Odporuje česká právní úprava data retention právu Evropské unie?

JAROSLAV DENEMARK*

Does Czech data retention legislation contravene EU law?

Summary: *The obligation of telecommunications network operators to retain traffic and location data had already been known to the Czech legal system before the infamous data retention directive came into force. The original data retention legislation was even repealed by the Constitutional Court of the Czech Republic before the judgment of the Court of Justice of the European Union, popularly called Digital Rights Ireland. However, the new version of the legislation was reviewed again by the Constitutional Court of the Czech Republic, but this time the legislation was found to be in line with the constitutional order. However, the question remains whether the Czech legislation is compatible with EU law, as the CJEU has already given some guidance in several cases on the admissibility of the nationwide retention of telecommunications metadata.*

Keywords: *Data Retention, Electronic Communications Act, traffic and location data, Court of Justice of the European Union*

Od roku 2005 je v České republice stanovena povinnost pro provozovatele telekomunikačních sítí plošně uchovávat provozní a lokalizační údaje. Ve své podstatě kontroverzní institut musel projít ještě před bohatou unijní judikaturou zabývající se stejným tématem posouzením ústavnosti ze strany Ústavního soudu České republiky (dále jen „**ÚS**"). Byť se ÚS nijak extenzivně nezabýval tehdy ještě platnou směrnicí 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 (dále jen „**směrnice o data retention**"), případně čl. 15 odst. 1 směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (dále jen „**ePrivacy směrnice**"), jsou jeho původní nálezy zásadní pro posouzení dalšího postupu českého zákonodárce a jeho úspěchu při zohlednění připomínek ÚS, které se velice podobají nosným argumentům pozdější judikatury Soudního dvoru Evropské unie (dále jen „**SDEU**").

ÚS nejdříve zhodnotil, že úprava data retention obsažená v § 97 odst. 3 zák. č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, (dále jen „**ZEK**") obsahující povinnost provozovatelů telekomunikačních sítí uschovávat provozní a lokalizační údaje je nesouladná s právem na informační sebeurčení, a tedy s ústavním pořádkem České republiky.[1] Stejně ÚS zhodnotil související právní úpravu obsaženou v § 88a zák. č. 141/1961 Sb., o trestním řízení soudním (dále jen „**trestní řád**"), pročež dotčené úpravy zrušil.[2]

I přes nově přijaté znění výše uvedených institutů se ÚS musel znovu vypořádat s jejich ústavní konformitou. V novém posouzení však ÚS došel k závěru, že úprava již splňuje test proporcionality a neodporuje tedy základním právům zaručeným Listinou základních práv a svobod ČR.[3]

* Autor působí jako interní doktorand na katedře evropského práva PF UK. E-mail: jaroslav.denemark@gmail.com. ORCID ID: 0000-0002-8304-1312. Tento text byl zpracován v rámci projektu studentského vědeckého výzkumu „Vývoj finančněprávní a trestněprávní regulace pod vlivem normotvorby Evropské unie", SVV 260 493.

1 Nález č. 94/2011 Sb. Ústavního soudu ze dne 22. března 2011, sp. zn. Pl. ÚS 24/10, ve věci návrhu na zrušení § 97 odst. 3 a 4 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a na zrušení vyhlášky č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání (dále jen „**Pl. ÚS 24/10**").

2 Nález č. 43/2012 Sb. Ústavního soudu ze dne 20. prosince 2011, sp. zn. Pl. ÚS 24/11, ve věci návrhu na zrušení § 88a zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů (dále jen „**Pl. ÚS 24/11**").

3 Nález Ústavního soudu ze dne 14. května 2019, sp. zn. Pl. ÚS 45/17, ve věci návrhu na zrušení § 97 odst. 3 a 4 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších

Během toho, kdy v České republice probíhal boj o ústavnost úpravy uchovávání údajů, probíhal na úrovni Evropské unie zápas o přípustnost této úpravy z pohledu Evropského práva. Příznačné je, že data retention provázely kontroverze již od legislativního procesu. Směrnice o data retention byla přijata v režimu tehdejšího prvního, komunitárního pilíře, když dle mnoha členských států měla být přijata v režimu pilíře třetího, protože upravovala problematiku justiční a policejní, spadající do dikce členských států. Zvolený proces přijímání směrnice eskaloval v první soudní přezkum, jemuž právní úprava čelila. SDEU nicméně zvolený způsob Komisí podpořil a žaloba Irska za podpory Slovenské republiky tedy nebyla úspěšná.[4]

V prvním soudním posouzení zabývajícím se meritem směrnice o data retention, tj. souladem unijní úpravy s primárním právem Evropské unie, již SDEU směrnici o data retention zrušil.[5] Vágnost, přílišná extenzivnost a neodůvodněnost zásahu a další problematické body unijní úpravy stojící za prohlášením směrnice o data retention za neplatnou *ab initio* nicméně zapříčinily v jednotlivých členských státech Evropské unie značnou nejistotu.[6] V některých členských státech tamní ústavní soudy úpravu data retention zrušily pro nesouladnost se závěry SDEU, v některých členských státech pospíchali s novelizací předmětných dotčených ustanovení tak, aby se alespoň částečně přizpůsobily byť prozatím relativně neurčitým požadavkům vyjádřeným v rozsudku Digital Rights Ireland, jiné členské státy, jako například Slovensko, plně opustily koncept data retention a přistoupily k tzv. data freezing.[7]

Postupně se však přetrvávající úpravy jednotlivých členských států začaly dostávat ve formě předběžných otázek k přezkumu SDEU. Zásadními rozsudky, které dále rozváděly nebo modifikovaly podmínky pro data retention stanovené ve věci Digital Rights Ireland, byly především ve spojené věci C-203/15 a C-698/15 s populárním názvem Tele2Sverige[8], ve věci C-207/16 s populárním názvem Ministerio Fiscal[9], ve věci C-623/17 s populárním názvem Privacy International[10] a především ve spojených věcech C-511/18, C-512/18 a C-520/18 s populárním názvem La Quadrature du Net.[11, 12]

Tento příspěvek má za úkol propojit dva přístupy k data retention, tj. přístup v České republice a Evropské unii. Je nutné se ptát, zda je česká právní úprava data retention souladná s možností aplikace výjimky dle čl. 15 odst. 1 ePrivacy směrnice. V první řadě se zaměřím na analýzu přístupu ÚS a možnosti užití jeho argumentace pro balanční test souladnosti české právní úpravy s unijním výkladem. Druhým krokem je aplikace podmínek stanovených SDEU ve výše uvedených případech na dikci české právní úpravy data retention společně s konfrontací se závěry ÚS a následné vyvození závěru, zda by česká právní úprava obstála v případě přezkumu SDEU.

Přístup Ústavního soudu České republiky

1) Pl. ÚS 24/10

Dne 26. 3. 2010 podala skupina 51 poslanců návrh k ÚS na zrušení ustanovení § 97 odst. 3 a 4 ZEK a prováděcí vyhlášky č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě způsobu jejich předávání orgánům oprávněným k jejich využívání, pro jejich nesoulad s ústavním pořádkem.

ÚS svou argumentaci založil především na obhajobě práva na respekt k soukromému životu a práva na informační sebeurčení. ÚS tak hned na začátku vytyčuje pole odůvodnění a dále rozvádí, že rozvoj technologický a technický je úzce spjat jak s požadavky na soukromí, tak i na svobodu „ohrožující potenciál státu".[13] Tím je v zásadě velmi dobře vyjádřena základní sporová hranice dvou argumentačních táborů vyslovujících se k data

předpisů, § 88a zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, § 68 odst. 2 a § 71 písm. a) zákona č. 273/2008 Sb., o Policii České republiky, a vyhlášky č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů, sbírka 161/2019, částka 69/2019 (dále jen „**Pl. ÚS 45/17**").

4 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.

5 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.

6 MUNIR, A., MOHD YASIN, S., ABU BAKAR, S. Data Retention Rules A Dead End. *European Data Protection Law Review*, roč. 3, č. 1, str. 75.

7 Ibidem, 74.

8 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.

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

10 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.

11 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.

12 Dále pak k vývoji přístupu SDEU k data retention a podrobný popis vývoje úpravy v DENEMARK, J. Kam jsme se posunuli od zrušení směrnice o uchování údajů. *Právník: teoretický časopis pro otázky státu a práva*. Praha: Ústav státu a práva AV ČR. ISSN 0231-6625, roč. 2021, č. 12.

13 Ibidem, bod 28.

retention. Tedy že technologický pokrok s sebou přináší svobodu, jež ale potenciálně může ohrozit veřejnou bezpečnost, ulehčuje komunikaci teroristickým skupinám, přináší nové výzvy s ohledem na páchání trestné činnosti a stát proti těmto hrozbám musí bojovat, zároveň ale technologický pokrok přináší další výzvy pro ochranu soukromí a práva na informační sebeurčení.

Ono právo na informační sebeurčení, jež je těžištěm i dalších nálezů ÚS dotýkajících se soukromí v digitálním světě, dovozuje ÚS z čl. 10 odst. 3 (ochrana údajů o své osobě) a čl. 13 (ochrana listovního tajemství) Listiny základních práv a svobod ČR a toto právo je třeba interpretovat ve spojitosti s právy garantovanými čl. 7 (nedotknutelnost osoby), 8 (procesní záruky trestního řízení), 10 (lidská důstojnost a soukromí) a 12 (nedotknutelnost obydlí) Listiny základních práv a svobod ČR.[14] ÚS konstatuje, že „… v podmínkách vševědoucího a všudypřítomného státu a veřejné moci se svoboda projevu, právo na soukromí a právo svobodné volby chování a konání stávají prakticky neexistujícími a iluzorními.“[15]

Dle konstatování ÚS může dojít k omezení osobní integrity a soukromí osob ze strany veřejné moci jen zcela výjimečně, je-li to v demokratické společnosti nezbytné a nelze-li sledovaného účelu dosáhnout jinými prostředky. Navíc takové omezení musí být založeno jen zákonem a musí dodržovat konkrétní záruky proti libovůli. Musí být stanoveny dostatečné garance a záruky proti zneužití pravomoci ze strany státní moci, čehož má být docíleno odpovídající právní úpravou a existencí účinné kontroly uplatňování těchto pravomocí, jež vykonává nezávislý a nestranný soud.[16]

Nadto právní úprava omezující osobní integritu a soukromí osob musí být přesná, zřetelná ve svých formulacích, dostatečně předvídatelná, musí striktně definovat pravomoci udělené příslušným orgánům, způsob a pravidla výkonu těchto pravomocí. Nakonec musí být dotčená právní úprava podrobena klasickému testu proporcionality.

Předně ÚS stanovil najisto, že byť není sbírán samotný obsah zpráv, lze z daných lokalizačních a provozních údajů „sestavit detailní informaci o společenské nebo politické příslušnosti, jakož i o osobních zálibách, sklonech nebo slabostech jednotlivých osob.“[17] Tím jednoznačně dochází k významnému zásahu do soukromí osob a práva na informační sebeurčení stejně, jako by byl ukládán obsah samotných zpráv.

ÚS právní úpravě vyčetl, že je příliš neurčitá v osobách, jimž mohou být ukládané údaje sděleny,[18] taktéž není jednoznačně vymezen účel, za jakým mohou být údaje předávány, a v zásadě tak bylo možné vyžádat provozní a lokalizační údaje v jakémkoli probíhajícím trestním řízení za účelem odhalení jakkoliv závažného trestného činu.[19] Taková úprava nemůže dle ÚS naplnit druhý krok testu proporcionality.

Úprava data retention nadto nestanovovala žádná pravidla obsahující alespoň minimální požadavky (technické, organizační) na zabezpečení uchovávání údajů, a tak žádný z dotčených subjektů nemá záruky proti zneužití jejich údajů a svévole třetích osob. Tím, že povinnost ukládání leží na soukromých osobách, jsou navíc posunuty „hranice mezi privátním a veřejným prostorem“.[20]

Za „zcela nedostačující“ označil ÚS vymezení povinnosti uchovávat údaje po dobu „ne kratší než 6 měsíců a delší než 12 měsíců“, přičemž po uplynutí této doby je nutné údaje zlikvidovat. Přitom ale není stanoveno, jak s údaji po dobu uložení nakládat, jak zajistit jejich ochranu, a především jak je poté zlikvidovat.[21] Úprava navíc postrádá jakoukoli efektivní soudní ochranu, ať už bezprostřední nebo následnou, čímž brání jednotlivcům účinné ochraně.[22]

Již na základě výše uvedeného ÚS stanovil dotčenou právní úpravu za neplatnou, když není naplněn ani druhý krok z testu proporcionality. Neubránil se ale konstatování v podobě *obiter dictum*, v němž vyjádřil skepsi nad plošným a preventivním uchováváním provozních a lokalizačních údajů obecně, tj. zda je takový nástroj vůbec nezbytný a přiměřený.[23]

2) Pl. ÚS 24/11

Nedlouho po vynesení výše uvedeného rozsudku byla ÚS předložena žádost o přezkoumání související úpravy s již přezkoumaným

14 Ibidem, bod 31.
15 Ibidem, bod 30.
16 Ibidem, bod 36.
17 Ibidem, bod 44.
18 Ibidem, bod 46.
19 Ibidem, bod 47.
20 Ibidem, bod 50.
21 Ibidem, bod 51.
22 Ibidem.
23 Ibidem, bod 55.

§ 97 odst. 3 a 4 ZEK, tj. úprava vztahující se k procesní úpravě získání ukládaných provozních a lokalizačních údajů orgány činnými v trestním řízení dle § 88a trestního řádu. Návrh na zrušení předmětné úpravy byl předložen Obvodním soudem pro Prahu 6 v řízení o nařízení zpřístupnění provozních a lokalizačních údajů policii za účelem objasnění trestné činnosti.[24]

Argumentace ÚS v zásadě vychází z nálezu Pl. ÚS 24/10, když meritum odůvodnění nálezu vychází z práva na respekt k soukromému životu v podobě práva na informační sebeurčení. V nynějším nálezu byly stejně tak stanoveny i podmínky přezkumu.[25]

Dotčená právní úprava dle ÚS nestanovuje „dostatečné garance proti zneužití předmětných údajů během celého trvání trestního řízení.“[26] Navíc je textace § 88a trestního řádu flagrantně vágní, kdy jedinou podmínkou pro vydání uložených údajů je, že se užijí k „objasnění skutečností důležitých pro trestní řízení.“ V takovém případě si údaje orgány činné v trestním řízení mohou vyžádat vždy, když prokáží ať už sebemenší souvislost s probíhajícím trestním řízením nehledě na závažnost spáchaného trestného činu či na možnost užít jiné důkazní prostředky.[27]

Ostatně ona neurčitost je dle ÚS největším nedostatkem přezkoumávané právní úpravy. Pro dotčené osoby je taková právní úprava nepředvídatelná a soudy nejsou s to zajistit dostatečnou ochranu základním právům a svobodám, když jejich rozhodovací praxí nelze nahradit v zásadě politická rozhodnutí.[28]

ÚS dále podotýká, že v případné nové právní úpravě musí být náležitě stanoveny postupy zacházení s vyžádanými provozními a lokalizačními údaji ze strany orgánů činných v trestním řízení, jasná pravidla pro zabezpečení těchto údajů a pro zničení údajů, které již nejsou potřeba. Dotčené subjekty by navíc měly být informovány, že jejich provozní a lokalizační údaje byly předány státním orgánům tak, aby měly možnost žádat soudní přezkum příslušného rozhodnutí.[29]

Na základě výše uvedených argumentů tak ÚS po vzoru nálezu Pl. ÚS 24/10 napadenou právní úpravu zrušil.

Pokud bychom měli stručně zopakovat argumenty ÚS v obou předešlých případech, je třeba uvést, že napadená právní úprava data retention a související procesní podmínky vyžádání si provozních a lokalizačních údajů ze strany orgánů činných v trestním řízení trpěla zvláště nedostatkem přesnosti, zřetelnosti, neobsahovala dostatečné záruky ochrany dotčených subjektů, byla příliš široká a neodůvodněným způsobem příliš extenzivně zasahovala do práva na informační sebeurčení. Zajímavé je, že v zásadě přesně tyto argumenty opakuje SDEU v rozhodnutí Digital Rights Ireland, kterým byla směrnice o data retention prohlášena za neplatnou. Přitom ÚS se ani v jednom z výše analyzovaných nálezů nevyslovuje k problémům dotčené směrnice a pouze konstatuje, že šíře směrnice umožňuje členským státům přijmout takovou právní úpravu (tj. uplatnit takovou diskreci), jež bude v souladu s ústavním pořádkem toho kterého členského státu.

3) Pl. ÚS 45/17

Nejzajímavější je však pro náš účel poslední nález ÚS, kterým byla úprava data retention společně se související procesní úpravou v trestním řádu [a v zák. č. 273/2008 Sb., o Policii ČR (dále jen „**ZPol**“)] přezkoumána. Tentokrát však nová právní úprava testem ústavnosti prošla. ÚS se musel nicméně vypořádat nejen se svými předešlými argumenty, byť vyjádřenými k dikci zrušené právní úpravy, ale též k rozsudkům ve věci data retention ze strany SDEU.

ÚS se v počátku své argumentace aktivně hlásí ke své vlastní prejudikatuře, když jako východisko pro posouzení ústavnosti napadené právní úpravy stanovuje především právo na informační sebeurčení.

ÚS neopominul zmínit i uvedené nálezy SDEU, kdy konstatuje, že data retention je problematika unijní, a byť původní směrnice byla zneplatněna, musí národní právní úprava dbát „nosných důvodů rozsudku SDEU, jímž byla dotčená unijní úprava zneplatněna.“[30]

Zajímavé je, že ve shrnutí prejudikatury ÚS přímo píše, že v rozhodnutí Tele2Svergie SDEU stanovil, že není akceptovatelná taková právní úprava, která z výjimky v čl. 15 odst. 1 ePrivacy směrnice stanovuje pravidlo, tj. není akceptovatelná právní úprava stanovující plošné a nerozlišující uchovávání velkého množství dat.[31] Zajímavé to je z toho

[24] Pl. ÚS 24/11, bod 1 a 2.
[25] Ibidem, bod 19.
[26] Ibidem, bod 23.
[27] Ibidem, bod 24.
[28] Ibidem.
[29] Ibidem, bod 27.
[30] Pl ÚS 45/17, bod 55.
[31] Ibidem, bod 60.

důvodu, že se s tímto argumentem ÚS dále v nálezu nevypořádal, byť závěry SDEU připomíná v nálezu vícekrát a navíc explicitně uvádí, že SDEU shledává plošný sběr provozních a lokalizačních metadat nejen v rozporu s čl. 15 odst. 1 ePrivacy směrnice, ale též v rozporu s čl. 7 a 8 Listiny základních práv Evropské unie. K tomuto je v nálezu pouze konstatováno, že mezi členskými státy nedošlo s ohledem na problematiku data retention k politické shodě.[32] Vypořádání se však s tak silnými závěry SDEU považuji ze strany ÚS za hrubě nepřesvědčivé, když z nich ani implicitně nevyplývá, proč by měla být česká úprava souladná se závěry v rozhodnutí ve věci Tele2Sverige.

ÚS v nálezu uvádí, že i kdyby neexistovala úprava stanovující povinnost data retention, provozní a lokalizační údaje by stejně byly shromažďovány, a to jak z nutných technických důvodů samotných operátorů, tak za účelem marketingu na základě souhlasu samotných subjektů (jak totiž vypověděla zástupkyně operátora při ústním jednání, až 70 % uživatelů dává souhlas ke zpracování údajů pro marketingové účely).[33] S tímto argumentem však nelze souhlasit a je nutné se přiklonit k argumentům soudkyně Šimáčkové uvedeným v jejím disentu k nálezu. ÚS se dopouští zjednodušování závěrů a míchání několika účelů ke zpracování dohromady.

Data retention je státem vynucená povinnost, kdy jsou údaje subjektů uchovávány po dobu minimálně 6 měsíců a mají k nim přístup orgány činné v trestním řízení a další subjekty při splnění stanovených podmínek. Údaje za účelem marketingu jsou uchovávány pouze na základě svobodného a informovaného souhlasu subjektů a tento souhlas může být kdykoliv odvolán. Navíc dané subjekty tento souhlas udělily, protože chtějí dostávat marketingová sdělení – vymezený účel zpracování je pro ně tedy dokonce kýžený. Další údaje uchovávané operátory za účelem samotného poskytování služeb nedosahují takového množství a retenční doba je také zásadně kratší (dle výslechu při ústním jednání 2 měsíce). Domnívám se proto, že tento analogický příměr používá ÚS chybně.[34]

ÚS dále argumentuje, že i kdyby byla úprava data retention zrušena (a s tím související procesní postup získání uchovávaných údajů v trestním řádu a dalších předpisech), doposud explicitně oprávněné orgány by si našly jinou cestu, tj. jiný mechanismus, jak dané údaje získat, a to často invazivnější, než je tomu doposud. ÚS tak raději než vytvoření „legislativního stínu" zrušením napadené úpravy volí cestu „menšího zla", kdy ponechává danou právní úpravu netknutou.[35]

Uvedený argument je však taktéž nepřesvědčivý, když ÚS má k dispozici instituty, kterými by předešel „legislativnímu stínu". Mohl právní úpravu zrušit, poskytnout jasná vodítka, co a jak je třeba doplnit, konkretizovat, kde je třeba přísnějších pravidel atd., a stanovit delší časový odklad vykonatelnosti nálezu.[36]

S ohledem na test proporcionality je v prvním kroku stanoveno, že cíl sledovaný dotčenou právní úpravou je legitimní[37], odpovídající silnému veřejnému zájmu.[38]

V druhém kroku testu proporcionality ÚS uvádí, že zkoumaná úprava data retention nemá ekvivalent, protože každá jiná úprava (např. data freezing) nedovoluje takový rozsah přístupu k údajům z minulosti. Je proto v zásadě naplněn požadavek potřebnosti, protože jednoduše nynější úprava data retention nemůže být ničím nahrazena. Tento argument ÚS považuji taktéž za zkratkovitý a chybně interpretující nahraditelnost napadené právní úpravy. Jak ostatně sám ÚS v úvodu nálezu konstatuje, např. v Německu zvolili kombinaci méně invazivního data retention a data freeze. Slovenská republika data retention opustila úplně a zvolila pouze přístup data freeze, přičemž tyto země mají obdobné výsledky při užití těchto institutů.[39] S ohledem na požadavek minimalizace zásahu by tak tyto instituty naopak měly být logickou alternativou k dnes velmi invazivnímu data retention.

S ohledem na třetí krok proporcionality se ÚS postupně zabývá retenční dobou, zabezpečením uchovávaných provozních a lokalizačních údajů, a to včetně podmínek přístupu k provozním a lokalizačním údajům.

Dobu 6 měsíců pro uchování provozních a lokalizačních údajů považuje ÚS za přiměřenou, a to hned z několika důvodů. Nejprve je konstatováno, že zákonodárce vybral tu

32 Ibidem, bod 74.
33 Ibidem, bod 76–77.
34 Obdobně Kateřina Šimáčková, bod 13 disentu k nálezu Pl. ÚS 45/17.
35 Pl. ÚS 45/17, bod 78–79.
36 Obdobně Kateřina Šimečková, bod 14 disentu k nálezu Pl. ÚS 45/17.
37 Odhalování trestné činnosti, pátrání po osobách pohřešovaných či ztracených, boj proti terorismu, činnost zpravodajských služeb, dohled nad kapitálovým trhem.
38 Pl. ÚS 45/17, bod 83–85.
39 Bod 11 disentu Kateřiny Šimáčkové k nálezu Pl. ÚS 45/17

nejmenší možnou dobu pro uchování podle směrnice o data retention.[40] Nutno podotknout, že v době posuzování této právní úpravy byla směrnice o data retention neplatná již přes 5 let, a byť tuto skutečnost i ÚS výslovně zmiňuje, nemůže to být „polehčující okolností". Zákonodárce měl totiž alespoň 5 let na úpravu doby uchovávání provozních a lokalizačních údajů odlišné od nejkratší možné dle směrnice o data retention, nicméně tak neučinil. Shledávám proto tento argument ÚS jako nepřesný.

Dále je argumentováno, že operátoři stejně dle ústní výpovědi zástupkyně jednoho z nich uchovávají některé údaje pro marketingové účely získané na základě souhlasu uživatelů po dobu 6 měsíců.[41] Jak nicméně uvedeno výše, uchovávání údajů pro marketingové účely na základě souhlasu nelze v žádném případě srovnávat s povinností data retention.

ÚS v této souvislosti nepředkládá příliš přesvědčivé argumenty, spíše se uchyluje k obecnějším tvrzením typu: „Nikdy neexistuje jediné správné řešení, jak určitou oblast společenských vztahů správně regulovat."[42] A dále, že: „Je však na zákonodárci, jaké řešení při úpravě doby uchovávání provozních a lokalizačních údajů a přístupu k nim zvolí. Šetří-li přitom soukromí jednotlivce tak, aby právní úprava *data retention* odpovídala reálné potřebě využití provozních a lokalizačních údajů, nepřísluší Ústavnímu soudu do jeho legislativní pravomoci zasahovat."[43] Jako by snad ÚS zapomněl na svou úlohu a alibisticky se vyhýbal větší intervenci do „zákonodárné činnosti", což je ve světle návrhu na zrušení právního předpisu, tj. v zásadě jediné reálné možnosti, jak může ÚS do zákonodárné činnosti zasáhnout, v důsledku až úsměvné.

Úroveň regulace zabezpečení uchovávaných provozních a lokalizačních údajů shledává ÚS také za dostatečnou. ÚS především kvituje, vzhledem k nemožnosti práva dostatečně rychle reagovat na technický pokrok, obecnější úpravu obsaženou v ZEK a ponechání technických podrobností na vyhlášce.[44] Dále je odkazováno především na § 88 ZEK, který stanovuje podmínky pro zpracování a uchovávání údajů, jež obsahuje povinnosti provozovatelů komunikačních sítí a zároveň odkazuje na specializované předpisy, přičemž v tomto ohledu jsou především relevantní předpisy zabývající se ochranou osobních údajů (GDPR, zák. č. 110/2019 Sb., o zpracování osobních údajů).

Následně se ÚS zabývá podmínkami přístupu k provozním a lokalizačním údajům, a to nejdříve v režimu trestního řízení a dále dle ZPol.

Dle zkoumané právní úpravy v § 88a odst. 1 trestního řádu je možné vyžádat si provozní a lokalizační údaje pouze v souvislosti se stíháním úmyslných trestných činů s horní hranicí trestní sazby nejméně tři roky a dále pro taxativně vyčtené trestné činy především v souvislosti s kyberkriminalitou a pro trestné činy, k jejichž stíhání zavazuje mezinárodní smlouva, jíž je Česká republika vázána.[45] V tomto smyslu skutečně došlo ke kvalitativnímu posunu v porovnání s předchozí právní úpravou, což je kvitováno i ÚS.[46]

Zákonodárcem uvedené trestné činy by nicméně měly spadat pod pojem „závažné trestné činnosti", který požaduje judikatura SDEU jako jediný možný účel pro užití provozních a lokalizačních údajů v rámci vyšetřování trestných činů.[47] Tento pojem sice není definován, ale zároveň nemůže být posuzován jako samoúčelný. ÚS přitom pouze konstatuje, že je ponechán členským státům prostor pro uvážení a s ohledem na „výsledky dokazování je Ústavní soud shledává přiměřeným".[48] Taková argumentace nicméně nemůže postačovat. Argumentem *ad absurdum* by se totiž dalo říci, že pokud by provozní a lokalizační údaje opět byly přístupné pro všechny typy trestných činů, také by výsledky dokazování mohly ukázat, že takové údaje přispívají k odhalování všech typů trestné činnosti. Pouhé „výsledky dokazování" ale nenapovídají nic o závažnosti trestné činnosti. V rámci řízení bylo sice (výslechem svědků) dle ÚS prokázáno, že nedochází ke zneužívání mechanismu vyžádání si ukládaných metadat, tolik nicméně s ohledem pro povolené trestné činy dle § 88a odst. 1 trestního řádu. Pokud bychom měli na „závažnost" trestného činu, jak činí ÚS, nahlížet tím, že data retention pomáhá při vyšetřování uvedených trestných činů, mohli bychom říct, že pokud bude data retention povoleno pro všechny trestné činy, jsou všechny trestné činy závažné.

40 Pl. ÚS 45/17, bod 89.
41 Ibidem.
42 Ibidem, bod 92.
43 Ibidem.
44 Ibidem, bod 93.
45 § 88 odst. 1 Trestního řádu.
46 Pl. ÚS 45/17, bod 100–101.
47 Tele2Sverige, body 49 a 50.
48 Pl. ÚS 45/17, bod 106.

Kam svými argumenty ÚS ostatně míří, vysvětluje sám dále v odůvodnění, kdy zdůrazňuje, že kriminalita se čím dál více přesouvá do kyberprostoru a k objasnění je třeba elektronických stop, přičemž absenci data retention spojuje s „bezzubostí" státu v rámci zajištění bezpečnosti a odhalování takovéto trestné činnosti.[49] V této souvislosti je opět třeba souhlasit s Kateřinou Šimáčkovou, která trefně glosuje přístup zbytku pléna, kde převládl názor „čím více se kriminalita přesouvá online, tím více musíme omezit soukromí a hledat další řešení pro větší pravomoci státu". Naopak by se ale dalo tvrdit, že čím víc se přesouvá život do světa online, tím více je třeba hledat prostředky, jak chránit exponované soukromí. V tomto smyslu se zákonodárce za podpory ÚS uchyluje s ohledem na data retention k doktríně „nice to have", když by s ohledem na ochranu lidských práv mělo převládnout pouhé „need to know".[50]

Pozitivní dle ÚS taktéž je, a s tím lze jistě souhlasit, že k vydání provozních a lokalizačních údajů je třeba předchozího a řádně odůvodněného soudního rozhodnutí[51] a až na určité výjimky je uživatel o předání metadat vyrozuměn a má možnost obrátit se na Nejvyšší soud s žádostí o přezkum.[52]

V ZPol není, na rozdíl od trestního řádu, stanovena povinnost informovat subjekt údajů o vydání lokalizačních dat[53] a není ani třeba předchozího soudního rozhodnutí k vyžádání si těchto dat od operátorů. ÚS nicméně toto právní úpravě odpouští především s ohledem na to, že se dle jeho názoru jedná o výjimečné, jasně definované situace, kdy je třeba jednat v jednotkách minut, maximálně hodin k ochraně lidského života. ÚS se přitom odvolává na rozhodnutí ve věci Tele2Sverige, kde se uvádí, že záruky přístupu k údajům chránící před libovůlí jsou vyžadovány s výjimkou naléhavých případů.[54] Tato argumentace není ale příléhavá, když v režimu ZPol lze vyžádat údaje k pátrání jak po osobě pohřešované, tak po osobě hledané, včetně identifikace nalezené mrtvoly. Jistě si lze představit naléhavý zájem u pátrání po pohřešované osobě, zvlášť v případě více chráněných osob jako dětí či starých lidí, nicméně u osob hledaných (tj. typicky osoby, která se nedostavila k výkonu trestu odnětí svobody) či u identifikace nalezených mrtvol si lze naléhavý případ představit jen stěží. ÚS se tak při své argumentaci dopouští přílišného zobecnění daných institutů, když je k nim třeba přistupovat rozdílně, a navíc vytrhuje závěry SDEU z kontextu, jak je demonstrováno dále v tomto příspěvku.

ÚS tak konstatuje, že absence soudního rozhodnutí není překážkou užití mechanismu dle ZPol, když lze tuto absenci soudního rozhodnutí zhojit interními postupy, předpisy, evidencemi a možnými postihy v rámci Policie ČR.[55] Dle mého názoru nelze ale požadavek soudního rozhodnutí nahradit „interními postupy, předpisy, evidencemi a možnými postihy uvnitř Policie ČR", když tyto stejné záruky jsou tak jako tak přítomné i v případě žádosti o vydání provozních a lokalizačních údajů v rámci trestního řízení a v případě trestního řízení byla absence předchozího odůvodněného soudního rozhodnutí shledána jako nepřekonatelná překážka pro data retention.

ÚS zdůvodňuje rozdílný přístup k trestnímu řízení a procesům v ZPol především tím, že procesy dle ZPol nelze zahájit „bez konkrétního podnětu", přičemž tento podnět by sám o sobě musel být nezákonný, aby došlo k nezákonnému vyžádání si provozních a lokalizačních metadat.[56] Navíc mechanismus vyžádání si provozních a lokalizačních metadat je dle ÚS velmi formalizovaný, a než dojde k podání samotné žádosti, projde mnoha dalšími kontrolními procesy uvnitř Policie ČR.[57] I přesto vnitřní mechanismy uvnitř jednoho orgánu dle mého názoru jednoduše nemůžou nahradit rozhodnutí nezávislého soudu, a to už z toho důvodu, že (byť odlišné) útvary uvnitř Policie ČR jsou stále „pod jednou střechou". Role nezávislého třetího nemůže být nikdy nahrazena vnitřními postupy, evidencemi a kárnými tresty uvnitř jednoho orgánu.

Na základě výše uvedeného se domnívám, že přezkum nynějšího znění české úpravy data retention ÚS není přesvědčivý. Souhlasím v dané věci s Kateřinou Šimáčkovou, když tvrdí, že dle jejího názoru nemusí být data retention *a priori* protiústavní, nicméně v dnešní podobě by spíše za protiústavní měla být prohlášenou.[58]

49 Ibidem.
50 Bod 11 a 12 disentu Kateřiny Šimáčkové k nálezu Pl. ÚS 45/17.
51 Ibidem, bod 107.
52 Ibidem, bod 108.
53 V režimu ZPol lze vyžádat pouze lokalizační data, nikoliv také provozní.
54 Pl. ÚS 45/17, bod 114.
55 Ibidem, bod 116.
56 Ibidem, bod 112.
57 Ibidem.
58 Disent Kateřiny Šimáčkové k nálezu Pl. ÚS 45/17.

Co se týká judikatury SDEU, ÚS se k ní vyjadřuje sporadicky. Buď tvrdí, že přezkoumávaná právní úprava je v souladu s dosavadní judikaturou, přičemž spíše nesystematicky vybírá pouze určité instituty, které zdánlivě odpovídají požadavkům SDEU. V případě jasného rozporu české právní úpravy se závěry SDEU se ÚS uchyluje k obecným prohlášením, která nikterak nereagují na nosné argumenty vyjádření unijním soudem. Z nálezu ÚS tak není patrné, především proč by měla být česká právní úprava data retention souladná s judikaturou SDEU. Je proto třeba zanalyzovat hlavní vodítka daná k data retention SDEU a tyto konfrontovat s českou právní úpravou.

Přístup Soudního dvoru Evropské unie

a) Digital Rights Ireland

Je pravdou, že v případě rozhodnutí ve věci Digital Rights Ireland se SDEU nezabýval otázkou souladu vnitrostátní úpravy s unijním *acquis*, přesto tento rozsudek o neplatnosti směrnice o data retention uvádí nosná východiska, na něž je navazováno v dalších rozsudcích.

Předně SDEU stavuje najisto, že z provozních a lokalizačních údajů lze sestavit velmi podrobný profil o subjektu údajů[59] a data retention a zpřístupnění údajů státním orgánům je tak zvlášť závažným zásahem do práv zaručených čl. 7 (právo na soukromí) a čl. 8 (právo na ochranu osobních údajů) Listiny základních práv EU (dále jen „**Listina**"). Je tedy nutné, aby úprava data retention splňovala veškeré záruky plynoucí z těchto článků.[60]

SDEU nadto považuje za přitěžující okolnost, když nejsou uživatelé informováni o uchovávání a předávání provozních a lokalizačních údajů.[61]

Zásah do základních práv zakotvených v Listině musí být ve smyslu čl. 52 odst. 2 Listiny I) stanoven zákonem; II) respektovat podstatu základních práv, do nichž je zasahováno; III) dodržet zásadu proporcionality v tom smyslu, zda jsou omezení základních práv nezbytná a odpovídají skutečně cílům obecného zájmu uznávaným Evropskou unií při potřebě ochrany práv a svobod druhého.[62]

SDEU stanovuje, že do podstaty základních práv není zasaženo, pokud v případě čl. 7 není umožněno seznámit se s obsahem elektronických sdělení, a v případě čl. 8 jsou stanoveny dostatečné záruky poskytovatelů služeb elektronických komunikací určené k zabezpečení uchovávaných údajů (technická a organizační opatření).[63]

Právní úprava data retention splňuje cíl obecného zájmu v případě, kdy jsou údaje uchovávány a předávány pro účely boje proti závažné trestné činnosti, která není dále specifikována. SDEU nicméně odkazuje na boj proti mezinárodnímu terorismu za účelem zachování mezinárodního míru a bezpečnosti a dále na boj proti organizované trestné činnosti.[64]

První krok testu proporcionality je dle SDEU taktéž splněn, kdy institut data retention je způsobilý dostát výše uvedenému cíli.[65] Aby právní úprava obstála i v dalším kroku, vyžaduje SDEU, aby tato úprava byla jasná a přesná s ohledem na rozsah a použití institutu vyžádání si uchovávaných údajů a stanovovala alespoň takové požadavky, aby uživatelé měli „dostatečné záruky umožňující účinně chránit jejich osobní údaje proti riziku zneužití a proti veškerému neoprávněnému přistupování k údajům a jejich protiprávnímu využívání."[66] Tyto záruky musí být o to přísnější v případě automatizovaného zpracování údajů, jak k němu dochází při data retention.[67]

Požadavek minimalizace zásahu nemůže být dle SDEU naplněn v případě, kdy dochází k plošnému, nerozlišujícímu uchovávání údajů, tj. všech osob bez „rozlišení, omezení či výjimky v závislosti na cíli boje proti závažné trestné činnosti",[68] a kdy není vyžadována „žádná souvislost mezi údaji, jejichž uchovávání je stanoveno, a ohrožením veřejné bezpečnosti a zejména se neomezuje na uchovávání údajů vztahujících se buď k určitému časovému období či určité zeměpisné oblasti či okruhu určitých osob, které mohou být jakýmkoli způsobem zapojeny do závažné trestné činnosti, anebo k osobám, které by prostřednictvím uchovávání jejich údajů mohly z jiných důvodů přispívat k předcházení, odhalování nebo stíhání závažných trestných činů".[69]

59 Digital Rights Ireland, bod 27.
60 Ibidem, body 29–37.
61 Ibidem, bod 37.
62 Čl. 52 odst. 1 Listiny a jeho interpretace v bodu 38 rozsudku ve věci Digital Rights Ireland.
63 Digital Rights Ireland, body 39–40.
64 Ibidem body 41–44.
65 Ibidem, bod 49.
66 Ibidem, bod 54.
67 Ibidem, bod 55.
68 Ibidem bod 57.
69 Ibidem, bod 59.

Jako zásadní považuje SDEU stanovení jasných a dostatečných procesněprávních a hmotněprávních pravidel pro určení, které konkrétní orgány si mohou vyžádat údaje, stanovit nezbytné minimum osob, které mají oprávněný přístup k údajům, trestné činy, pro které mohou být údaje využity a musí být stanoveny přesně.[70]

Byť směrnice o data retention stanovovala rozpětí povinnosti uchovávání údajů 6–24 měsíců a český zákonodárce se rozhodl pro nejnižší možnou dobu uchování, SDEU kritizuje i tuto nejkratší možnou dobu uchovávání bez dalších rozlišujících znaků (na rozdíl od ÚS). Dle SDEU je třeba stanovit rozdílnou dobu uchování pro jednotlivé kategorie údajů podle jejich případné užitečnosti pro účely sledovaného cíle nebo podle dotčených osob.[71] Takovou podmínku mohl český zákonodárce již zohlednit a českou úpravu data retention řádně novelizovat. ÚS v nálezu Pl. ÚS 45/17 tuto podmínku unijního práva plně opomíjí, ba naopak kvituje zvolenou dobu uložení metadat s odvoláním na v tu dobu již neplatné znění směrnice o data retention.

Z výše uvedeného je již částečně zřetelné, že česká právní úprava data retention nemůže dostát podmínkám stanoveným v rozsudku Digital Rights Ireland především s ohledem na plošné a nerozlišující uchovávání provozních a lokalizačních údajů bez stanovení výjimek. SDEU nicméně dále ve své judikaturní činnosti některé podmínky upřesňuje a jiné rozmělňuje. Je tak možné, že ve světle novějších rozsudků bude česká právní úprava souladná s požadavky SDEU.

b) Tele2Sverige

V rámci případu Tele2Sverige již SDEU přistoupil k posouzení, zda národní právní úprava data retention odpovídá nejen čl. 7, 8 a 52 odst. 1 Listiny, ale též čl. 15 odst. 1 ePrivacy směrnice. Posuzována je úprava data retention, která „za účelem boje proti trestné činnosti stanoví plošné a nerozlišující uchovávání veškerých provozních a lokalizačních údajů všech účastníků a registrovaných uživatelů, které se vztahuje na veškeré prostředky elektronické komunikace."[72] Principiálně se tedy jedná o shodnou úpravu, která je dnes platná na území České republiky.

Hlavním problémem zdůrazněným SDEU je skutečnost, že ePrivacy směrnice má za cíl „zajistit důvěrný charakter sdělení přenášených pomocí veřejné komunikační sítě a veřejně dostupných služeb elektronických komunikací a s nimi souvisejících provozních údajů."[73] Tato „zásada důvěrnosti" prostupuje celou ePrivacy směrnicí a je určujícím pravidlem pro vnitrostátní právní řády implementující tuto směrnici. ePrivacy směrnicí je v zásadě stanoven zákaz uchovávat provozní a lokalizační údaje bez souhlasu účastníků, krom výjimek uvedených v čl. 15 odst. 1 směrnice a za účelem technického uchování nezbytného pro přenos sdělení.[74] Dle čl. 6 ePrivacy směrnice lze provozní a lokalizační údaje ukládat pro dobu nezbytnou z důvodu účtování, marketingu a poskytování služeb s přidanou hodnotou.

Výjimka daná čl. 15 odst. 1 ePrivacy směrnice se nesmí dle SDEU stát pravidlem, protože by pak došlo k vyprázdnění předešlých ustanovení směrnice a byl by vůbec opuštěn základní smysl této směrnice.[75, 76]

SDEU se v rozsudku Tele2Sverige plně hlásí k závěrům vysloveným v rozsudku Digital Rights Ireland a nemůže proto jinak než vyslovit, že dotčená právní úprava „překračuje meze toho, co je naprosto nezbytné, a nelze ji v demokratické společnosti považovat za odůvodněnou, jak vyžaduje čl. 15 odst. 1 směrnice 2002/58 ve spojení s články 7, 8, 11 a čl. 52 odst. 1 Listiny."[77] Dotčená národní právní úprava totiž nerozlišuje mezi kategoriemi údajů a nepřisuzuje jim rozdílnou dobu uchování, nerozlišuje mezi dotčenými subjekty, nesoustředí se nikterak na určité časové období, zeměpisnou oblast či okruh určitých osob, nestanovuje žádnou výjimku pro osoby, jež jsou předmětem profesního tajemství. Je patrné, že to stejné platí i pro českou právní úpravu, která nezohledňuje žádnou ze záruk SDEU zmíněných jak v Digital Rights Ireland, tak v Tele2Sverige.

Tele2Sverige rozvíjí podmínky stanovené v Digital Rights Ireland v tom smyslu, že vnitrostátní právní úprava musí obsahovat objektivní kritéria pro stanovení okruhu osob, jejichž údaje mohou vykazovat alespoň nepřímou souvislost se „závažnou trestnou činností nebo určitým způsobem přispívat k boji proti závažné trestné činnosti či k předcházení

70 Ibidem, body 60–61.
71 Ibidem, bod 63.
72 Tele2Sverige, bod 62.
73 Ibidem, bod 83; SDEU cituje z bodů 6 a 7 odůvodnění ePrivacy směrnice.
74 Ibidem, bod 85.
75 Ibidem, bod 89.
76 Ibidem, bod 104.
77 Ibidem, bod 107.

závažného ohrožení veřejné bezpečnosti."[78] Takovým objektivním kritériem může být např. kritérium zeměpisné, pokud je v určité oblasti větší hrozba spáchání kupříkladu teroristického útoku.

Dále SDEU stanovuje, že provozní a lokalizační údaje mohou být uchovávány a vyžádány státními orgány pouze za účely vyjmenovanými v čl. 15 odst. 1 ePrivacy směrnice,[79] což do určité míry souvisí s otázkou, zda lze vůbec vyžádat lokalizační údaje policií pro účely pátrání po pohřešovaných a hledaných osobách. S ohledem na pohřešované osoby se domnívám, že takové údaje lze vyžádat vzhledem k přímému ohrožení života a zdraví, byť nejsou naplněny hmotněprávní a procesněprávní požadavky ochrany před zneužitím přístupu k těmto údajům vyslovené v bodu 120 odůvodnění Tele2Sverige, kdy jsou tyto požadavky relativizovány v případě „naléhavých případů".[80] S ohledem na to, že již v tomto případě je institut data retention a vyžádání lokalizačních údajů na hraně, nelze si představit, že by jakkoli mohl obstát institut vyžádání si lokalizačních údajů při pátrání po hledaných osobách ve smyslu § 68 odst. 2 ZPol.[81]

Úprava data retention musí vyžadovat k předchozímu vydání provozních a lokalizačních údajů státním orgánům odůvodněné rozhodnutí nezávislého soudu nebo nezávislého správního orgánu[82] a dotčené osoby musí být vyrozuměny o předání jejich údajů státním orgánům, pokud by taková informace nezpůsobila ohrožení probíhajícího vyšetřování.[83] Tato podmínka je v ZEK ve spojení s trestním řádem splněna stejně tak jako další podmínka stanovení dohledu na provozovateli elektronických komunikací (u nás dokonce částečně dvojkolejní, když dohled zčásti vykonává ČTÚ a zčásti UOOU). Přesto ani s ohledem na rozsudek Tele2Sverige nelze konstatovat, že by česká právní úprava byla souladná s unijním právem. Je až tristní, jak ÚS v nálezu Pl. ÚS 45/17 opomenul veškeré nosné závěry SDEU a nebyl s to se s nimi argumentačně vypořádat.

c) Ministerio Fiscal

Rozhodnutí v této věci zásadně doplňuje požadavek vyjádřený v rozsudcích Digital Rights Ireland a Tele2Sverige s ohledem na omezení užití data retention pouze pro potřebuju boje se „závažnými trestnými činy". SDEU rozvádí, že v případě, kdy data retention zasahuje do základních práv závažným způsobem, musí být účelem tohoto zásahu pouze „prevence, vyšetřování, odhalování a stíhání trestných činů", které jsou taktéž kvalifikovány jako „závažné".[84]

Pokud ale zásah do základních lidských práv není „závažný", lze jej odůvodnit i prevencí, vyšetřováním, odhalováním a stíháním trestných činů obecně (nikoliv tedy pouze závažných).[85]

Ve světle projednávaného případu je pak stanoveno, že závažným zásahem do soukromí osob není, pokud státní orgán vyžádá po poskytovateli služeb elektronických komunikací jméno, příjmení a adresu držitele SIM karty aktivované v odcizeném mobilním zařízení.[86] Určujícím hlediskem zde přitom je, zda lze na základě vyžádaných údajů osobu lokalizovat, přičemž lokalizační údaje vyžádány nebyly, a sestavit její podrobný profil, což v daném případě též nepřipadá v úvahu, protože nebyly vyžádány informace týkající se uskutečněných a přijatých hovorů, včetně telefonních čísel, doby trvání hovorů, lokace, odkud byl hovor uskutečněn, apod.[87]

Závěry tohoto rozsudku nejsou pro posouzení české právní úpravy data retention příliš zásadní, spíše mohou sloužit jako vodítko pro zákonodárce pro možnou novelizaci.

d) Privacy International

Tento rozsudek se týká především možnosti plošného předávání provozních a lokalizačních údajů bezpečnostním a zpravodajským službám za účelem národní bezpečnosti. V tomto smyslu je možné dovodit nesoulad úpravy předávání provozních a lokalizačních údajů Bezpečnostní informační službě (dále

78 Ibidem, bod 111.
79 „… omezení představuje v demokratické společnosti nezbytné, přiměřené a úměrné opatření pro zajištění národní bezpečnosti (tj. bezpečnosti státu), obrany, veřejné bezpečnosti a pro prevenci, vyšetřování, odhalování a stíhání trestných činů nebo neoprávněného použití elektronického komunikačního systému, jak je uvedeno v čl. 13 odst. 1 směrnice 95/64/ES."
80 „K tomu, aby byly v praxi tyto podmínky plně dodržovány, je zásadní, aby byl přístup příslušných vnitrostátních orgánů k uchovávaným údajům, s výjimkou naléhavých případů, řádně odůvodněn, podléhal předchozímu přezkumu ze strany soudu nebo nezávislého správního orgánu a aby tento soud nebo orgán rozhodoval na základě odůvodněné žádosti těchto příslušných orgánů, zejména v rámci postupů pro předcházení, odhalování nebo stíhání trestných činů".
81 Byť např. pro účely pátrání po osobách, jež spáchaly teroristický trestný čin, si lze představit možnost využití tohoto institutu i ve světle Tele2Sverige. Nicméně by tato možnost musela být v ZPol specifikována, což v nynějším znění zákona není.
82 Tele2Sverige, bod 120.
83 Ibidem, bod 121.
84 Ministerio Fiscal, bod 56.
85 Ibidem, bod 57.
86 Ibidem, bod 59.
87 Ibidem, bod 60.

jen „**BIS**“) dle § 8a písm. b) zák. č. 154/1994 Sb., o bezpečnostní informační službě. Ve smyslu uvedeného ustanovení může BIS vyžádat provozní a lokalizační údaje po poskytovatelích služeb elektronických komunikací v rozsahu potřebném pro plnění konkrétního úkolu, přičemž dále je odkázáno na § 97 ZEK bez dalších podrobností. Takovému vyžádání nepředchází povolení soudu nebo jiného nezávislého správního orgánu a subjekty údajů o něm nejsou informovány.

SDEU připomíná, že podmínky stanovené v ePrivacy směrnici, včetně podmínky prejudikatury SDEU, se vztahují na všechny orgány veřejné moci, včetně bezpečnostních a zpravodajských služeb.[88]

SDEU rekapituluje, že pokud jsou údaje bezpečnostním a zpravodajským službám předávány plošně a nerozlišujícím způsobem, tj. bez větší specifikace možného předávání za konkrétními účely,[89] stává se z výjimky zakotvené v čl. 15 odst. 1 ePrivacy směrnice pravidlo.[90]

SDEU zdůrazňuje, že zkoumaný zásah je zvláště závažný, a navíc způsobilý odradit uživatele komunikačních prostředků od „výkonu svobody projevu zaručené v článku 11 Listiny“,[91] přičemž omezení svobody projevu je o to zřetelnější pro osoby podléhající předpisům o profesním tajemství.[92] ÚS v nálezu Pl. ÚS 45/17 nevěnoval námitce navrhovatelky ohledně profesní mlčenlivosti některých dotčených subjektů přílišnou pozornost a pouze konstatoval, že je na soudu, aby *ad hoc* posoudil, zda má převládnout žádost o přístup k údajům s ohledem na sledovaný cíl nebo profesní tajemství.[93]

SDEU v rozsudku vznáší zásadní obavu v tom smyslu, že při samotném plošném a nerozlišujícím ukládání provozních a lokalizačních údajů „vzniká riziko zneužití a neoprávněného přístupu již samotným uložením těchto údajů poskytovateli služeb elektronických komunikacích.“[94] Čímž opět potvrdil, že data retention takového rozsahu nelze v zásadě odůvodnit.

Na druhou stranu SDEU přiznává, že s ohledem na cíl národní bezpečnosti, který stojí nad všemi ostatními cíli vyjádřenými v čl. 15 odst. 1 ePrivacy směrnice, lze do základních práv zasáhnout ještě extenzivněji než u těchto jiných cílů.[95]

I přesto, zdůrazňuje SDEU, je třeba dbát testu proporcionality a stanovit dostatečné procesní a hmotněprávní podmínky přístupu. Obecný přístup k provozním a lokalizačním údajům „bez jakékoli, byť i nepřímé souvislosti se sledovaným cílem nelze považovat za omezený na to, co je nezbytně nutné.“[96] Dotčené plošné a nerozlišující předávání komunikačních metadat lze považovat za obecné, když nejsou stanovena žádná objektivní kritéria k předání takových údajů, přičemž takovou právní úpravu nelze v demokratické společnosti považovat za odůvodněnou.[97]

Byť se tento rozsudek netýkal přímo plošného a nerozlišujícího uchovávání, ale předávání údajů, lze na jeho základě konstatovat, že úprava obsažená v zákoně o BIS není slučitelná s unijní judikaturou.

e) La Quadrature du Net

V tomto rozhodnutí SDEU ve věci data retention dochází k rozsáhlé rekapitulaci východisek předchozí judikatury SDEU. Opět je zmíněna neopomenutelná role zásady důvěrnosti, jež je hlavní zásadou ePrivacy směrnice, stejně jako podmínky pro uplatnění výjimek z této zásady zakotvených v čl. 15 odst. 1 předmětné směrnice.

SDEU zmiňuje jednu velmi důležitou věc, ne tolik zdůrazňovanou v předchozích rozhodnutích. Už samotné uchovávání údajů je dostatečně způsobilé k onomu často zmiňovanému „závažnému zásahu do základních práv“. Jinými slovy pro posouzení data retention vůbec není rozhodné, zda jsou údaje předávány, protože předání údajů je odlišnou kategorií zásahu do základních práv (ostatně vyžádání si/předání údajů se věnuje rozsudek ve věci Privacy International).[98]

SDEU se v tomto rozsudku zabývá, tak jako v Privacy International, národní bezpečností, ale s tím rozdílem, zda je za účelem obrany národní bezpečnosti možné uložit poskytovatelům služeb elektronických povinnost plošného a nerozlišujícího uchovávání provozních a lokalizačních údajů. SDEU i zde uvádí, že národní bezpečnost je v rámci čl. 15

88 Privacy International, bod 56.
89 Přičemž dle české právní úpravy je možné, aby si BIS vyžádala jakékoli údaje bez jakéhokoli dalšího odůvodnění neomezeného počtu osob bez předchozího souhlasu soudu nebo jiného nezávislého správního orgánu.
90 Ibidem, bod 69.
91 Ibidem, bod 72.
92 Ibidem.
93 Pl.ÚS 45/17, bod 81.
94 Privacy International, bod 73.
95 Ibidem, bod 75.
96 Ibidem, bod 78.
97 Ibidem, bod 80.
98 La Quadrature du Net, bod 116.

odst. 1 ePrivacy směrnice nad ostatními důvody pro zavedení výjimky ze zásady důvěrnosti. SDEU v tomto smyslu shledává plošné a nerozlišující data retention za souladné s evropským právem, ale pouze v případě vysoce přísných záruk. Předně musí být ohrožení národní bezpečnosti závažné, skutečné a aktuální či předvídatelné.[99] Příkaz preventivně uchovávat komunikační metadata musí být časově omezen na nezbytně nutnou dobu a musí být stanoveny přísné mechanismy pro ochranu osobních údajů před zneužitím.[100] Takové rozhodnutí musí být navíc přezkoumatelné soudem nebo nezávislým správním orgánem.[101] V této chvíli je dobré si uvědomit, za jakých podmínek SDEU připustil plošné a nerozlišující preventivní uchovávání provozních a lokalizačních údajů, čímž lze jednoduše dojít k závěru, že česká právní úprava tyto podmínky nesplňuje, kdy příkaz k preventivnímu uchovávání komunikačních metadat je stanoven přímo zákonem a není nijak časově omezen na dobu nezbytně nutnou a navíc není odůvodněn národní bezpečností.

Dále SDEU po vzoru Tele2Sverige staví najisto, že: „Vnitrostátní právní úprava, která stanoví plošné a nerozlišující uchovávání provozních a lokalizačních údajů za účelem boje proti závažné trestné činnosti, překračuje meze toho, co je naprosto nezbytné, a nelze ji v demokratické společnosti považovat za odůvodněnou, jak vyžaduje čl. 15 odst. 1 směrnice 2002/58 ve spojení s články 7, 8 a 11 a čl. 52 odst. 1 Listiny.“[102] Dle SDEU provozní a lokalizační údaje nesmí být uchovávány „systematicky a průběžně“ tak, aby takové uchovávání nebylo pravidlem vytvořeným z výjimky.[103] Česká právní úprava zavádí přesně takové pravidlo, které SDEU nepovažuje za souladné, kdy ukládání údajů je systematické a průběžné.

SDEU si v režimu čl. 15 odst. 1 za účelem boje proti závažné trestné činnosti a předcházení závažnému narušení veřejné bezpečnosti, jakož i za účelem národní bezpečnosti dokáže jako souladné představit cílené uchovávání provozních a lokalizačních údajů. To však za podmínky, že je naplněna podmínka omezení uchovávání na to, co je nezbytně nutné (včetně doby uchovávání, kategorie údajů, komunikačních prostředků a dotčené osoby).[104]

Dále je rozsudkem stanoveno v návaznosti na rozsudek ve věci Ministerio Fiscal, že může být nařízeno uchovávání údajů týkajících se totožnosti uživatelů prostředků elektronické komunikace za účelem prevence, vyšetřování, odhalování stihání trestných činů obecně (nikoliv jen závažných).[105] Je též stanoveno, že za účelem boje proti závažné trestné činnosti je možné nařídit plošné a nerozlišující uchovávání IP adres fyzických osob, které jsou vlastníky koncových zařízení, protože se jedná o jediný možný prostředek nápomocný pro vyšetřování kybernetických trestných činů. Samozřejmě však za splnění výše již několikrát zmíněných podmínek.[106]

V bodech 160–168 rozsudku SDEU výslovně povoluje úpravu data freeze a stanovuje dodatečné podmínky pro to, aby tato úprava byla souladná s čl. 15 odst. 1 ePrivacy směrnice. Nutno podotknout, že je SDEU k této úpravě značně přívětivější než k úpravě data retention.

Další předběžné otázky nejsou pro posouzení souladu nynější české úpravy data retention relevantní, mohou být ale zásadním vodítkem při tvorbě nové právní úpravy v případě, že bude vůle ze strany zákonodárce uvést úpravu data retention do souladu s evropským právem.

Opětovné potvrzení předchozích závěrů

Po provedení výše uvedené hlavní analýzy se před SDEU dostaly další případy, jež svým způsobem potvrdily již v jiných případech vyslovené závěry. Jedná se o dva rozsudky SDEU[107] a jedno stanovisko generálního advokáta Szpunara.[108]

1) SpaceNet

Němečtí poskytovatelé veřejně dostupných služeb internetového připojení a telefonních

99 Ibidem, bod 137.
100 Ibidem, bod 138.
101 Ibidem, bod 139.
102 Ibidem, bod 141.
103 Ibidem, bod 142.
104 Ibidem, bod 147.
105 Ibidem, bod 158. Pro bližší argumentaci odkazuji na rozsudek ve věci Ministerio Fiscal.
106 Ibidem, body 153–155.
107 Rozsudek SDEU ve spojených věcech C-793/19 a C-794/19, Bundesrepublik Deutschland proti SpaceNet AG, Telekom Deutschland GmbH, ECLI:EU:C:2022:702 (dále jen „**SpaceNet**“); rozsudek SDEU ve spojených věcech C-339/20 a C 397/20, VD, SR, ECLI:EU:C:2022:703 (dále jen „**VD, SR**).
108 Stanovisko generálního advokáta Macieje Szpunara ve věci C-470/21, La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net, French Data Network proti Premier ministre, Ministére de la Culture, ECLI:EU:C:2022:838 (dále jen „**French Data Network**“).

služeb se v daném případě bránili povinnosti stanovené německým právem uchovávat plošným a nerozlišujícím způsobem provozní údaje po dobu 10 týdnů a lokalizační údaje po dobu 4 týdnů za účelem boje proti závažné trestné činnosti a ochrany veřejné bezpečnosti (s důrazem na slovo *veřejné*).[109]

SDEU v daném případě, plně se hlásící k závěrům předchozí judikatury, opětovně potvrdil, že plošné a nerozlišující preventivní uchovávání provozních a lokalizačních údajů, a to i v případě 4 či 10 týdnů, není zásadně obhajitelné, tj. je nepřípustné.[110] Tento závěr dle SDEU platí i v německém případě, kdy docházelo k ukládání nikoliv všech provozních a lokalizačních údajů, nýbrž *většiny*, a nadto po v zásadě velmi omezenou dobu (4, resp. 10 týdnů). SDEU totiž připomíná, že jakékoli uchovávání metadat má závažnou povahu, a to bez ohledu na délku období uchovávání, a dokonce na množství či povahu metadat, „pokud lze z uvedeného souboru údajů vyvodit přesné závěry o soukromém životě subjektu údajů".[111]

SDEU navíc zdůrazňuje, že jsou-li metadata uchovávána plošně a nerozlišujícím způsobem za účelem ochrany národní bezpečnosti, tj. za velmi přísných hmotněprávních a procesněprávních podmínek a pouze na základě soudem přezkoumatelného *ad hoc* rozhodnutí, nelze tato metadata vyžádat za účelem boje proti závažné trestné činnosti.[112]

Na druhou stranu zde SDEU potvrzuje závěry z rozsudku La Quadrature du Net, že je možné na základě velmi přísných podmínek a pouze na omezenou dobu *ad hoc* za účelem ochrany národní bezpečnosti (s důrazem na slovo *národní*) stanovit plošné a nerozlišující uchovávání osobních údajů.[113]

Stejně tak jsou potvrzeny závěry s ohledem na cílené uchovávání[114], uchovávání IP adres[115] a urychlené uchovávání (tzv. data freezing).[116]

2) VD, SR

V daném případě se SDEU vyslovuje, zda je možné stanovit plošné a nerozlišující uchovávání metadat za účelem ochrany kapitálového trhu tak, jak to v České republice stanovuje § 8 odst. 1 písm. d) zák. č. 15/1998 Sb., o dohledu v oblasti kapitálového trhu a o změně doplnění dalších zákonů (dále jen „**ZoDNKT**"). Ostatně česká vláda ve vyjádření zaslaném ÚS v rámci řízení Pl. ÚS 45/17 uvádí, že česká právní úprava data retention a možnost vyžádání si těchto údajů Českou národní bankou je v souladu s evropským právem, protože z evropského práva vychází.[117]

SDEU dokonce stanovuje, že unijní právo, konkrétně nařízení o zneužívání trhu (ani předchozí směrnice o zneužívání trhu),[118] nemůžou v žádném případě odůvodnit takovou národní právní úpravu, která stanovuje plošné a nerozlišující preventivní uchovávání provozních a lokalizačních údajů.[119]

Nadto SDEU stanovil, že (čl. 15 odst. 1) ePrivacy směrnice představuje referenční akt pro všechny druhy možného uchovávání provozních a lokalizačních údajů a je třeba všechny předpisy vykládat v souladu s výkladem SDEU v této věci.[120]

V této souvislosti lze tedy konstatovat, že ani úprava v ZoDNKT nemůže ve světle judikatury SDEU obstát.

3) French Data Network

Generální advokát se ve svém stanovisku hlásí k závěrům SDEU v rozsudcích La Quadrature du net a SpaceNet v tom smyslu, že pro šetření kriminality páchané výhradně na internetu je možné plošné a nerozlišující uchovávání IP adres tak, aby byla možná identifikace uživatelů těchto IP adres.[121]

Svými závěry nicméně navrhuje modifikovat judikaturu SDEU v tom smyslu, že výše uvedené uchovávání je možné v takovém případě, kdy IP adresy tvoří jediný prostředek vyšetřování takových trestných činů, čímž by byl naplněn požadavek uchovávání v takovém rozsahu, který je nezbytně nutný.[122]

---

109 SpaceNet, body 22–24.
110 Ibidem, bod 312.
111 Ibidem, bod 88.
112 Ibidem, bod 130.
113 Ibidem, bod 93.
114 Ibidem, body 105–109.
115 Ibidem, body 101–102.
116 Ibidem, body 114–118.
117 Pl. ÚS 45/17, bod 27.
118 Nařízení Evropského parlamentu a Rady (EU) č. 596/2014 ze dne 16. dubna 2014 o zneužívání trhu (nařízení o zneužívání trhu) a o zrušení směrnice Evropského parlamentu a Rady 2003/6/ES a směrnic Komise 2003/124/ES, 2003/125/ES a 2004/72/ES Text s významem pro EHP.
119 VD, SR, bod 78.
120 Ibidem, bod 79.
121 French Data Network, bod 111.
122 Ibidem, bod 85.

Závěr

Je sice pravdou, že SDEU do určité míry až příliš zohledňuje hypotetická rizika spojená ať už s ukládáním nebo předáváním provozních a lokalizačních údajů,[123] to ale nemění nic na skutečnosti, že je třeba závěry vyslovené SDEU v české právní úpravě zohlednit.

Z výše provedené analýzy je zřejmé, že SDEU institut preventivního plošného a nerozlišujícího ukládání provozních a lokalizačních údajů povolil pouze v případě závažného ohrožení národní bezpečnosti, které je bezprostřední, aktuální a reálné, a to odůvodněným příkazem přezkoumatelným soudem nebo nezávislým správním orgánem na dobu nezbytně nutnou při zachování zásady minimalizace zásahu na to, co je absolutně nezbytné. Ve všech dalších případech SDEU ve své judikatuře konstantně potvrzuje, že preventivní plošné a nerozlišující uchovávání komunikačních metadat není souladné s čl. 7, čl. 8 a čl. 11 Listiny a nenaplňuje ani podmínky výjimky stanovené v čl. 15 odst. 1 ePrivacy směrnice. Takovou úpravu nelze proto třeba vnímat jako v demokratické společnosti odůvodněnou.

Česká právní úprava do určité míry může stanovovat institut tzv. omezeného data retention,[124] kdy sice dochází k preventivnímu plošnému a nerozlišujícímu uchovávání komunikačních metadat, hmotněprávní a procesněprávní podmínky by dle mého názoru musely být nicméně více zpřísněny (jak ostatně uvedeno výše v části příspěvku věnující se nálezu ÚS Pl. 45/17).

Dodávám, že otázka, kterou se SDEU zabýval snad ve všech rozsudcích o data retention, zda vůbec národní úpravy spadají pod čl. 15 odst. 1 ePrivacy směrnice, je bezpředmětná.[125] Je třeba se soustředit pouze na uvedení souladu české právní úpravy s unijním právem. Zřetelné podmínky byly stanoveny již v rozsudcích Digital Rights Ireland a Tele2Sverige, které měl k dispozici při svém přezkumu i ÚS, který ale na nosné argumenty buď reagoval velmi obecně, případně vůbec, nebo si vybíral určité velmi specifické instituty české právní úpravy a nekoncepčně je validoval z kontextu vytrženými dílčími závěry SDEU. Takový přístup není a nemůže být souladný s povinností eurokonformního výkladu.

Dle mého závěru situaci nemůže zlepšit ani připravované ePrivacy nařízení,[126] které ve svém čl. 11 v zásadě kopíruje obsah a význam nyní platného čl. 15 odst. 1 ePrivacy směrnice a budou na něj moci být aplikovány závěry SDEU dané doposud v režimu směrnice. Ze strany českého zákonodárce by tak mělo dojít k urychlenému uvedení národní úpravy do souladu s unijním výkladem čl. 15 odst. 1 ePrivacy směrnice.

Je tak nepochybné, že česká právní úprava data retention ve všech obsažených předpisech přímo odporuje unijnímu právu.

123 SERDULA, O. Plošné uchovávání komunikačních metadat v EU ve světle rozsudku La Quadrature du Net. *Jurisprudence*, ročník 2021, č. 3, str. 46.
124 Ibidem.
125 GUMZEJ, N., *Applicability of ePrivacy Directive to National Data Retention Measures following Invalidation of the Data Retention Directive*, Juridical Tribune 11, roč. 2021, č. 3, str. 446.
126 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).