soudní dvůr v něm toliko odkázal na věc *La Quadrature du Net*. Z tohoto důvodu není rozsudek *Prokuratuur* v tomto článku blíže rozebírán. Srov. rozsudek Soudního dvora ze dne 2. března 2021, *Prokuratuur*, C-746/18, EU:C:2021:152, bod 30. Srov. také stanovisko GA Pitruzzelly ze dne 21. ledna 2020 ve věci *Prokuratuur*, C-746/18, EU:C:2020:18, bod 51.

10 Článek se záměrně soustředí toliko na unijní rovinu dotčené problematiky. Byť analýza judikatury Soudního dvora v této oblasti může dle názoru autora přispět k diskuzi o otázkách souvisejících s data retention na vnitrostátní úrovni, tyto otázky stojí mimo zaměření tohoto článku, a proto zde nejsou řešen.

11 VOBOŘIL, J. Ústavní soud posvětil plošné sledování elektronické komunikace. In: *Lupa.cz* [online]. 23. 5. 2019. Dostupné na <https://www.lupa.cz/clanky/ustavni-soud-posvetil-plosne-sledovani-elektronicke-komunikace/>

úpravy data retention je tak velice odlišná od sledovacích programů, které používají např. zpravodajské služby USA a které skutečně spočívají v hromadné analýze sdělení. Soudní dvůr i vnitrostátní soudy navíc vyžadují, aby právní úpravy data retention obsahovaly řadu dodatečných záruk v rovině uchovávání i přístupu.[12]

To samozřejmě neznamená, že by data retention nepředstavovala zásah do základních práv. Tento zásah je navíc bezesporu extrémně rozsáhlý (jelikož se týká veškerých uživatelů služeb elektronické komunikace) i poměrně závažný (s ohledem na vysokou vypovídací hodnotu některých těchto údajů o soukromí osob). Nicméně je třeba si uvědomit, v čem spočívá pravá podstata tohoto zásahu. Kritici data retention – stejně jako Soudní dvůr – spatřují zásah do soukromí způsobený data retention v tom, že z uchovaných údajů lze „vyvozovat velmi přesné závěry o soukromém životě osob", včetně těch osob, „v jejichž případě neexistuje důvod se domnívat, že by jejich chování mohlo, byť nepřímo nebo vzdáleně, souviset se závažnou trestnou činností".[13] Tyto závěry lze však vyvozovat až na základě přístupu k těmto údajům. Pokud bychom tedy žili v ideálním světě, ve kterém si můžeme být jisti, že k uchovávaným údajům bude přistupováno jen v zákonem vymezených případech, samo uchovávání by nepředstavovalo větší problém. Veškeré otázky o nezbytnosti a přiměřenosti právní úpravy data retention by se soustředily na to, jak tyto oprávněné případy vymezit. Rizika spojená se samotným uchováváním údajů by prakticky odpadla. Samozřejmě, v reálném světě nikdy takovou jistotu mít nemůžeme. Zásah do základních práv způsobený již samotným uchováváním údajů proto spočívá v tom, že riziko neoprávněného přístupu nelze nikdy vyloučit. Již samo uchovávání tak může v některých osobách vyvolávat „pocit, že je jejich soukromí pod neustálým dohledem".[14]

Plošnost uchovávání je však nejen hlavním problémem data retention z hlediska její přiměřenosti, ale bohužel také nezbytným předpokladem její účinnosti. Podstata data retention spočívá v tom, že příslušným orgánům je umožněno v určitých případech „číst minulost", tedy např. získat přístup ke komunikačním metadatům podezřelého z doby, kdy toto podezření ještě neexistovalo. Podstata data retention tak nemůže být zachována, aniž by docházelo k uchovávání komunikačních metadat týkajících se osob, u kterých v daném okamžiku neexistuje souvislost s určitou bezpečnostní hrozbou.

O tom, jak důležité takové čtení minulosti může v moderním kontextu být, přitom nemůže být pochyb. Dojde-li např. k sérii vloupání, můžeme data retention použít ke zjištění, zda se určitý mobilní telefon v rozhodnou dobu nacházel na více místech činu. Dojde-li k únosu, může být nenahraditelná možnost lokalizovat telefon oběti. V případě vraždy může být zase zcela zásadní zjistit, s kým oběť komunikovala bezprostředně před tím, než byla usmrcena. Obdobných případů, z nichž je užitečnost data retention zcela zjevná, lze přitom uvést nespočet.

Význam data retention navíc roste v souvislosti s tím, jak roste význam elektronické komunikace v každodenním životě. V dnešní době lze jen těžko očekávat, že by komunikace mezi pachateli trestného činu či mezi obětí a pachatelem byla zachycena v jiné než elektronické podobě. Samo páchání trestných činů se mnohdy přesouvá do kyberprostoru, přičemž dochází ke vzniku řady nových, značně společensky nebezpečných trestných činů, jež jsou páchány převážně či výhradně prostřednictvím internetu. Prostředí internetu je přitom charakteristické tím, že v něm žádné stopy nevznikají náhodně. Zatímco v případě „běžného" trestného činu lze spoléhat na to, že onen „pohled do minulosti" poskytnou příslušným orgánům výpovědi svědků, stopy v blátě či otisky prstů, v prostředí internetu žádná obdobná stopa nevznikne, resp. ne bez předem jasně daného technologického pravidla. Těchto skutečností si jsou pachatelé samozřejmě dobře vědomi, a proto dnes hojně využívají prostředků komunikace na dálku. Zatímco tedy v minulosti bychom o data retention hovořili jako o užitečném nástroji pro boj proti bezpečnostním hrozbám, s tím, jak se celý náš život (včetně trestné činnosti a terorismu) přesouvá do kyberprostoru, stává se z data retention nástroj nejen užitečný, ale – přinejmenším z pohledu příslušných orgánů členských států – také nezbytný.

[12] V rovině uchovávání jde především o omezení doby uchovávání údajů na nezbytné minimum, povinnost uchovávat údaje na území Unie a zajištění mimořádně vysoké úrovně zabezpečení údajů. Co se týče zpřístupňování údajů, to je – s výjimkou údajů o předplatitelích – možné pouze za účelem boje proti závažné trestné činnosti. Je vyžadováno, aby ve vnitrostátní právní úpravě byl vymezen jak okruh trestných činů, tak okruh orgánů, které mohou o údaje žádat. S výjimkou naléhavých situací je vyžadován předchozí souhlas soudu i následná notifikace dotčených osob.

[13] Rozsudek Tele2 Sverige, c. d., bod 105.

[14] Ibidem, bod 100.

Tele2 Sverige a požadavek na cílené uchovávání

Ve věci Digital Rights Ireland se Soudní dvůr přípustností plošného uchovávání údajů jako takového explicitně nezabýval. Soudní dvůr sice v rámci posuzování závažnosti zásahu do základních práv způsobeným směrnicí 2006/24 přikládal velkou váhu tomu, že se povinnost uchovávání vztahuje i na osoby, v jejichž případě neexistuje jakákoliv souvislost s trestnou činností,[15] ovšem důvodem ke zrušení směrnice byla krom rozsahu a závažnosti zásahu především neexistence dostatečných záruk proti zneužití.[16] Otázka přípustnosti plošného uchovávání jako takového tak reálně vyvstala až ve věci Tele2 Sverige, která se týkala právních úprav data retention ve Švédsku a Spojeném království, a to v návaznosti na výslovný dotaz správního odvolacího soudu ve Stockholmu.

Generální advokát v souladu s názory vlád členských států a Komise a s odkazem na podstatu data retention, která spočívá ve „čtení minulosti", dospěl k závěru, že plošné uchovávání je přípustné, ovšem pouze při stanovení přísných podmínek v oblasti uchovávání a přístupu k údajům.[17] Soudní dvůr však zaujal opačný postoj. Soudní dvůr v prvé řadě navázal na své závěry z věci Digital Rights Ireland, když vyhodnotil zásah způsobený data retention jako rozsáhlý (vzhledem k tomu, že se vztahuje na všechny účastníky elektronické komunikace) a zvlášť závažný (vzhledem k tomu, že na základě komunikačních metadat lze činit přesné závěry o životě osob).[18] Klíčovým argumentem pro odmítnutí data retention se pak stala zásada důvěrnosti sdělení obsažená ve směrnici 2002/58. Dle Soudního dvora představuje uchovávání komunikačních metadat *výjimku* z této zásady, která musí být vykládána restriktivně, a tudíž nemůže mít plošnou povahu, jelikož v takovém případě by se stala *pravidlem*.[19]

Soudní dvůr dále uvedl, že čl. 15 odst. 1 směrnice 2002/58 vykládán ve světle čl. 7, 8 a 11 Listiny nebrání tomu, aby členský stát přijal právní úpravu, která umožňuje preventivní *cílené* uchovávání komunikačních metadat, které je omezené co do kategorií uchovávaných údajů, komunikačních prostředků, dotčených osob a doby uchovávání. Dle Soudního dvora je dále nezbytné, aby se povinnost uchovávání vztahovala pouze na okruh osob, jejichž údaje mohou vykázat minimálně nepřímou souvislost se závažnou trestnou činností, což lze zajistit například prostřednictvím omezení povinnosti uchovávání pouze na oblasti, ve kterých existuje zvýšené riziko přípravy či páchání závažných trestných činů.

Tento přístup Soudního dvora byl problematický hned v několika ohledech. Zaprvé, jak ostatně upozornil i předtím generální advokát, lze zpochybňovat samotný přístup k data retention jako k výjimce ze zásady důvěrnosti sdělení, která musí být vykládána restriktivně.[20] Nic o výjimečném charakteru uchovávání údajů či o vyloučení jeho plošného charakteru nevyplývá přímo ze znění čl. 15 odst. 1 směrnice 2002/58. Toto ustanovení je navíc nadepsáno „Použití některých ustanovení směrnice 95/46/ES", na rozdíl od čl. 10 směrnice 2002/58, který je výslovně nadepsán jako „Výjimky". Čl. 5 odst. 1 směrnice 2002/58 navíc uvádí, že zásada důvěrnosti sdělení spočívá v zákazu zachycování komunikace jinými osobami než uživateli „bez souhlasu dotčených uživatelů, pokud k takovému jednání nejsou zákonem oprávněny v souladu s čl. 15 odst. 1." Účelem zásady důvěrnosti sdělení dle čl. 5 odst. 1 směrnice 2002/58 tak dle mého názoru bylo, aby k zachycování komunikace nedocházelo bez souhlasu či bez zákonného podkladu, nikoliv to, aby k jakémukoliv zákonnému zachycování komunikace mohlo docházet pouze ve výjimečných případech. V neposlední řadě je třeba vzít v potaz i znění bodu 11 odůvodnění směrnice, dle kterého směrnice 2002/58 „*nemění stávající rovnováhu mezi právem jednotlivce na soukromí a možností, aby členské státy přijaly opatření uvedená v čl. 15 odst. 1 této směrnice*, […] Tato směrnice se tedy *nedotýká možnosti členských států provádět zákonné zachycování elektronických sdělení* nebo přijímat jiná opatření, je-li to nezbytné pro některý z těchto účelů a je-li to v souladu s Evropskou úmluvou o ochraně lidských práv a základních svobod, jak je vykládána v rozhodnutích Evropského soudu pro lidská práva. Tato opatření musí být vhodná, plně přiměřená vzhledem k zamýšlenému účelu a nezbytná

15 Rozsudek *Digital Rights Ireland*, c. d., body 56–59.
16 Ibidem, body 60–68.
17 Sanovisko GA Saugmansgaarda Øe ze dne 19. července 2016 ve věci Tele2 Sverige a Watson a další, spojené věci C-203/15 a C-698/15, EU:C:2016:572, bod 261.
18 Rozsudek Tele2 Sverige, c. d., bod 100.
19 Ibidem, body 97 a 104–106.
20 Srov. stanovisko GA ve věci *Tele2 Sverige*, c. d., body 109–110.

v demokratické společnosti a musí být předmětem odpovídajících záruk v souladu s Evropskou úmluvou o ochraně lidských práv a základních svobod."[21] Mám proto vážné pochybnosti o tom, že čl. 5 a 15 odst. 1 směrnice 2002/58 zákonodárce opravdu zamýšlel tak, jak je Soudní dvůr nakonec vyložil.

Ovšem nejde pouze o chápání uchovávání údajů jako výjimky z pravidla, ale obecněji taktéž o míru závažnosti, kterou Soudní dvůr přisuzuje zásahu do základních práv způsobenému samotným uchováváním údajů. Byť nelze se Soudním dvorem polemizovat ohledně nevídaného *rozsahu* zásahu do základních práv z hlediska počtu dotčených osob, je otázkou, zda nedochází k přílišnému nadhodnocení *závažnosti* zásahu způsobeného toliko uchováváním údajů. Jak bylo uvedeno výše, skutečný zásah do základních práv způsobený uchováváním údajů spočívá v riziku neoprávněného přístupu, které však lze prostřednictvím dodatečných zásad poměrně efektivně minimalizovat přinejmenším na úroveň, která se příliš neliší od jiných nástrojů, jež mají příslušné orgány členských států v tomto ohledu k dispozici.

Je navíc otázkou, do jaké míry je samo plošné uchovávání údajů v praxi schopno vyvolávat v širší populaci významnější *chilling effect*, vezmeme-li v potaz masivní zpracování (nejen uchovávání) rozmanitých kategorií osobních údajů (nejen metadat), které dnes běžně provádějí soukromé subjekty (provozovatelé vyhledávačů, sociálních sítí apod.) za komerčními účely (jejichž váha je ve srovnání s cíli sledovanými data retention bezesporu nižší). Samozřejmě lze namítat, že v případě těchto komerčních zpracování má subjekt zpravidla volbu, zda s takovým zpracováním udělí souhlas. O tom, do jaké míry se jedná o skutečnou možnost volby, by však bylo možné polemizovat.[22] To, že jsou metadata ve značném rozsahu uchovávána i pro vlastní komerční účely samotných poskytovatelů telekomunikačních služeb, pak dokládají statistiky. Např. v Německu po zrušení právní úpravy data retention Spolkovým ústavním soudem příslušné orgány zjistily, že se k potřebným údajům nedostanou zhruba pouze ve 4 % případů.[23] To, že poskytovatelé služeb pro vlastní účely uchovávají většinu těchto údajů, potvrzují i údaje z Dánska[24] či České republiky.[25] Tato skutečnost dokládá, že „dodatečný" zásah do základních práv způsobený data retention se pravděpodobně zásadněji neliší od rozsahu zásahu do základních práv způsobeného uchováváním údajů pro komerční účely. Tento dodatečný zásah má však vysokou přidanou hodnotu, jelikož vylučuje, aby se úspěšnost vyšetřování trestného činu či odvrácení hrozby pro národní bezpečnost odvíjela *de facto* od náhody, zda údaje nezbytné pro vyšetřování nebudou právě v tom malém procentu údajů, které se poskytovatel služeb rozhodl neuchovávat pro vlastní potřebu.

Zásadním problémem konceptu cílené data retention, jak jej Soudní dvůr v rozsudku načrtl, je jeho praktická nerealizovatelnost. Jde o to, jak v praxi data retention účinně omezit jen na určité časové období, určité zeměpisné oblasti či okruh určitých osob a zároveň zachovat účinnost tohoto nástroje. V současnosti asi není možné tvrdit, že by se závažná trestná činnost obecně vyskytovala pouze v určitém časovém období. Lze si sice představit, že by se k plošné data retention přistoupilo např. v případě indicií o předpokládaném teroristickém útoku. V takovém případě je ale značně omezen potenciál data retention jakožto nástroje ke čtení minulosti, jelikož k ukládání údajů bude docházet až v době po vzniku takového podezření. Zároveň se tím značně omezuje okruh trestných činů, k jejichž potírání může být data retention využito. Obdobně je to s územním zacílením. Např. hrozba teroristických činů je primárně spojena s velkými aglomeracemi, totéž ale nelze tvrdit v případě jiné závažné trestné činnosti. K přípravě a plánování těchto činů může navíc docházet na zcela jiném místě, než na kterém jsou následně realizovány. V případě trestných činů páchaných prostřednictvím internetu pak možnost územního omezení odpadá zcela. Totéž platí pro zaměření na určité osoby, jelikož i to je závislé na prvotní identifikaci souvislosti mezi těmito osobami a určitou hrozbou. Nelze také zapomínat na to, že jedním ze základních požadavků na jakoukoliv úpravu umožňující skryté zpracování osobních údajů je její jasnost a předvídatelnost. Pokud by však měla být předvídatelně stanovena kritéria pro zacílení data retention, pachatelé závažných

[21] Zvýraznění doplněno.
[22] Ke skutečné roli souhlasu se zpracováním údajů v dnešním kontextu viz např. MÍŠEK, J. Souhlas se zpracováním osobních údajů za časů Internetu. *Revue pro právo a technologie*, 2014, roč. 5, č. 9, s. 3–74.
[23] Srov. European Digital Righs. *Shadow evaluation report on the Data Retention Directive (2006/24/EC)* [online], 2011, s. 13. Dostupné na <https://edri.org/files/shadow_drd_report_110417.pdf>
[24] Ibidem, s. 14.
[25] Srov. nález Ústavního soudu sp. zn. Pl. ÚS 45/17, c. d., bod 89.

trestných činů by se mohli povinnosti uchovávat údaje poměrně snadno vyhnout. Identifikace určitých rizikových oblastí či okruhů osob by také v mnoha případech mohla narážet na problémy spojené se zákazem diskriminace.

S ohledem na výše uvedené zřejmě není divu, že žádný z členských států neprovedl koncept cílené data retention do praxe.[26] Není ani divu, že v následujících řízeních před Soudním dvorem týkajících se data retention všechny zúčastněné členské státy i Komise usilovaly o přehodnocení zákazu plošného uchovávání údajů. Pochybnosti ohledně toho, zda přístup Soudního představuje nalezení odpovídající rovnováhy mezi základními právy ve smyslu čl. 7, 8 a 11 Listiny a bezpečnostními zájmy členských států, byly zjevné i z předkládacích rozhodnutí v těchto věcech.[27] Co více, v mezidobí se k problematice zpracovávání osobních údajů osob, u nichž v okamžiku zpracování neexistuje souvislost s hrozbou pro veřejnou bezpečnost, vyjádřil i Evropský soud pro lidská práva, který dospěl k závěru, že ani hromadné režimy skrytého sledování komunikace za účelem boje proti bezpečnostním hrozbám nejsou v rozporu s čl. 8 Úmluvy, existují-li odpovídající záruky proti zneužití.[28] Na výše uvedené výhrady reagoval Soudní dvůr právě v navazujícím rozsudku La Quadrature du Net, jehož předmětem byly francouzská a belgická právní úprava data retention.

La Quadrature du Net a výjimky ze zákazu plošného uchovávání

Když se požadavkem na přehodnocení striktního zákazu plošného uchovávání zabýval generální advokát, zastával názor, že Soudní dvůr by měl na svém požadavku na cílené uchovávání setrvat.[29] Nicméně dle generálního advokáta bylo možné požadavku Soudního dvora na cílené uchovávání dostát nejen zacílením na zvláštní skupiny osob nebo zeměpisné oblasti (které jsou z výše uvedených důvodů prakticky nerealizovatelné), ale také prostřednictvím omezením kategorií uchovávaných údajů.[30] Dle generálního advokáta by tak požadavek Soudního dvora na cílenou data retention mohl být splněn, pokud by sice docházelo k uchovávání údajů o všech uživatelích, ovšem kategorie uchovávaných údajů a doba uchovávání by byly omezeny tak, aby takto uchované údaje neumožnily poskytnout podrobný obraz o životě dotčených osob (tj. zejména vytváření profilů osob).[31] Doba uchovávání jednotlivých kategorií údajů by se dále měla odvíjet na jedné straně od toho, v jaké míře umožňují tyto údaje vyvozovat přesné závěry o životě osob, a na druhé straně od toho, v jaké míře jsou tyto údaje nezbytné pro cíle sledované dotčenou právní úpravou.[32]

Mám za to, že přístup navrhovaný generálním advokátem nechává – na rozdíl od přístupu zastávaného Soudním dvorem ve věci Tele2 Sverige – prostor pro skutečné hledání rovnováhy mezi dotčenými zájmy. Ne všechny údaje jsou stejně citlivé z hlediska soukromí dotčených osob. Ne všechny údaje jsou stejně užitečné pro zajišťování bezpečnosti. Řešení, které sice *a priori* nevylučuje plošné uchovávání, avšak zároveň od členských států vyžaduje, aby omezily riziko vytváření profilů osob na absolutní minimum, je z mého pohledu správnou cestou.

Přesto je třeba upozornit na dva problematické aspekty. Zaprvé, v praxi nebude možné zcela zabránit tomu, že na základě uchovaných dat bude možné v určitých případech vyvozovat přesné závěry o životě osob. I když budou uchovávány jen omezené kategorie metadat a jen po velmi omezenou dobu, může dojít k tomu, že i tyto údaje budou mít potenciál odhalit velmi citlivé informace o soukromí osob. Ostatně, i informace o jediném volaném čísle může např. odhalit citlivé údaje o zdravotním stavu, půjde-li např. o číslo kliniky zabývající se léčbou pacientů s HIV. To však nic nemění na tom, že při velmi krátkých lhůtách pro uchovávání zejména citlivějších kategorií údajů (nejčastěji těch lokalizačních) lze riziko vytváření jakýchsi ucelených profilů osob, ve kterém Soudní dvůr zjevně spatřuje hlavní rizika spojená s data retention, značně minimalizovat. Zadruhé, jen stěží lze právní úpravu, která umožňuje preventivní uchovávání (byť

[26] Eurojust. *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 – Report* [on-line], 2017, s. 6 a 12. Dostupné na <https://www.statewatch.org/media/documents/news/2017/nov/eu-eurojust-data-retention-MS-report-10098-17.pdf>

[27] Srov. předkládací rozhodnutí citovaná v poznámce pod čarou č. 8.

[28] Srov. rozsudek ESLP ze dne 13. září 2018 ve věci Big Brother Watch v. Spojené království, stížnosti č. 58170/13, 62322/14, a 24960/15, CE:ECHR:2018:0913JUD005817013, body 314 až 316.

[29] Stanovisko GA Campos Sánchez-Bordony ze dne 15. ledna 2020 ve věci Ordre des barreaux francophones a germanophone a další, C-520/18, EU:C:2020:7, bod 72. Tato věc byla následně pro účely rozsudku spojena s věcmi La Quadrature du Net a další, C-511/18 a C-512/18.

[30] Ibidem, bod 92.

[31] Ibidem, body 83 a 93.

[32] Ibidem, bod 97.

omezeného množství) komunikačních metadat o všech uživatelích elektronické komunikace, považovat za cílenou data retention v tom smyslu, jak ji měl na mysli Soudní dvůr ve věci Tele2 Sverige. Proto když členské státy o obdobném řešení hovořily v rámci pracovních skupin Rady, které řešily dopady rozsudku Tele2 Sverige, záměrně jej neoznačovaly jako *cílenou* data retention, ale jako *omezenou* data retention.[33]

Soudní dvůr se nicméně cestou naznačenou generálním advokátem nevydal, byť došlo k poměrně zásadní modifikaci striktního zákazu plošného uchovávání. Ten byl sice v obecné rovině Soudním dvorem zachován, avšak bylo z něj nově umožněno několik výjimek. První z těchto výjimek se týká údajů o totožnosti uživatelů prostředků elektronické komunikace, v případě kterých Soudní dvůr nově nejenže výslovně povolil plošné uchovávání, avšak zároveň uvedl, že k tomuto uchovávání může docházet i za účelem boje proti trestné činnosti obecně, nikoliv pouze závažné trestné činnosti. Dle Soudního dvora totiž tyto údaje samy o sobě neumožňují zjistit datum, čas, dobu trvání, místo, četnost či adresáta komunikace uskutečněné v určitém období. Zásah, který s sebou nese uchovávání těchto údajů, tak dle Soudního dvora v zásadě nelze považovat za závažný.[34] Poněkud zarážející je ale to, že tento mírnější přístup platí dle Soudního dvora pouze tehdy, „nemohou-li uvedené údaje být spojeny s informacemi o uskutečněných komunikacích".[35] Krom toho, že v praxi budou často tyto údaje potřebné právě k identifikaci autora určitého sdělení, je otázkou, jak by tato „nemožnost spojení s dalšími údaji" měla být v praxi zajištěna v rámci samotného uchovávání údajů. Zdá se tedy, že Soudní dvůr zamýšlel svůj požadavek směřovat spíše do roviny přístupu, v tom smyslu, že zatímco přístup např. k údaji o totožnosti majitele SIM karty, která byla vložena do odcizeného telefonu, může být umožněn i za účelem vyšetřování méně závažné trestné činnosti (krádeže), přístup např. k informaci o totožnosti majitele SIM karty za účelem identifikace autora určité SMS zprávy může být umožněn pouze za účelem vyšetřování závažné trestné činnosti. Způsob, jakým Soudní dvůr svůj požadavek naformuloval, je každopádně matoucí. Samotné plošné uchovávání údajů tohoto druhu v praxi jednoduše nemůže být podmíněno tím, že tyto údaje v budoucnu nebude možné spojit s jinými údaji.

Plošné uchovávání – ovšem pouze na nezbytně nutnou dobu a za účelem boje proti závažné trestné činnosti a hrozbám v oblasti národní bezpečnosti – připustil Soudní dvůr také v případě IP adres. Soudní dvůr tímto krokem výslovně reagoval na skutečnost, že v případě trestného činu spáchaného on-line může IP adresa představovat jediný prostředek umožňující identifikovat osobu, které byla tato adresa přidělena v okamžiku spáchání tohoto trestného činu.[36] Rozdíl mezi přístupem Soudního dvora k IP adresám na straně jedné a k údajům o identitě uživatelů na straně druhé pak spočívá v tom, že na IP adresy může být navázána internetová historie uživatele.[37] IP adresy představují klíčový nástroj pro vyšetřování trestné činnosti páchané prostřednictvím internetu, a zmírnění přístupu Soudního dvora bylo tedy rozhodně namístě.

Soudní dvůr zároveň připustil, aby docházelo k plošnému uchovávání ostatních komunikačních metadat, ovšem pouze po omezenou dobu, pokud existují dostatečně konkrétní okolnosti svědčící o tom, že dotčený členský stát čelí aktuální či předvídatelné závažné hrozbě pro národní bezpečnost, přičemž konstatování existence této hrozby musí podléhat Soudnímu přezkumu.[38] V těchto případech Soudní dvůr dokonce připustil, že takto uchované údaje mohou být automaticky hromadně analyzovány za účelem odhalení osob představujících bezpečnostní riziko, za podmínky, že kritéria této analýzy jsou nediskriminační a že každý pozitivní výsledek je přezkoumán za použití neautomatizovaných prostředků.[39]

Francouzská Státní rada v návaznosti na tyto závěry Soudního dvora celkem nepřekvapivě rozhodla, že Francie v současnosti takové aktuální a závažné hrozbě čelí, a plošné uchovávání metadat za účelem ochrany národní bezpečnosti je tak v současnosti ve Francii přípustné. Své závěry Státní rada odůvodnila tím, že v roce 2020 bylo ve Francii spácháno šest teroristických útoků a v roce 2021 byly již dva teroristické útoky úspěšně odvráceny. Krom toho Státní rada poukázala

33 Ibidem, bod 92 a zde citované dokumenty pracovních skupin Rady.
34 Rozsudek *La Quadrature du Net a další*, c. d., bod 157.
35 Ibidem, bod 158.
36 Ibidem, bod 154.
37 Ibidem, bod 153.
38 Ibidem, bod 134–139.
39 Ibidem, 172–182.

na to, že Francie konstantně čelí vysokému riziku zahraniční špionáže s ohledem na své vojenské, technologické a ekonomické kapacity.[40] Je otázkou, do jaké míry hodlá Soudní dvůr v budoucnu závěry vnitrostátních soudů ohledně existence aktuální a závažné hrozby ospravedlňující plošné uchovávání metadat přehodnocovat, dostane-li k tomu možnost. Nemůže být totiž pochyb o tom, že případné přehodnocování takových závěrů ze strany Soudního dvora vyvolává zásadní otázky ohledně rozdělení pravomocí mezi členské státy Unii, vzhledem k tomu, že dle čl. 4 odst. 2 SEU je národní bezpečnost výhradní odpovědností členských států.[41]

Co je však důležitější, výše uvedený přístup z mého pohledu potvrzuje, že Soudní dvůr nadále poněkud nedůvodně nadhodnocuje rizika spojená s plošným uchovávaním provozních a lokalizačních údajů. To lze dobře demonstrovat právě tím, že stanovuje *de facto* stejné podmínky pro plošné uchovávání údajů jako pro jejich plošnou automatizovanou analýzu. Právě v možnosti plošné automatické analýzy provozních a lokalizačních údajů osobně spatřuji ta největší rizika spojená se zpracováním komunikačních metadat. Tato rizika jsou neporovnatelně vyšší, než je tomu v případě typických právních úprav data retention spočívajících v plošném uchovávání údajů a adresném přístupu k nim, navíc při stanovení přísných záruk v rovině uchovávání i přístupu. To, že je oba tyto nástroje možné použít za stejných podmínek (tj. pouze v případě aktuálního či předvídatelného závažného ohrožení národní bezpečnosti), tedy z hlediska přiměřenosti nepovažuji za rozumné řešení. Z mého pohledu není vhodné stejným způsobem přistupovat k opatření, jež umožňuje automatickou analýzu metadat celé populace za účelem hledání potenciálních pachatelů, jako k opatření, jež ukládá povinnost tato metadata pouze ukládat za účelem individuálního přístupu k nim na základě předchozího povolení soudu, ukáže-li se takový přístup jako nezbytný v konkrétním případě.

Závěr

Přestože umožnění výjimek ze striktního zákazu plošného uchovávání ve věci La Quadrature du Net představuje krok správným směrem, mám za to, že tento zákaz měl být spíše zcela opuštěn ve prospěch tzv. omezené data retention, tj. přístupu, který sice umožňuje plošné uchovávání komunikačních metadat, ovšem za dodržení opravdu přísných dodatečných záruk v oblasti uchovávání i přístupu k údajům. Klíčovou roli by v tomto ohledu měla hrát hlavně doba uchovávání, jež by měla být omezena na absolutní minimum, aby bylo v co největší míře vyloučeno, že uchovávaná data umožní sestavení podrobného profilu osob.[42] Mám za to, že ačkoliv Soudní dvůr svůj předchozí extrémně přísný přístup věci Tele2 Sverige svým rosudkem ve věci La Quadrature du Net z rozumných důvodů zmírnil, nadále nedůvodně nadhodnocuje rizika spojená se samotným plošným uchováváním komunikačních metadat, aniž by bral v potaz, že riziko neoprávněného přístupu lze zejména v moderních demokratických státech, kterými členské státy EU rozhodně jsou, poměrně účinně minimalizovat. Toto nadhodnocování intenzity zásahu způsobeného plošným uchováváním provozních a lokalizačních údajů je zřetelné, zejména pokud vezmeme v potaz masivní zpracování rozmanitých kategorií osobních údajů, které dnes běžně provádějí soukromé subjekty za komerčními účely, jejichž význam je ve srovnání s cíli sledovanými data retention bezesporu nižší.

40 I přesto byla část napadených vnitrostátních předpisů Státní radou shledána v rozporu s právem EU z důvodu, že nevyhovovala některým dalším požadavkům Soudního dvora, např. kvůli tomu, že plošné uchovávání metadat umožňovala i za jinými cíli, než je ochrana národní bezpečnosti, či že nevyžadovala souhlas soudu pro přístup zpravodajských služeb k uchovávaným údajům. Srov. Conseil d'État. *Connection data: the Council of State conciliates the implementation of European Union law and the effectiveness of the fight against terrorism and crime* [on-line], 2021. Dostupné na <https://www.conseil-etat.fr/en/news/connection-data-the-council-of-state-conciliates-the-implementation-of-european-union-law-and-the-effectiveness-of-the-fight-against-terrorism-and>

41 Blíže k této problematice viz SERDULA, O. K rozšiřování věcné působnosti unijních pravidel na ochranu osobních údajů ze strany SDEU. *Právník*, 2020, roč. 159, č. 8, str. 641–660.

42 Na tomto místě je vhodné doplnit, že navrhovaný přístup není v rozporu s pozdějšími závěry Soudního dvora v rozsudku *Prokuratuur*. V něm sice Soudní dvůr uvedl, že i v případech, kdy je přistupováno k údajům jen z velmi krátkého časového období, představuje takový přístup závažný zásah do základních práv, a je tudíž možný pouze za účelem vyšetřování závažných trestných činů, nikoliv trestných činů obecně. Jak však bylo uvedeno výše, tento případ se týkal výhradně podmínek přístupu k uchovávaným údajům, nikoliv podmínek plošného uchovávání údajů. Srov. rozsudek *Prokuratuur*, c. d., body 27–45.