Česká republika
NÁLEZ
Ústavního soudu

Jménem republiky

Ústavní soud rozhodl v plénu složeném z předsedy Pavla Rychetského a soudců Ludvíka Davida, Jaroslava Fenyka, Josefa Fialy, Jana Filipa, Jaromíra Jirsy (soudce zpravodaj), Tomáše Lichovníka, Vladimíra Sládečka, Radovana Suchánka, Kateřiny Šimáčkové, Vojtěcha Šimíčka, Milady Tomkové, Davida Uhlíře a Jiřího Zemánka o **návrhu skupiny poslanců**, zastoupené Mgr. et Mgr. Janem Vobořilem, advokátem se sídlem v Praze 7, U Smaltovny 1115/32, na zrušení ustanovení § 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, § 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 uchování, předávání a likvidaci provozních a lokalizačních údajů, za účasti **Parlamentu** a **Ministerstva průmyslu a obchodu** jako účastníků řízení a **vlády ČR** jako vedlejší účastnice řízení, takto:

Návrh se zamítá.

Odůvodnění

I. Vymezení věci

1. Skupina 58 poslanců (dále jen „skupina poslanců“ nebo „navrhovatelka“) se podle čl. 87 odst. 1 písm. a) a b) Ústavy České republiky (dále jen „Ústava“) návrhem ze dne 20. 12. 2017 domáhá u Ústavního soudu v řízení podle § 64 a násl. zákona č. 182/1993 Sb., o Ústavním soudu, ve znění pozdějších předpisů (dále jen „zákon o Ústavním soudu“), zrušení v záhlaví uvedených ustanovení.

2. Návrh napadá některá ustanovení právní úpravy preventivního uchovávání provozních a lokalizačních údajů o elektronické komunikaci u poskytovatelů telekomunikačních služeb (dále též „*data retention*“) a možnosti jejich následného poskytnutí: a) orgánům činným v trestním řízení, b) Policii České Republiky (dále jen „policie“) pro účely zahájeného pátrání po konkrétní hledané nebo pohřešované osobě, zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly, či předcházení nebo odhalování konkrétních hrozeb v oblasti terorismu, c) Bezpečnostní informační službě, d) Vojenskému zpravodajství, e) České národní bance (dále též „ČNB“) pro účely dohledu nad kapitálovým trhem.

3. Napadená právní úprava sleduje, jak vyplývá i z příslušných důvodových zpráv, různé cíle, které jsou odvoditelné také z výčtu orgánů oprávněných s uchovanými údaji nakládat. Jde o bezpečnost a obranu státu, ochranu osob i majetku před trestnou činností, pátrání po osobách hledaných, pohřešovaných či ztracených a o dohled

nad kapitálovým trhem. Původní právní úprava zakládající povinnost uchovávat provozní a lokalizační údaje byla v roce 2005 přijata v reakci na zvyšující se rizika v oblasti bezpečnosti, související s narůstajícím využitím elektronických komunikačních systémů, kterým bylo nezbytné přizpůsobit pravomoci orgánů příslušných k plnění úkolů pro zajištění bezpečnosti a obrany České republiky, a představovala implementaci 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 změně směrnice 2002/58/ES (dále jen „směrnice o *data retention*“), z rozhodnutí Soudního dvora Evropské unie (dále též „SDEU“) dnes již neplatné (viz dále).

4. Pro naplnění uvedených cílů nařizuje napadená právní úprava povinným subjektům (poskytovatelé služeb elektronické komunikace, dále jen „operátoři“) uchovávat o všech klientech, uživatelích telekomunikačních služeb, „balíky dat“ po dobu šesti měsíců zpětně. Například u telefonních hovorů či SMS a MMS zpráv (včetně neúspěšných pokusů o spojení) provozovatel uchovává údaje o telefonních číslech volajícího i volaného, datu a času zahájení i ukončení komunikace, poloze i pohybu uživatele dané služby. V případě využití internetových služeb a e-mailové komunikace jsou dále operátoři povinni shromažďovat zejména uživatelské účty, identifikátor počítače i vyhledaného serveru (IP adresa, číslo portu), údaje o e-mailové adrese účastníků komunikace a protokolu elektronické pošty.

5. Zjednodušeně řečeno, na základě napadené právní úpravy operátoři uchovávají informace o každém telefonickém spojení, textové zprávě, internetovém připojení či e-mailové korespondenci, tj. podrobná data o veškeré komunikaci, lokalizaci účastníků komunikace a poskytnutých internetových službách. Některé z těchto údajů uchovávají operátoři pro vlastní potřeby (vyúčtování služeb, reklamace, marketing) i bez povinnosti stanovené napadeným zákonem.

II. Argumentace navrhovatelky

6. Skupina poslanců navrhuje napadenou právní úpravu zrušit, jelikož neústavně zasahuje do Listinou základních práv a svobod (dále jen „Listina“) zaručeného práva na soukromí podle čl. 7 odst. 1 Listiny, na ochranu před neoprávněným zasahováním do soukromého a rodinného života podle čl. 10 odst. 2 Listiny, práva na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě podle čl. 10 odst. 3 Listiny a práva na zachování tajemství zpráv podávaných telefonem nebo jiným podobným zařízením podle čl. 13 Listiny. Navrhovatelka dále namítá rozpor napadené úpravy s čl. 8 Úmluvy o ochraně lidských práv a základních svobod (dále jen „Úmluva“).

7. Navrhovatelka svou argumentaci uvozuje odkazem na prejudikaturu Ústavního soudu a Soudního dvora Evropské unie, která se již problematikou *data retention* zabývala [nález Ústavního soudu sp. zn. Pl. ÚS 24/10 ze dne 22. 3. 2011 (N 52/60 SbNU 625; 94/2011 Sb.); nález Ústavního soudu sp. zn. Pl. ÚS 24/11 ze dne 20. 12. 2011 (N 217/63 SbNU 483; 43/2012 Sb.); rozsudky Soudního dvora Evropské unie ze dne 8. 4. 2014 ve spojených věcech C-293/12 a C-594/12 (*Digital Rights Ireland Ltd*) a ze dne 21. 12. 2016 ve spojených věcech C-203/15 a C-698/15 (*Tele2 Sverige AB*)].

8. V návrhu je předně namítáno, že napadená právní úprava je neproporcionální ve vztahu k ústavně zaručenému právu na ochranu soukromí, neboť nešetří jeho podstatu a smysl podle čl. 4 odst. 4 Listiny. Podle přesvědčení navrhovatelky je protiústavní již samotné sledování, shromažďování a uchovávání provozních a lokalizačních údajů, jelikož je plošné a nevýběrové. Navrhovatelka uvádí, že opatření vytváří oprávněný pocit, že jsou všichni pod konstantním dohledem, a neumožňuje žádné rozlišení. V dnešní době vzniká podstatně více údajů, než tomu bylo v roce 2011, kdy naposledy o věci Ústavní soud rozhodoval, neboť se rozšířilo užívání datových služeb v mobilních („chytrých“) telefonech, což umožňuje získat detailní přehled nejen o sociálních vazbách a návycích jednotlivce, ale také o jeho pohybu. Za nadále neúnosnou považuje navrhovatelka skutečnost, že uchovávání provozních a lokalizačních údajů se vztahuje rovněž na osoby s povinností mlčenlivosti – profesního tajemství (advokáti, lékaři, poradci). Plošné uchovávání citlivých údajů s sebou nese riziko jejich zneužití – v zahraničí byly zneužity údaje o žurnalistech (Polsko) nebo podle nich byli určeni účastníci protivládní demonstrace (Bělorusko).

9. Dále ve vztahu k jednotlivým napadeným ustanovením navrhovatelka namítá, že vymezení účelů, pro které je možné provozní a lokalizační údaje podle vnitrostátního práva uchovávat, je neúměrně široké a ve svém důsledku porušující čl. 15 odst. 1 Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. 7. 2002, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích), v účinném znění (dále jen „e-privacy směrnice“), neboť omezit soukromí jednotlivce lze v tomto ohledu pouze za účelem zajištění veřejné bezpečnosti, obrany státu a pro prevenci, vyšetřování, odhalování a stíhání trestných činů. Možnost použití provozních a lokalizačních údajů policií při pátrání po pohřešované či hledané osobě už ze své podstaty nemůže odůvodnit výjimky z ochrany soukromí, stejně jako dohled České národní banky nad kapitálovým trhem. Navrhovatelka je přesvědčena, že oprávnění podle ustanovení § 97 odst. 3 písm. b) a písm. e) zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), v účinném znění (dále jen „ZEK“), ve spojení s § 68 odst. 2 a § 71 písm. a) zákona č. 273/2008 Sb., o Policii České republiky, v účinném znění (dále jen „zákon o policii“ nebo „ZPol“), nejsou v souladu s legitimními cíli, které taxativně vymezuje citovaná směrnice.

10. V užším smyslu, co do možnosti poskytovat provozní a lokalizační údaje orgánům činným v trestním řízení podle § 97 odst. 3 písm. a) ZEK ve spojení s § 88a zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), v účinném znění (dále jen „trestní řád“), není podle navrhovatelky opatření způsobilé naplnit legitimní cíl – snížení trestné činnosti a zvýšení její objasněnosti. Z dostupných statistik kriminality policie za období 2011 – 2013 podle navrhovatelky vyplývá, že možnost použití provozních a lokalizačních údajů nemá vliv ani na četnost trestné činnosti, ani na její objasněnost – u závažné kriminality jsou statistické závěry totožné, což mají dokládat i zahraniční studie; orgány činné v trestním řízení jsou schopné zajistit potřebné důkazy i jinak. Dále navrhovatelka poukazuje na skutečnost, že sledování provozních a lokalizačních údajů je možné jednoduše obejít pomocí různých nástrojů, např. použitím anonymní předplacené telefonní SIM karty, čehož si jsou dobře vědomi především právě pachatelé závažné trestné činnosti. Výsledkem je pak sledování komunikace celé společnosti, která se trestné činnosti nedopouští, na ochranu před pachateli, kteří dobře vědí, jak se sledování technicky vyhnout – opatření je tak

v rámci testu proporcionality nevhodné k naplnění legitimního cíle. Navíc je zřejmé, že předmětná data jsou nadužívána, protože nejsou vyžadována jen k objasnění zvlášť závažného zločinu, ale často slouží jako důkaz v běžných trestních řízeních.

11. Ve vztahu k § 97 odst. 3 písm. b) ZEK ve spojení s § 68 odst. 2 a § 71 písm. a) ZPol nerespektuje napadená zákonná úprava podle navrhovatelky závěry kasačního nálezu sp. zn. Pl. ÚS 24/10 (zejm. bod 36), podle něhož poskytnutí provozních a lokalizačních údajů musí předcházet rozhodnutí nezávislého soudu, což nyní zákon nevyžaduje. Policie má v některých případech přístup k provozním a lokalizačním údajům, aniž by jej povolil soud a nemá povinnost o použití údajů ani následně informovat jejich subjekt (jako v případě odposlechů), takže dotčená osoba se o zásahu do svých ústavních práv ani nedozví.

III. Aktivní procesní legitimace a podmínky řízení

12. Podle § 64 odst. 1 písm. b) zákona o Ústavním soudu má právo podat návrh na zrušení zákona nebo jeho jednotlivých ustanovení skupina nejméně 41 poslanců. Podle § 64 odst. 2 písm. b) zákona o Ústavním soudu může podat návrh na zrušení jiného právního předpisu nebo jeho jednotlivých ustanovení skupina nejméně 25 poslanců. Návrh v této věci podala skupina 58 poslanců a v souladu s § 64 odst. 5 zákona o Ústavním soudu k němu připojila i podpisovou listinu, na které každý z nich jednotlivě potvrdil, že se k návrhu připojuje. Podmínku aktivní legitimace tedy navrhovatelka splňuje.

13. Návrh obsahuje veškeré zákonem požadované náležitosti a je přípustný ve smyslu ustanovení § 66 zákona o Ústavním soudu; současně neexistuje žádný důvod pro zastavení řízení podle ustanovení § 67 téhož zákona.

IV. Průběh řízení před Ústavním soudem

14. Ústavní soud podle § 69 zákona o Ústavním soudu vyzval Poslaneckou sněmovnu i Senát Parlamentu a Ministerstvo průmyslu a obchodu (dále též „MPO“) jako účastníky řízení a vládu spolu s veřejnou ochránkyní práv jako vedlejší účastníky řízení k vyjádření. O vyjádření k návrhu požádal Ústavní soud podle § 48 odst. 2 zákona o Ústavním soudu i prezidenta republiky, Ministerstvo spravedlnosti, Nejvyšší státní zastupitelství (dále též „NSZ“) a Úřad pro ochranu osobních údajů.

15. Veřejná ochránkyně práv Ústavní soud informovala, že do řízení nevstupuje. Vyjádření prezidenta republiky neobsahuje žádné podstatné (nové) skutečnosti, proto je Ústavní soud nepovažuje za nutné blíže rekapitulovat.

a) Vyjádření komor Parlamentu

16. Poslanecká sněmovna a Senát ve svém vyjádření pouze popsaly průběh legislativního procesu přijímání napadené úpravy.

17. Vládní návrh zákona č. 273/2012 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a některé další zákony, obsahující napadená znění § 97 odst. 3 a 4 ZEK a § 88a trestního řádu, byl poslancům

rozeslán jako tisk č. 615 dne 27. 2. 2012. První čtení návrhu zákona bylo uskutečněno 14. 3. 2012 a následně výbory doporučily návrh zákona schválit. Druhým čtením prošel návrh zákona dne 14. 6. 2012. V podrobné rozpravě vystoupil s pozměňovacím návrhem poslanec Jaroslav Krupka, který navrhl v § 97 odst. 3 ZEK pouze legislativně technickou změnu – přečíslování poznámek pod čarou v souvislosti s přijetím zákona č. 142/2012 Sb., o změně některých zákonů v souvislosti se zavedením základních registrů. Návrh zákona byl Poslaneckou sněmovnou schválen ve znění pozměňovacího návrhu ve třetím čtení dne 20. 6. 2012. Poslanecká sněmovna postoupila návrh zákona dne 26. 6. 2012 Senátu, který jej k doporučení všech dotčených výborů schválil ve znění přijatém Poslaneckou sněmovnou jako senátní tisk č. 383 dne 18. 7. 2012. Při jednání v Senátu ministr vnitra zdůraznil, že se právní úprava uchovávání provozních a lokalizačních údajů a jejich využití podstatně zpřísňuje. Prezident republiky zákon podepsal a dne 22. 8. 2012 byl vyhlášen ve Sbírce zákonů.

18. Ustanovení § 88a trestního řádu bylo dále novelizováno zákonem č. 455/2016 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů (dále jen „trestní zákoník“), a další související zákony, jehož vládní návrh byl poslancům rozeslán jako sněmovní tisk č. 886 dne 16. 8. 2016. První čtení návrhu zákona bylo uskutečněno dne 16. 9. 2016 a 19. 10. 2016, Poslanecká sněmovna návrh přijala ve zvláštním režimu již v prvním čtení a následně jej postoupila Senátu dne 4. 11. 2016. Senát návrh na doporučení Ústavně-právního výboru schválil ve znění přijatém Poslaneckou sněmovnou jako senátní tisk č. 348 dne 30. 11. 2016. Prezident republiky zákon podepsal a 29. 12. 2016 byl vyhlášen ve Sbírce zákonů.

19. Vládní návrh ZPol včetně napadených ustanovení § 68 odst. 2 a § 71 písm. a) byl poslancům rozeslán jako tisk č. 439 dne 29. 2. 2008. První čtení návrhu zákona proběhlo 25. 3. 2008 a následně jej výbory doporučily schválit ve znění jimi navržených pozměňovacích návrhů; ve druhém čtení prošel návrh zákona 10. a 18. 6. 2008. V podrobné rozpravě vystoupilo se svými pozměňovacími návrhy devět poslanců. Návrh zákona byl schválen ve znění přijatých pozměňovacích návrhů ve třetím čtení dne 25. 6. 2008. Poslanecká sněmovna postoupila návrh dne 8. 7. 2008 Senátu, který jej k doporučení všech dotčených výborů schválil ve znění přijatém Poslaneckou sněmovnou jako senátní tisk č. 301 dne 17. 7. 2008. Prezident republiky zákon podepsal a dne 11. 8. 2008 byl vyhlášen ve Sbírce zákonů.

b) Vyjádření Ministerstva průmyslu a obchodu

20. Ministerstvo průmyslu a obchodu, které vydalo napadenou vyhlášku č. 357/2012 Sb., o uchování, předávání a likvidaci provozních a lokalizačních údajů (dále jen „vyhláška“), považuje právní úpravu za vyváženou a vyhovující. Na podporu svého stanoviska odkazuje ministerstvo na sdělení Úřadu pro ochranu osobních údajů z roku 2012, který v meziresortním připomínkovém řízení označil návrh příslušné novely ZEK za přiměřený s ohledem na rozsah i podrobnost úpravy a na zakotvení práva člověka být informován o zpracování svých osobních údajů. Ministerstvo průmyslu a obchodu dále zdůrazňuje, že na tvorbě vyhlášky, vypracované v dohodě s Ministerstvem vnitra, se aktivně podíleli operátoři, Český telekomunikační úřad (dále též „ČTÚ“) i Úřad pro ochranu osobních údajů. Vyhláška vznikla jako kompromis mezi potřebami oprávněných subjektů, technickými možnostmi operátorů a požadavky kladenými na ochranu soukromí.

c) Vyjádření vlády

21. Vláda (dále též „vedlejší účastnice“) ve svém vyjádření nesouhlasí s tím, že napadená právní úprava nereaguje na rozhodnou judikaturu Soudního dvora Evropské unie a Ústavního soudu. Podle vlády bylo napadenou úpravou na všechny výtky ze strany Ústavního soudu reagováno adekvátně a nelze jí nic vyčíst. Ve vztahu k výše citovaným rozsudkům SDEU *Digital Rights Ireland Ltd* a *Tele2 Sverige AB* vláda upozorňuje, že ani v jednom z nich nebyla předmětem přezkumu česká právní úprava; rozsudky proto nemohly pro národní legislativu znamenat přímou ani nepřímou změnu. Vláda považuje českou právní úpravu v porovnání s jinými evropskými zeměmi za přísnou a souladnou s požadavky Soudního dvora Evropské unie.

22. Na příkladech z praxe vláda demonstruje, v jakých případech by bylo objasnění trestné činnosti bez využití ze zákona uchovaných provozních a lokalizačních údajů znemožněno. Vláda argumentuje tím, že ZEK stanoví nejen potřebný rozsah uchovaných údajů co do množství i časového intervalu jdoucí nad rámec údajů, které povinné subjekty uchovávají pro vlastní potřeby (např. vyúčtování služeb), ale i jednotnou formu zpracovávání, bez níž by se přístup k žádaným údajům ztížil. Požadavky na zabezpečení uchovávaných provozních a lokalizačních údajů obsažené v § 88 a násl. ZEK považuje vláda rovněž za dostačující.

23. K § 88a trestního řádu a námitce navrhovatelky ohledně příliš široké definice pojmu závažné trestné činnosti (*serious crime*) vláda uvádí, že právo EU konkrétní definici neposkytuje a je na členských státech, jak uvedený pojem vyloží. Do účinného znění § 88a trestního řádu byla podle vlády doplněna řada omezení a záruk, které již reflektují požadavky Ústavního soudu i Soudního dvora Evropské unie a nároky kladené na ochranu dotčených základních práv splňují. Vláda dodává, že konstrukce záruk a omezení je téměř totožná s nároky kladenými na využití odposlechu a záznamu telekomunikačního provozu podle § 88 trestního řádu, vyjma horní hranice trestní sazby a navazujícího taxativního výčtu trestných činů, u nichž lze provozní a lokalizační údaje využít. Nepostradatelná přidaná hodnota uchovávání předmětných údajů spočívá ve zjišťování informací o již uskutečněném telekomunikačním provozu, směřuje tedy na rozdíl od § 88 trestního řádu do minulosti – přitom se nedotýká obsahu komunikace, což je další podstatný rozdíl. V testu proporcionality by podle názoru vlády citované ustanovení obstálo ve všech třech krocích.

24. Provozní a lokalizační údaje představují důležitou „elektronickou stopu“, která hraje nezastupitelnou roli a vede policii k přijetí dalších efektivních opatření pro objasnění páchané trestné činnosti. Nadto podle vlády získání provozních a lokalizačních údajů šetří práva třetích osob, jelikož na jejich základě policie vyloučí možné podezřelé a vyhodnotí, že již není třeba žádat podání vysvětlení od většího počtu osob, ale jen od těch relevantních. Názor navrhovatelky, že pachatelé trestné činnosti používají mechanismy zajišťující důvěrnost komunikace a napadený nástroj proto nelze považovat za efektivní, vláda nesdílí, naopak jej považuje za argument ve prospěch zachování povinnosti provozní a lokalizační údaje uchovávat a za stanovených podmínek je oprávněným subjektům zpřístupňovat.

25. K údajnému nadužívání napadeného institutu vláda upozorňuje na chybnou interpretaci statistik, která je způsobena odlišnými metodami zpracování dat ze strany

ČTÚ a policie. Závěr o masivním zjišťování provozních a lokalizačních údajů orgány činnými v trestním řízení vláda s odkazem na grafy uvedené ve vyjádření odmítá.

26. Také napadená ustanovení ZPol považuje vláda za vyhovující. Podle § 68 odst. 2 uvedeného zákona je policie oprávněna údaje vyžádat v případě pátrání po hledané či pohřešované osobě, což jsou termíny zákonem definované; k tomu musí být kumulativně splněno několik podmínek. Riziko zneužití je minimální, zákonná úprava je nastavena přísně a je doplněna stejně přísnými interními akty. Absence soudního přezkumu je obhajitelná potřebou rychlé reakce, jelikož může být ohroženo zdraví i život osob, po kterých se pátrá. K § 71 písm. a) ZPol, týkajícímu se předcházení a odhalování hrozeb v oblasti terorismu, vláda dodává, že podle statistik jde o málo využívané ustanovení.

27. Oprávnění České národní banky získávat provozní a lokalizační údaje pro stíhání správních deliktů na úseku kapitálového trhu vychází podle vyjádření vlády z evropské legislativy a je s ní souladné [čl. 69 odst. 2 písm. r) směrnice Evropského parlamentu a Rady č. 2014/65/EU ze dne 15. 5. 2014 o trzích finančních nástrojů a o změně směrnic 2002/92/ES a 2011/61/EU (dále jen „směrnice o kapitálových trzích")].

d) Vyjádření Nejvyššího státního zastupitelství

28. Stanovisko Nejvyššího státního zastupitelství se zaměřuje na právní úpravu *data retention* ve spojení s § 88a trestního řádu; je v něm vyjádřeno přesvědčení, že i pokud by Ústavní soud dospěl k závěru o protiústavnosti § 97 odst. 3 a 4 ZEK, byl by § 88a trestního řádu udržitelný i samostatně, stejně jako v minulosti. Citované ustanovení podle NSZ splňuje požadavky Soudního dvora Evropské unie vyjádřené v rozsudku *Tele2 Sverige AB*, neboť závažná trestná činnost je zde vymezena dostatečně přísně a další kontrolní mechanismy (zejména odůvodněný soudní příkaz) jsou rovněž vyhovující. Nejvyšší státní zastupitelství se vymezuje proti tvrzení navrhovatelky, že hojné využívání provozních a lokalizačních údajů ze strany orgánů činných v trestním řízení nemá vliv na míru objasněnosti trestné činnosti. Přístup k údajům je podle NSZ pro směr a průběh (rychlost, a tedy i nižší nákladnost) trestního řízení určující; nelze odhlédnout od skutečnosti, že postupem doby je trestná činnost stále sofistikovanější, častěji se přesouvá na elektronické komunikační platformy (včetně internetu) a je páchána s jejich využitím.

29. Ve světle rozsudků SDEU Nejvyšší státní zastupitelství shledává nedostatečnou právní úpravu ZPol, neboť chybí podmíněnost přístupu policie předchozím souhlasem nezávislého orgánu rozhodujícího na základě odůvodněné žádosti a povinnost vyrozumět o přístupu k uchovávaným údajům dotčené osoby. Ustanovení § 68 odst. 2 však NSZ pro policii považuje za velmi důležité.

e) Vyjádření Úřadu pro ochranu osobních údajů

30. Ve svém vyjádření se Úřad pro ochranu osobních údajů ztotožnil s návrhem na zrušení napadených ustanovení; domnívá se, že kritéria nově nastavená v judikatuře SDEU nejsou v české právní úpravě zohledněna. Úřad vyzdvihuje přínos expertní skupiny WP 29 [Pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů, zřízená na základě čl. 29 Směrnice Evropského

parlamentu a Rady 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „WP 29“)], která již v roce 2001 v souvislosti s bojem proti terorismu upozorňovala na potřebu vyváženého přístupu z hlediska ochrany osobních údajů jakožto součásti základních práv a svobod jednotlivce. Již tehdy WP 29 vyjádřila obavy z narůstající tendence označovat ochranu osobních údajů za překážku efektivního boje proti terorismu a vyzvala k tomu, aby opatření proti terorismu nesnížila standard lidských práv.

31. Úřad pro ochranu osobních údajů ve vyjádření upozorňuje na skutečnost, že projednávanou věc je třeba vnímat i ve světle účinného nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, dále jen „GDPR“), jehož cílem je nalezení rovnováhy mezi ochranou základních práv a rozvojem komunikačních technologií.

f) Replika navrhovatelky

32. Ústavní soud zaslal výše uvedená vyjádření zástupci navrhovatelky k replice. Navrhovatelka odkázala na argumentaci přednesenou v návrhu na zrušení dotčených předpisů a nepovažovala za nutné na zaslaná vyjádření dále reagovat.

g) Ústní jednání

33. Ústavní soud nařídil ve věci veřejné ústní jednání podle § 44 zákona o Ústavním soudu, neboť pro lepší objasnění technických souvislostí a detailů projednávané problematiky považoval za nutné provést dokazování výslechem informovaných osob z řad odborné veřejnosti a osob z praxe podle § 49 odst. 1 téhož zákona. K ústnímu jednání byli předvoláni Mgr. Vanda Kellerová (zástupce jednoho z největších operátorů na trhu), doc. JUDr. Radim Polčák, Ph. D. (vedoucí Ústavu práva a technologií PrF MU), Mgr. Karel Bačkovský (vedoucí Oddělení bezpečnostně právního, Odbor bezpečnostní politiky Ministerstva vnitra), JUDr. Tomáš Sokol (prezident spolku Unie obhájců České republiky, z. s.), vrchní státní zástupkyně JUDr. Lenka Bradáčová a zástupci dotčených útvarů policie (plk. Ing. Vladimír Šibor, ředitel Útvaru zvláštních činností služby kriminální policie a vyšetřování Policejního prezidia ČR; plk. Ing. Bc. Josef Mareš, zástupce vedoucího Odboru obecné kriminality krajského ředitelství policie hl. města Prahy; plk. Mgr. Bc. František Habada, vedoucí Operačního odboru Policejního prezidia ČR).

34. Z výslechu Mgr. Kellerové Ústavní soud zjistil, že orgány činné v trestním řízení vyžadovaly v minulosti provozní a lokalizační údaje i bez konkrétní právní úpravy *data retention*, využívaly k tomu pouze jiné právní prostředky (§ 8 trestního řádu). U společnosti T-Mobile Czech Republic a. s. jsou údaje podle § 97 odst. 3 ZEK uchovávány zvlášť, přístup k nim je umožněn za splnění přísných podmínek; náklady spojené s plněním této zákonné povinnosti operátorovi hradí stát. Nejčastěji jsou žádána data za první tři měsíce od okamžiku jejich vzniku. Operátor pro své vlastní potřeby (vyúčtování a reklamace služeb) uchovává provozní a lokalizační údaje (v jiném, než napadenou vyhláškou stanoveném rozsahu, pro svou potřebu nepotřebuje všechny) po dobu dvou měsíců. K marketingovým účelům lze údaje uchovávat pouze na základě

souhlasu zákazníka (v případě společnosti T-Mobile Czech Republic a. s. jde zhruba o 70 % zákazníků), operátor je pak uchovává po dobu šesti měsíců. Zrušení napadené právní úpravy by znamenalo pro operátory stav značné právní nejistoty.

35. Z výslechu doc. Polčáka bylo zjištěno, že napadená právní úprava se nevymyká evropskému standardu; lze si představit, že budou např. nastaveny přísnější požadavky na zabezpečení uchovávaných údajů, příp. odstupňován přístup k nim podle závažnosti trestné činnosti (nikoli šest měsíců paušálně pro všechny zákonné účely). Absence právní úpravy *data retention* v některých státech neznamená, že by v nich příslušné orgány provozní a lokalizační údaje k vyšetřování trestné činnosti nevyužívaly, jsou pouze získávány jinými cestami.

36. Výslechem Mgr. Bačkovského bylo prokázáno, že při přípravě návrhu napadené úpravy bylo postupováno s vědomím nálezů Ústavního soudu sp. zn. Pl. ÚS 24/10 a Pl. ÚS 24/11; byl zvažován i vznik speciálního úřadu, u něhož by byla data shromažďována, nebezpečí jejich potenciálního zneužití při centrálním uchovávání u jedné instituce by však bylo větší. Vymezení trestné činnosti podle § 88a trestního řádu je podle něj dostatečně přísné, využití provozních a lokalizačních údajů v trestním řízení je nenahraditelné. Využití § 68 odst. 2 ZPol slouží k ochraně života a zdraví pohřešovaných osob, soudní přezkum z povahy věci nedává smysl.

37. JUDr. Sokol při výslechu uvedl, že podle jeho praktických zkušeností je záznam o provozních a lokalizačních údajích marginální záležitostí; týká se malého počtu případů, jeho vypovídající hodnota je spíše podpůrná, nepřímá, nejde o usvědčující důkaz.

38. Z výslechu JUDr. Bradáčové Ústavní soud zjistil, že z důvodu společenského i technologického vývoje nelze srovnávat roky 2008 a 2019, každý rok vznikají nové a sofistikovanější („modernější“) formy trestné činnosti. Z ročního nápadu trestních věcí se žádosti o záznam telekomunikačního provozu týkají cca 3 % případů. Záznam představuje mírnější opatření a slouží mnohdy jako „startovací“ důkaz, který orgány činné v trestním řízení dále nasměruje k využití invazivnějších prostředků (zejm. odposlechů). Při zvýšení horní hranice trestní sazby v § 88a trestního řádu by se povinné zadržování údajů netýkalo řady trestných činů, při jejichž vyšetřování se bez provozních a lokalizačních údajů obejít nelze (šíření toxikomanie, nebezpečné pronásledování, nebezpečné vyhrožování, trestné činy z nenávisti, šíření poplašné zprávy, dětská pornografie). Jde o novodobou, moderní stopu, nenahraditelnou vyšetřovací metodu, jež nemá adekvátní ekvivalent.

39. Výslechem plk. Ing. Šibora bylo zjištěno, že veškeré žádosti podle § 88a trestního řádu zpracovává a dotazy u operátorů realizuje celorepublikově výhradně Útvar zvláštních činností služby kriminální policie a vyšetřování Policejního prezidia ČR (dále jen „Útvar zvláštních činností“ nebo „ÚZČ“). Žádosti jsou autorizovány, uskutečněné dotazy jsou archivovány a lze je zpětně verifikovat, a to pouze prostřednictvím ředitele ÚZČ. Výpis provozních a lokalizačních údajů je méně invazivní než odposlech, často povolení odposlechu předchází. Zpráva o telekomunikačním provozu (o „zadržených datech“) je důkazem důležitým, nikoliv však jedinečným, musí být podložena i jinými důkazy. Činnost ÚZČ kontroluje pravidelně komise Poslanecké sněmovny (Stálá komise pro kontrolu použití odposlechu

a záznamu telekomunikačního provozu, použití sledování osob a věcí a rušení provozu elektronických komunikací) i Úřad na ochranu osobních údajů.

40. Z výslechu plk. Ing. Bc. Mareše vyplynulo, že záznam o provozních a lokalizačních údajích se často používá při vyšetřování závažné násilné a majetkové trestné činnosti. Zatímco u násilné trestné činnosti je výhodou, že se pachatel v nějakém okamžiku musí na místě činu fyzicky vyskytovat, u majetkové trestné činnosti tomu tak být nemusí, a pak orgánům činným v trestním řízení často nezbývají jiné než elektronické stopy. Záznam telekomunikačního provozu také napomáhá vyřadit některé vytipované osoby (recidivisty) ze seznamu podezřelých. V obecné rovině nelze říci, zda je šestiměsíční doba potřebná či nadbytečná, vždy záleží na okolnostech konkrétního případu. V době po prvním zásahu Ústavního soudu do oblasti *data retention* mohly 2-3 vraždy v jeho obvodu zůstat neobjasněny z důvodu nedostupnosti provozních a lokalizačních údajů.

41. Z výslechu plk. Mgr. Bc. Habady Ústavní soud k aplikaci § 68 odst. 2 ZPol zjistil, že jeho odbor spravuje centrální komunikační systém, do něhož se pohřešované osoby zadávají prostřednictvím čtrnácti krajských pracovišť, která zpracovávají tísňová volání. Ke zneužití nedochází, vyžádání lokalizace lze zpětně verifikovat. Oznamovatel je navíc vždy osobně konfrontován a „vytěžen" policejní hlídkou, případné zneužití pátrání by si tak rozmyslel. Asi v polovině případů se pohřešovaná osoba najde přesně v místě, kde bylo lokalizováno její elektronické zařízení. Takto se podaří např. včas vypátrat osoby pokoušející se o sebevraždu a tento následek odvrátit.

42. Z provedeného dokazování vyplynul tento závěr o skutkovém stavu: Operátoři se napadené právní úpravě přizpůsobili vytvořením nových technických řešení, vlastní náklady jim nevznikly a nevznikají ani v souvislosti s vyřizováním žádostí o přístup k provozním a lokalizačním údajům, tyto náklady hradí stát. Přístup k údajům probíhá výhradně prostřednictvím Útvaru zvláštních činností, v režimu ZPol lze získat pouze lokalizaci elektronického zařízení, nikoli všechny provozní a lokalizační údaje jako v případě žádostí podle § 88a trestního řádu. Napadená právní úprava se evropskému standardu nevymyká. Stejně jako technologie se vyvíjí i forma páchání trestné činnosti, stále častěji vznikají po pachatelích pouze elektronické stopy, vyšetřovací metody minulých let proto nelze srovnávat. Dosud nebylo v souvislosti s uchováváním provozních a lokalizačních údajů ani s jejich zpřístupňováním zjištěno žádné systémové selhání.

V. Přezkum procedury přijetí napadených předpisů

43. Ústavní soud v intencích § 68 odst. 2 zákona o Ústavním soudu přezkoumal, zda byla napadená ustanovení ZEK, trestního řádu a ZPol přijata i vydána v mezích Ústavou stanovené kompetence a předepsaným způsobem. Dospěl k závěru, že v tomto směru nelze zákonodárci nic vytýkat – účastníci řízení ani vedlejší účastnice ostatně žádné deficity legislativního procesu neuvádějí. Pro stručnost Ústavní soud odkazuje na shrnutí průběhu legislativního procesu ve vyjádřeních komor Parlamentu.

44. Vyhláška byla vydána Ministerstvem průmyslu a obchodu. Pravomoc ministerstev vydávat právní předpisy k provedení zákona vyplývá z článku 79 odst. 3 Ústavy, materiálně je však podmíněna existencí výslovného zákonného zmocnění a jeho mezemi. V daném případě je zmocněním právě napadené ustanovení

§ 97 odst. 4 ZEK – materiální podmínka pro vydání podzákonného předpisu je splněna. Vyhláška byla podepsána ministrem průmyslu a obchodu a řádně publikována ve Sbírce zákonů s účinností dnem jejího vyhlášení (17. 10. 2012).

VI. Meritorní přezkum návrhu

45. Po přezkoumání formálních náležitostí návrhu, bezvadnosti procesu přijetí napadených právních předpisů a provedeném dokazování Ústavní soud věcně přezkoumal námitky navrhovatelky k napadené právní úpravě a dospěl k následujícím závěrům.

a) Obecná východiska

Právo na soukromí, informační sebeurčení a komunikační svoboda

46. Uchovávání provozních a lokalizačních údajů se bezprostředně dotýká ústavně garantovaného práva na ochranu soukromí ve smyslu čl. 10 odst. 2 a 3, čl. 13 Listiny a čl. 8 Úmluvy. Soukromí představuje jeden ze stěžejních prvků svobody jednotlivce, která patří mezi nejdůležitější hodnoty liberální demokracie, a jeho ochrana se projevuje v mnoha různých aspektech, o čemž svědčí komplexní zakotvení tohoto základního práva v několika různých ustanoveních Listiny. V projednávané věci jde konkrétněji o tzv. právo na informační sebeurčení (čl. 10 odst. 3 Listiny) a komunikační svobodu (čl. 13 Listiny). Právo na informační sebeurčení chrání jednotlivce před neoprávněným shromažďováním, zveřejňováním anebo jiným zneužíváním údajů o jeho osobě. Komunikační svobodou je chráněno listovní tajemství a tajemství přepravovaných zpráv, ať již uchovávaných v soukromí, nebo zasílaných poštou, podávaných telefonem, telegrafem nebo jiným zařízením či způsobem.

47. Ústavní soud podrobně vyložil obecná východiska týkající se práva na soukromí a přípustnost omezení tohoto práva ve prospěch ústavně aprobovatelného veřejného zájmu již ve výše zmíněném nálezu sp. zn. Pl. ÚS 24/10, na jehož odůvodnění zejména v bodech 26 až 40 Ústavní soud odkazuje. Pouze ve stručnosti – Ústavní soud zejména vyložil, že svou povahou i významem právo na informační sebeurčení spadá mezi základní lidská práva a svobody, protože spolu se svobodou osobní, svobodou v prostorové dimenzi (domovní) a komunikační dotváří osobnostní sféru jedince, jehož individuální integritu, jako nezbytnou podmínku důstojné existence a rozvoje lidského života vůbec, je nutno respektovat a důsledně chránit. Respekt a ochrana této sféry je garantována ústavním pořádkem, neboť jde o výraz úcty k právům a svobodám člověka (čl. 1 odst. 1 Ústavy).

48. Z ustálené judikatury Ústavního soudu, zejména ve vztahu k problematice odposlechů telefonních hovorů, zřetelně vyplývá, že ochrana práva na respekt k soukromému životu ve smyslu čl. 10 odst. 3 a čl. 13 Listiny se vztahuje nejen k vlastnímu obsahu zpráv podávaných telefonem, ale i k údajům o volaných číslech, datu a čase hovoru, době jeho trvání, v případě mobilní telefonie i základnových stanicích zajišťujících hovor [srov. např. nález sp. zn. II. ÚS 502/2000 ze dne 22. 1. 2001 (N 11/21 SbNU 83), sp. zn. IV. ÚS 78/01 ze dne 27. 8. 2001 (N 123/23 SbNU 197), sp. zn. I. ÚS 191/05 ze dne 13. 9. 2006 (N 161/42 SbNU 327)

či sp. zn. II. ÚS 789/06 ze dne 27. 9. 2007 (N 150/46 SbNU 489)]. Uvedené informace o probíhající elektronické komunikaci tvoří právě provozní a lokalizační údaje.

49. Prostřednictvím shromažďovaných informací lze, přestože není (na rozdíl od odposlechů) uchováván obsah komunikace, sestavit podrobný záznam pohybu jednotlivce i jeho osobní a komunikační profil (osobní vazby, prostředí, společenské postavení, politická orientace, zdravotní stav nebo sexuální orientace). Jednotlivcem je přitom každý uživatel mobilního telefonu a počítače, tedy téměř každý občan České republiky. V případě internetových služeb je navíc velmi tenká, někdy sotva seznatelná hranice mezi provozním údajem a samotným obsahem.

50. Tzv. „metadata“ o uskutečněné komunikaci (tj. vše kromě obsahu) mohou být z hlediska zásahu do soukromí jednotlivce ve skutečnosti mnohem cennější a fakticky i „nebezpečnější“ než znalost samotného obsahu komunikace, neboť jsou strojově zpracovatelná a analyzovatelná; z výsledků takového zpracování pak lze usuzovat budoucí chování jednotlivce. Obsah naopak může být ve skutečnosti „bezobsažný“ – nepřejí-li si účastníci komunikace, aby byl srozumitelný, dorozumívají se pomocí náznaků či předem smluvených šifer. Sběr a uchovávání provozních a lokalizačních údajů proto také představuje významný zásah do práva na soukromí a zasluhuje z hlediska práva na soukromí obdobnou úroveň záruk proti zneužití jako samotný obsah komunikace. Je proto nezbytné pod rozsah ochrany základního práva na respekt k soukromému životu zahrnout nejen ochranu vlastního obsahu zpráv podávaných prostřednictvím telefonické komunikace nebo komunikace prostřednictvím tzv. veřejných sítí, ale i provozní a lokalizační údaje o nich (srov. nález sp. zn. Pl. ÚS 24/10).

51. Základní právo lze omezit jen na základě zákona a pouze v míře, která je v podmínkách demokratického právního státu nezbytná, při zachování záruk ochrany jednotlivce před projevy libovůle ze strany veřejné moci. Omezení základního práva musí především odpovídat nárokům plynoucím z principu právního státu a naplňovat požadavky vycházející z testu proporcionality – v případech střetů základních práv či svobod s veřejným zájmem nebo s jinými základními právy či svobodami je třeba posuzovat účel (cíl) zásahu ve vztahu k použitým prostředkům, přičemž měřítkem pro posouzení je zásada proporcionality (v širším smyslu). Předmětná právní úprava musí být přesná, zřetelná ve svých formulacích a dostatečně předvídatelná, aby potenciálně dotčeným jednotlivcům poskytovala dostatečnou informaci o okolnostech a podmínkách, za kterých je veřejná moc oprávněna k zásahu do jejich soukromí (čl. 2 odst. 2 Listiny), a ti případně mohli upravit své chování, aby se nedostali do konfliktu s omezující normou (čl. 2 odst. 3 Listiny). Rovněž musí být striktně definovány i pravomoci udělené příslušným orgánům, způsob a pravidla jejich provádění tak, aby jednotlivcům byla poskytnuta ochrana proti svévolnému zasahování.

52. Posouzení přípustnosti daného zásahu podle zásady proporcionality (v širším smyslu) zahrnuje tři kritéria. Prvním z nich je posouzení způsobilosti naplnění účelu (nebo také vhodnosti) – je zjišťováno, zda je konkrétní opatření vůbec schopno dosáhnout zamýšleného cíle, jímž je ochrana jiného základního práva nebo veřejného statku. Dále se ve druhém kroku posuzuje potřebnost – je zkoumáno, zda byl při výběru prostředků použit ten, který je k základnímu právu nejšetrnější. Konečně je hodnocena přiměřenost (v užším smyslu), tj. zda újma na základním právu není nepřiměřená ve vazbě na zamýšlený cíl. Opatření omezující základní lidská práva a svobody tedy

nesmějí, jde-li o kolizi základního práva či svobody s veřejným zájmem, svými negativními důsledky převyšovat pozitiva, která představuje veřejný zájem na přijatých opatřeních [srov. nález sp. zn. Pl. ÚS 3/02 ze dne 13. 8. 2002 (N 105/27 SbNU 177; 405/2002 Sb.)].

Právo EU a Soudní dvůr Evropské unie

53. Česká republika podle čl. 1 odst. 2 Ústavy dodržuje závazky, které pro ni vyplývají z mezinárodního práva. Unijní právo proniká do českého právního řádu prostřednictvím čl. 10a Ústavy, na jehož základě český zákonodárce přenesl část své pravomoci na zákonodárce unijního. Vztah ústavního pořádku České republiky a unijního práva, za jehož součást je považována i judikatura SDEU, prošel v průběhu doby určitým vývojem, k němuž měl Ústavní soud v minulosti více příležitostí se vyjádřit.

54. Obsah čl. 1 odst. 2 Ústavy ve vztahu k právu Evropské unie Ústavní soud vyložil tak, že domácí právní předpisy, včetně Ústavy, mají být interpretovány souladně s principy evropské integrace a spolupráce unijních orgánů a orgánů členského státu. Existuje-li několik interpretací ustanovení ústavního pořádku a jen některé z nich vedou k dosažení závazku, který převzala Česká republika v souvislosti se svým členstvím v Evropské unii, je nutno volit eurokonformní výklad podporující realizaci závazku, nikoli výklad, jenž realizaci znemožňuje [viz nález sp. zn. Pl. ÚS 50/04 ze dne 8. 3. 2006 (N 50/40 SbNU 443; 154/2006 Sb.), či nález sp. zn. Pl. ÚS 66/04 ze dne 3. 5. 2006 (N 93/41 SbNU 195; 434/2006 Sb.)]. Jinými slovy, v oblasti spadající do působnosti práva EU interpretuje ústavní právo s přihlédnutím k principům plynoucím z práva unijního [obdobně viz také nález sp. zn. Pl. ÚS 36/05 ze dne 16. 1. 2007 (N 8/44 SbNU 83; 57/2007 Sb.). Vše uvedené platí při zachování limitu, kterým je tzv. materiální jádro ústavního pořádku, tedy podstatných náležitostí demokratického právního státu ve smyslu čl. 9 odst. 2 Ústavy [viz nález sp. zn. Pl. ÚS 19/08 ze dne 26. 11. 2008 (N 201/51 SbNU 445; 446/2008 Sb.)]. Unijní právo sice není referenčním kritériem pro posuzování ústavnosti vnitrostátního právního předpisu a rozpor s normou unijního práva sám o sobě k derogaci zákona vést nemůže, přesto je při interpretaci ústavního práva k předpisům unijního práva a judikatuře SDEU třeba přihlížet.

55. Problematika *data retention* spadá do působnosti unijního práva, jak patrno ze snahy evropského zákonodárce o zakotvení jednotného rámce pro vnitrostátní právní úpravy. Směrnice o *data retention*, na jejímž základě byla přijata napadená právní úprava, byla Soudním dvorem Evropské unie prohlášena za neplatnou a nová evropská úprava dosud přijata nebyla. Vznikl tak legislativní prostor uvolněný zneplatněním směrnice o *data retention*, který mohou členské státy (tedy i Česká republika) zaplnit – jelikož jde o oblast pravomoci jimi sdílené s EU (nikoliv výlučné pravomoci EU) – v rozsahu, v jakém ji EU nevykonala nebo ji přestala efektivně vykonávat (čl. 2 odst. 2 Smlouvy o fungování Evropské unie); při zaplňování uvolněného legislativního prostoru dbá zákonodárce členského státu nosných důvodů rozsudku SDEU, jímž byla dotčená unijní úprava zneplatněna (zde konkrétně rozsudek *Digital Rights Ireland Ltd*).

b) Prejudikatura

56. Napadená právní úprava ZEK a trestního řádu byla přijata v reakci na výše uvedené derogační nálezy Ústavního soudu sp. zn. Pl. ÚS 24/10 a Pl. ÚS 24/11.

V navazující časové souslednosti vydal Soudní dvůr Evropské unie též výše uvedené rozsudky *Digital Rights Ireland Ltd* a *Tele2 Sverige AB*.

57. Prvním ze zmiňovaných nálezů sp. zn. Pl. ÚS 24/10 ze dne 22. 3. 2011 zrušil Ústavní soud ustanovení § 97 odst. 3 a 4 ZEK, v tehdejším znění, jakož i vyhlášku Ministerstva informatiky č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání. Ústavní soud aplikoval judikaturu Evropského soudu pro lidská práva (dále též „ESLP"), vztahující se k užití odposlechů (zejména rozhodnutí ve věci *Malone proti UK*, stížnost č. 8691/79 ze dne 2. 8. 1984), a zopakoval jeho požadavky na právní úpravu umožňující zásah do práva na soukromý život veřejnou mocí. Evropský soud pro lidská práva považuje za nutné vymezit na zákonné úrovni jasná pravidla upravující rozsah použití omezujících opatření, stanovit minimální požadavky na délku a způsob uložení získaných informací, na jejich použití i přístup třetích osob k nim, a zakotvit procedury k ochraně důvěrnosti údajů i k jejich zničení; vše tak, aby jednotlivci disponovali dostatečnými zárukami ochrany proti jejich zneužití. V § 97 odst. 3 ZEK v původním znění nebyl jasně a přesně vymezen okruh oprávněných orgánů, účel poskytnutí provozních a lokalizačních údajů ani podmínky jejich použití, a to ani v návaznosti na zvláštní předpisy, na něž napadená norma odkazovala. Ústavní soud zkritizoval také absenci jasných a detailních pravidel obsahujících minimální požadavky na zabezpečení uchovávaných údajů (zamezení přístupu třetích osob, stanovení procedury vedoucí k ochraně důvěrnosti a celistvosti údajů, procedury jejich ničení) a záruk proti riziku jejich zneužití.

58. O několik měsíců později Ústavní soud v návaznosti na nález sp. zn. Pl. ÚS 24/10 zrušil nálezem sp. zn. Pl. ÚS 24/11 ze dne 20. 12. 2011 pro vágnost a neurčitost také § 88a trestního řádu. V testu proporcionality nebylo naplněno druhé kritérium nezbytnosti, neboť neurčitá a široká formulace účelu *(„objasnění skutečností důležitých pro trestní řízení")* umožňovala vyžádání a použití údajů v podstatě v jakékoli souvislosti s libovolným trestním řízením. Uvedený nedostatek nebylo podle Ústavního soudu možné překlenout ani ústavně konformním výkladem. Ústavní soud nenalezl důvod, pro který by se měl lišit rozsah zákonem stanovených garancí při využití nástrojů podle § 88 trestního řádu (odposlechy – budoucí telekomunikační provoz včetně obsahu komunikace) a § 88a trestního řádu (provozní a lokalizační údaje – v minulosti uskutečněný telekomunikační provoz bez obsahu komunikace), neboť v obou případech je intenzita zásahu do práva na soukromí srovnatelná. Nad rámec požadavků kladených na dotčenou právní úpravu v nálezu sp. zn. Pl. ÚS 24/10 zde Ústavní soud doplnil, že účinná ochrana před nezákonným zásahem do základních práv a svobod dotčených osob by měla být zaručena prostřednictvím povinnosti dodatečně informovat uživatele služeb elektronické komunikace o tom, že jeho provozní a lokalizační údaje byly sděleny orgánům činným v trestním řízení.

59. Soudní dvůr Evropské unie později rozsudkem *Digital Rights Ireland Ltd* ze dne 8. 4. 2014 prohlásil směrnici o *data retention* za neplatnou pro rozpor s čl. 7 (respektování soukromého a rodinného života) a čl. 8 (ochrana osobních údajů) Listiny základních práv EU. Přestože byla směrnice způsobilá dosáhnout sledovaného cíle (harmonizace úpravy *data retention* na poli boje proti závažné trestné činnosti), ani takový cíl sám o sobě nemohl odůvodnit, aby opatření týkající se všech prostředků elektronické komunikace a spočívající v uchovávání údajů téměř celé evropské populace bylo považováno za nezbytné. Soudní dvůr Evropské unie vyslovil požadavek

cílené souvislosti mezi uchovávanými údaji a ohrožením veřejné bezpečnosti (údaje vztahující se k určitému časovému období, určité zeměpisné oblasti či okruhu určitých osob, jež mohou být jakýmkoli způsobem zapojeny do závažné trestné činnosti, anebo k osobám, které by prostřednictvím uchovávání jejich údajů mohly z jiných důvodů přispívat k boji proti závažné trestné činnosti).

60. Následně Soudní dvůr Evropské unie rozsudkem *Tele2 Sverige AB* ze dne 21. 12. 2016 zodpověděl předběžné otázky Velké Británie a Švédska ohledně výkladu čl. 15 odst. 1 *e-privacy* směrnice v souvislosti se zneplatněním směrnice o *data retention* a z toho plynoucích důsledků pro vnitrostátní právní úpravy členských států. Podle čl. 15 odst. 1 *e-privacy* směrnice členské státy mohou přijmout legislativní opatření omezující rozsah ochrany osobních údajů ve smyslu směrnice, představuje-li omezení 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 prevenci neoprávněného použití elektronického komunikačního systému. Soudní dvůr Evropské unie uvedl, že citované ustanovení, umožňující členským státům výjimku z pravidla poskytování ochrany osobním údajům, je třeba vykládat restriktivně – nelze akceptovat stav, kdy se z výjimky stane pravidlo, jako je tomu v případě plošného a nevýběrového uchovávání velkého množství dat. Vnitrostátní právní úprava musí podle SDEU účinně vymezovat vztah mezi údaji, které mají být uchovávány, a sledovaným účelem, tj. musí umožňovat účinné vymezení rozsahu opatření (okruh osob z řad veřejnosti, jejichž údaje mohou vykázat minimálně nepřímou souvislost se závažnou trestnou činností, nebo mohou přispívat k boji proti ní a k předcházení závažného ohrožení veřejné bezpečnosti).

61. Dalším rozsudkem ve věci C-207/16 ze dne 2. 9. 2018 (*Ministerio Fiscal*) SDEU částečně zmírnil přísný tón v otázce účelu zpřístupňování provozních a lokalizačních údajů; k samotnému principu *data retention* se zde nevyjádřil. K předběžné otázce španělského soudu ohledně výkladu téhož ustanovení jako v předchozím případě – čl. 15 *e-privacy* směrnice – konstatoval, že zpřístupnění údajů, jako je jméno, příjmení a adresa držitelů SIM karet aktivovaných v odcizeném mobilním telefonu za účelem jejich identifikace orgánům veřejné moci nezasahuje do základních práv těchto držitelů zakotvených v čl. 7 a 8 Listiny základních práv EU natolik závažným způsobem, aby přístup k nim měl být v oblasti prevence, vyšetřování, odhalování a stíhání trestných činů omezen pouze na boj proti závažné trestné činnosti.

62. V nedávné době měl i Evropský soud pro lidská práva příležitost rekapitulovat svoji judikaturu vztahující se k odposlechům a při té příležitosti se vyjádřit k *data retention*. V rozsudku ze dne 13. 9. 2018, stížnosti č. 58170/13, 62322/14 a 24960/15 (*Big Brother Watch proti Spojenému království*), konstatoval v souvislosti s poskytnutím komunikačních údajů porušení nejen čl. 8 Úmluvy garantujícího respekt k soukromému životu, ale i čl. 10 Úmluvy, který zaručuje svobodu projevu. Porušení čl. 8 Úmluvy bylo konkrétně spatřováno ve vyžádání údajů o několika telefonních číslech ze strany vyšetřujících orgánů, jehož účelem bylo odhalení informačního zdroje novináře (nikoli cíl sledující vymezený veřejný zájem) a jež nepodléhalo předchozímu schválení soudem nebo nezávislým správním úřadem. V těchto dvou aspektech se podle závěrů ESLP postup dotčených orgánů a platná legislativa Velké Británie neslučovaly ani s požadavky plynoucími z prezentované judikatury SDEU. Soud spatřoval v absenci zvláštní právní úpravy, která by poskytovala přísnější ochranu

využívání provozních a lokalizačních údajů ve vztahu k ochraně svobody tisku (činnost novinářů), také porušení svobody projevu ve světle čl. 10 Úmluvy.

c) Ústavněprávní přezkum napadené právní úpravy

63. Projednávanou problematiku je třeba rozdělit do dvou rovin, které jsou na sobě zdánlivě nezávislé, ve skutečnosti však z hlediska ústavněprávního přezkumu představují spojené nádoby.

64. Zaprvé je třeba zodpovědět otázku, zda je ve světle výše vyložených základních práv vůbec přípustné, aby byla plošně, neadresně a preventivně shromažďována a uchovávána data napadeného rozsahu (§ 97 odst. 3 a 4 ZEK a vyhláška) – musí být tedy zkoumána zákonná povinnost ke sběru a uchovávání provozních a lokalizačních údajů jako taková.

65. Zadruhé je v případě kladné odpovědi na první otázku třeba zabývat se otázkou vhodného vymezení okruhu orgánů oprávněných k přístupu ke shromažďovaným údajům ve vazbě na stanovení legitimních cílů, jejichž naplnění má využití provozních a lokalizačních údajů sloužit, včetně stanovení zákonných podmínek a záruk ochrany pro minimalizaci zásahu do základních práv jednotlivců [§ 97 odst. 3 ZEK, § 88a trestního řádu a § 68 odst. 2 a § 71 písm. a) ZPol].

66. Ústavní soud vzal v úvahu argumentaci zúčastněných, zhodnotil důkazy, následně provedl test proporcionality a dospěl k závěru, že současná úprava *data retention* naplňuje požadavky kladené citovanou dřívější judikaturou Ústavního soudu a lze ji aplikovat ústavně konformním způsobem, tedy tak, aby byla maximálně šetřena práva jednotlivců, garantovaná články 10 a 13 Listiny. Návrh byl proto zamítnut z důvodů dále uvedených.

Napadená právní úprava

67. Ustanovení § 97 odst. 3 a 4 ZEK zní:

Odposlech a záznam zpráv
§ 97

(3) Právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna uchovávat po dobu 6 měsíců provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování jejích veřejných komunikačních sítí a při poskytovávání jejích veřejně dostupných služeb elektronických komunikací. Provozní a lokalizační údaje týkající se neúspěšných pokusů o volání je právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací povinna uchovávat pouze tehdy, jsou-li tyto údaje vytvářeny nebo zpracovávány a zároveň uchovávány nebo zaznamenávány. Současně je tato právnická nebo fyzická osoba povinna zajistit, aby při plnění povinnosti podle věty první a druhé nebyl uchováván obsah zpráv a takto uchovávaný dále předáván. Právnická nebo fyzická osoba, která provozní a lokalizační údaje uchovává, je na požádání povinna je bezodkladně poskytnout

a) orgánům činným v trestním řízení pro účely a při splnění podmínek stanovených zvláštním právním předpisem,

b) Policii České republiky pro účely zahájeného pátrání po konkrétní hledané nebo pohřešované osobě, zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly, předcházení nebo odhalování konkrétních hrozeb v oblasti terorismu nebo prověřování chráněné osoby a při splnění podmínek stanovených zvláštním právním předpisem,

c) Bezpečnostní informační službě pro účely a při splnění podmínek stanovených zvláštním právním předpisem,

d) Vojenskému zpravodajství pro účely a při splnění podmínek stanovených zvláštním právním předpisem,

e) České národní bance pro účely a při splnění podmínek stanovených zvláštním právním předpisem.

Po uplynutí doby podle věty první je právnická nebo fyzická osoba, která provozní a lokalizační údaje uchovává, povinna je zlikvidovat, pokud nebyly poskytnuty orgánům oprávněným k jejich využívání podle zvláštního právního předpisu nebo pokud tento zákon nestanoví jinak (§ 90).

(4) Provozními a lokalizačními údaji podle odstavce 3 jsou zejména údaje vedoucí k dohledání a identifikaci zdroje a adresáta komunikace a dále údaje vedoucí ke zjištění data, času, způsobu a doby trvání komunikace. Rozsah provozních a lokalizačních údajů uchovávaných podle odstavce 3, formu a způsob jejich předávání orgánům oprávněným k využívání podle zvláštního právního předpisu a způsob jejich likvidace stanoví prováděcí právní předpis.

68. Dikci vyhlášky Ústavní soud pro její rozsah nepovažuje za nutné uvádět; pro účely odůvodnění nálezu postačí stručná rekapitulace jejího znění, které konkretizuje druh uchovávaných údajů. Podle § 2 vyhlášky jsou to zejména telefonní čísla účastníků komunikace, datum a čas zahájení komunikace (odeslání zprávy), délka komunikace, u mobilních telefonů dále identifikátor IMSI (mezinárodní identifikátor účastníka veřejné mobilní komunikační sítě přidělený operátorem) a identifikátor mobilního přístroje účastníků komunikace. V případě internetových služeb se uchovává zejména typ připojení, označení uživatele, datum a čas připojení k internetu, označení přístupového bodu, adresa IP a u služeb elektronické komunikace rovněž údaje o připojení ke schránce elektronické pošty, odesílání i přijímání pošty včetně adres odesílatelů a příjemců. Dále vyhláška upravuje podrobnosti procesu poskytování uchovávaných údajů oprávněným orgánům a jejich likvidace po uplynutí zákonem stanovené doby.

69. Ustanovení § 88a trestního řádu zní:

§ 88a

(1) Je-li třeba pro účely trestního řízení vedeného pro úmyslný trestný čin, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně tři roky, pro trestný čin porušení tajemství dopravovaných zpráv (§ 182 trestního zákoníku), pro trestný čin podvodu (§ 209 trestního zákoníku), pro trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací (§ 230 trestního zákoníku), pro trestný čin opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 trestního zákoníku), pro trestný čin nebezpečného vyhrožování (§ 353 trestního zákoníku), pro trestný čin nebezpečného pronásledování (§ 354 trestního zákoníku), pro trestný čin šíření poplašné zprávy (§ 357 trestního zákoníku), pro trestný čin podněcování k trestnému činu (§ 364 trestního zákoníku), pro trestný čin schvalování trestného činu (§ 365 trestního zákoníku), nebo pro úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva, kterou je Česká republika vázána, zjistit údaje o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat a nelze-li sledovaného účelu dosáhnout jinak nebo bylo-li by jinak jeho dosažení podstatně ztížené, nařídí v řízení před soudem jejich vydání soudu předseda senátu a v přípravném řízení nařídí jejich vydání státnímu zástupci nebo policejnímu orgánu soudce na návrh státního zástupce. Příkaz k zjištění údajů o telekomunikačním provozu musí být vydán písemně a odůvodněn, včetně konkrétního odkazu na vyhlášenou mezinárodní smlouvu v případě, že se vede trestní řízení pro trestný čin, k jehož stíhání tato mezinárodní smlouva zavazuje. Vztahuje-li se žádost ke konkrétnímu uživateli, musí být v příkazu uvedena jeho totožnost, je-li známa.

(2) Státní zástupce nebo policejní orgán, jehož rozhodnutím byla věc pravomocně skončena, a v řízení před soudem předseda senátu soudu prvního stupně po pravomocném skončení věci informuje o nařízeném zjišťování údajů o telekomunikačním provozu osobu uživatele uvedenou v odstavci 1, pokud je známa. Informace obsahuje označení soudu, který vydal příkaz k zjištění údajů o telekomunikačním provozu, a údaj o období, jehož se tento příkaz týkal. Součástí informace je poučení o právu podat ve lhůtě šesti měsíců ode dne doručení této informace Nejvyššímu soudu návrh na přezkoumání zákonnosti příkazu k zjištění údajů o telekomunikačním provozu. Informaci podá předseda senátu soudu prvního stupně bezodkladně po pravomocném skončení věci, státní zástupce, jehož rozhodnutím byla věc pravomocně skončena, podá informaci bezodkladně po uplynutí lhůty pro přezkoumání jeho rozhodnutí nejvyšším státním zástupcem podle § 174a a policejní orgán, jehož rozhodnutím byla věc pravomocně skončena, podá informaci bezodkladně po uplynutí lhůty pro přezkoumání jeho rozhodnutí státním zástupcem podle § 174 odst. 2 písm. e).

(3) Informaci podle odstavce 2 předseda senátu, státní zástupce nebo policejní orgán nepodá v řízení o zločinu, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně osm let, spáchaném organizovanou skupinou, v řízení o trestném činu spáchaném ve prospěch organizované zločinecké skupiny, v řízení o trestném činu účasti

na organizované zločinecké skupině (§ 361 trestního zákoníku), v řízení o trestném činu účasti na teroristické skupině (§ 312a trestního zákoníku) nebo pokud se na spáchání trestného činu podílelo více osob a ve vztahu alespoň k jedné z nich nebylo trestní řízení doposud pravomocně skončeno, nebo pokud je proti osobě, jíž má být informace sdělena, vedeno trestní řízení, anebo pokud by poskytnutím takové informace mohl být zmařen účel tohoto nebo jiného trestního řízení, nebo by mohlo dojít k ohrožení bezpečnosti státu, života, zdraví, práv nebo svobod osob.

(4) Příkazu podle odstavce 1 není třeba, pokud k poskytnutí údajů dá souhlas uživatel telekomunikačního zařízení, ke kterému se mají údaje o uskutečněném telekomunikačním provozu vztahovat.

70. Ustanovení § 68 odst. 2 a 71 písm. a) ZPol zní:

Pátrání po osobách a věcech
§ 68
(2) Policie může žádat pro účely zahájeného pátrání po konkrétní hledané nebo pohřešované osobě a za účelem zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly poskytnutí provozních a lokalizačních údajů od právnické nebo fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací způsobem umožňujícím dálkový a nepřetržitý přístup, nestanoví-li jiný právní předpis jinak. Informace se poskytne ve formě a v rozsahu stanoveném jiným právním předpisem.

§ 71
Útvar policie, jehož úkolem je boj s terorismem, může za účelem předcházení a odhalování konkrétních hrozeb v oblasti terorismu v nezbytném rozsahu žádat od

a) právnické nebo fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací poskytnutí provozních a lokalizačních údajů způsobem umožňujícím dálkový a nepřetržitý přístup, nestanoví-li jiný právní předpis jinak; informace se poskytne ve formě a v rozsahu stanoveném jiným právním předpisem,
...

Princip *data retention*

71. Především je podle Ústavního soudu třeba zabývat se z hlediska omezení dotčených základních práv otázkou přípustnosti zákonem upraveného principu plošného uchovávání provozních a lokalizačních údajů soukromými subjekty – jako takového. Omezení osobní integrity a soukromí osob veřejnou mocí připouští Listina pouze ve výjimečných případech – je-li to v demokratické společnosti nezbytné, nelze-li účelu sledovaného veřejným zájmem dosáhnout jinak a je-li to akceptovatelné z pohledu zákonné existence a dodržení účinných a konkrétních záruk proti libovůli.

72. Nyní napadená ustanovení § 97 odst. 3 a 4 ZEK a § 88a trestního řádu byla přijata zákonem č. 273/2012 Sb. s účinností od 1. 10. 2012 v reakci na nález

sp. zn. Pl. ÚS 24/10. Ústavní soud v citovaném nálezu, jímž bylo zrušeno dřívější znění § 97 odst. 3 a 4 ZEK, uzavřel, že plošný, preventivní sběr a uchovávání údajů je zásah do práva na soukromí a na informační sebeurčení natolik intenzivní, že je třeba na splnění výše uvedených požadavků přípustnosti zásahu klást co nejpřísnější měřítka – dřívější právní úprava ZEK v tomto ohledu podle Ústavního soudu neobstála. Ústavní soud v již citovaném nálezu jako *obiter dictum* vyjádřil pochybnosti nad nezbytností a přiměřeností samotného nástroje plošného a preventivního sběru metadat veškeré elektronické komunikace z hlediska intenzity zásahu do soukromé sféry značného počtu jednotlivců, stejně jako nad skutečností, že jsou citlivá data soustředěna v rukou soukromých osob – operátorů (tj. poskytovatelů služeb v oblasti internetu a telefonní a mobilní komunikace).

73. Zákonodárce zareagoval na výtky Ústavního soudu tak, že zkrátil dobu uchovávání provozních a lokalizačních údajů na šest měsíců, explicitně vyjmenoval subjekty oprávněné k vyžádání uchovaných údajů včetně účelů, k jakým mohou oprávněné subjekty údaje žádat, doplnil zákonnou definici provozních a lokalizačních údajů a v podrobnostech opět odkázal na prováděcí předpis (napadená vyhláška).

74. V mezidobí byla rozsudkem SDEU *Digital Rights Ireland* zneplatněna směrnice o *data retention*, na jejímž základě byl princip *data retention* do českého právního řádu zaveden (viz bod 59). V reakci na tento rozsudek pak členské státy pokládaly Soudnímu dvoru Evropské unie předběžné otázky ohledně souladu vnitrostátních úprav uchovávání provozních a lokalizačních údajů a nakládání s nimi se směrnicí o soukromí a elektronických komunikacích, z nichž stěžejní je rozsudek *Tele 2 Sverige AB* (viz bod 60). Soudní dvůr Evropské unie podle této judikatury shledal princip obecného a plošného sběru všech údajů o veškeré uskutečněné elektronické komunikaci rozporným s čl. 15 odst. 1 *e-privacy* směrnice, potažmo s čl. 7 a 8 Listiny základních práv Evropské unie, zaručujících ochranu soukromí a osobních údajů. Na evropské úrovni však nepanuje politická shoda na podobě unifikované úpravy problematiky *data retention*, o čemž svědčí skutečnost, že od zneplatnění směrnice o *data retention* rozsudkem *Digital Rights Ireland* dosud nevznikl návrh nové právní úpravy, jež by uvedenou směrnici nahradila. Na úrovni vnitrostátních legislativ se proto lze setkat s různými přístupy zákonodárců.

75. Pro představu o možných alternativách Ústavní soud na tomto místě uvádí příklady geograficky i historicky nejbližších, tedy sousedních zemí. V Německu byla po kasačním zásahu Spolkového ústavního soudu [nález ze dne 2. 3. 2010, sp. zn. 1 BvR 256/08 (BVerfGE 125, 260-385)] přijata nová a do značné míry omezující právní úprava *data retention*. Nově lze vymezené kategorie provozních údajů uchovávat pouze po dobu deseti týdnů, lokalizační údaje jen čtyři týdny. Dále jsou stanoveny kategorie údajů, které nesmějí být uchovávány vůbec (vedle obsahu komunikace též např. údaje o navštívených webech a službách elektronické pošty); k tomu byl pro doplnění zaveden mechanismus „*data freeze*“ (shromažďování budoucích údajů telekomunikačního provozu konkrétní podezřelé osoby z podnětu orgánu činného v trestním řízení). Na Slovensku zákonodárce po zásahu tamního Ústavního soudu (nález ze dne 29. 4. 2015, sp. zn. PL. ÚS 10/2014) princip plošného uchovávání údajů opustil a namísto toho zavedl mechanismus „*data freeze*“, což je z časového hlediska obdoba odposlechu, neboť nezpřístupňuje údaje zpětně do minulosti. V Rakousku po zásahu Ústavního soudního dvora (viz nález ze dne 27. 6. 2014, sp. zn. G 47/2012 a další) nová právní úprava dosud přijata nebyla, neboť na řešení této otázky nepanuje

politická shoda. Pouze v Polsku lze v současné době nalézt právní úpravu volnější z hlediska ochrany soukromí jednotlivce a benevolentnější k ochraně bezpečnosti státu a jeho obyvatel; časové omezení pro uchovávání metadat není zákonem stanoveno a není vyžadován předchozí soudní souhlas, soudu se pouze v půlročním intervalu zasílají statistiky o získaných datech. Tato úprava je nyní (také již podruhé) předmětem přezkumu polského Ústavního tribunálu k návrhu ombudsmana.

76. Ústavní soud se nyní vrací k posouzení přípustnosti principu *data retention* jako takového a konstatuje, že zdráhal-li se explicitně vyslovit nepřiměřenost principu v roce 2011, tím spíše k takovému závěru nemůže dospět dnes. Od posledního rozhodování ve věci vývoj v oblasti informačních technologií značně pokročil, jednotlivci využívají služby elektronických komunikací stále častěji, údaje o telekomunikačním provozu jejich aktivním přičiněním vznikají, existují a jsou operátory (soukromými subjekty, s nimiž zákazníci uzavřeli soukromoprávní smlouvy) po určitou dobu uchovávány (zajištění poskytovaných služeb, jejich následné vyúčtování, reklamace apod.); většina zákazníků navíc uděluje souhlas se zpracováním svých údajů i nad rámec nutný pro poskytnutí poptávané služby (pro marketingové účely). Je tak nepopiratelnou skutečností, že údaje o elektronické komunikaci jednotlivce budou v nějaké podobě shromažďovány vždy, i bez právní úpravy *data retention* (tj. bez zákonné povinnosti je „zadržovat"), jinak by elektronickou komunikaci nebylo možné vůbec uskutečňovat.

77. Jinými slovy, provozní a lokalizační údaje o uskutečněné elektronické komunikaci nejsou uchovávány pouze z důvodu stanovené zákonné povinnosti, jsou a budou pro potřeby zajištění realizace těchto služeb, jejich vyúčtování a vyřizování případných reklamací uchovávány i bez zákonné povinnosti (ve více či méně totožném rozsahu, po více či méně totožnou dobu). Jak vyplynulo např. z výpovědi doc. Polčáka, absence legislativně zavedeného principu *data retention* v konkrétním členském státě neznamená, že by orgány veřejné moci s provozními a lokalizačními údaji nepracovaly, dostávají se k nim pouze jinými cestami – nelze přitom zaručit, že tyto alternativní cesty jsou z hlediska zásahu do práva na soukromí méně invazivní než postup podle právní úpravy využívající princip *data retention*.

78. Proto Ústavní soud logicky řešil, která z možností představuje „menší zlo", a dospěl k závěru, že z hlediska transparentnosti postupu orgánů veřejné moci, stejně jako kontroly nad zásahy do soukromí jednotlivce, je lepší jasně, přesně a dostatečně přísně vymezený zákonný rámec principu *data retention* (viz dále), než „legislativní stín", v němž by se jinak pohybovali jak operátoři při uchovávání provozních a lokalizačních údajů, tak orgány veřejné moci (zejména orgány činné v trestním řízení) ve snaze získat přístup k nim. Je mylná představa, že opuštění principu *data retention* eliminuje riziko zneužití vzniklých údajů.

79. Mohlo by se jevit, že svým současným postojem Ústavní soud jakožto ochránce ústavnosti paradoxně poskytuje soukromí jednotlivce nižší míru ochrany než Soudní dvůr Evropské unie, jehož primárním posláním není ochrana základních práv a který se staví s odkazem na ochranu soukromí k principu *data retention a priori* (obecně) negativně. Nicméně opak je pravdou – zejména právě s poukazem na požadavek předvídatelnosti, jasnosti a přísnosti právní úpravy zasahující do práva na soukromí. Ústavní soud svým přístupem chrání soukromí jednotlivce více, než kdyby svým zásahem vytvořil prostor k hledání jiných, alternativních a méně transparentních

cest, jak se k metadatům elektronické komunikace dostat. Výsledkem zavržení principu *data retention* by totiž nebyl stav, v němž by provozní a lokalizační údaje nevznikaly a nebyly uchovávány a využívány (minimálně ze strany orgánů činných v trestním řízení); důsledkem by byla naopak ztráta veřejnoprávních mezí a kontroly nad rozsahem uchovávání provozních a lokalizačních údajů, nad způsobem zabezpečení i jejich zpřístupňováním. Odpovědnost za nakládání s provozními a lokalizačními údaji ze strany orgánů veřejné moci by se pak *de facto* přenesla ze státu na operátory (soukromé osoby), což by byl v podmínkách právního státu nepřípustný stav.

80. Ústavní soud nemůže odhlédnout od výše naznačeného společenského a technologického vývoje, který od jeho posledního rozhodování ve věci nastal. Mezilidská komunikace stále více přesouvá své těžiště do prostředí telekomunikačních a elektronických služeb. Za současného stavu by proto bylo nemoudré bránit státu jako nositeli řady úkolů k naplnění daných veřejných zájmů (zde zejména bezpečnost státu, ochrana zdraví a majetku obyvatel), aby měl za vhodně nastavených podmínek přístup k údajům, jež mohou být cenným zdrojem důležitých informací. Princip *data retention* jako takový proto Ústavní soud bez dalšího nezavrhuje (stejně jako v nosných důvodech odůvodnění nálezu Pl. ÚS 24/10); stanovit operátorům povinnost shromažďování provozních dat v reálném čase ostatně zákonodárci ukládá závazek vyplývající z Úmluvy o počítačové kriminalitě, vyhlášené pod č. 104/2013 Sb. m. s.

81. Proti samotné existenci principu *data retention* navrhovatelka brojí mimo jiné tvrzením o ohrožení profesního tajemství (advokáti, sociální pracovníci, pracovníci telefonických poraden). Tomuto tvrzení by bylo možné přisvědčit za předpokladu, že by nebyl dostatečně definován účel, pro který je možné provozní a lokalizační údaje vyžádat, a nebyly by vhodně nastaveny podmínky přístupu k nim včetně záruk dotčených osob proti svévoli oprávněných orgánů (viz dále). V samotném zabezpečeném uchovávání údajů o elektronické komunikaci bez návaznosti na jejich zpřístupnění oprávněnému orgánu však nepřiměřený zásah do soukromí osob vázaných povinností mlčenlivosti spatřovat nelze. V případě žádosti o přístup k údajům o mlčenlivostí chráněné elektronické komunikaci – a nejen tehdy, ale v zásadě vždy – je na aplikujících orgánech (zejména soudech), aby podle konkrétních okolností případu rozhodly, zda převáží zájem na dosažení cíle sledovaného využitím provozních a lokalizačních údajů (pro naplnění konkrétního veřejného zájmu), a je tedy přiměřené údaje zpřístupnit, či převáží zájem na ochraně soukromí a tajnosti okolností uskutečněné komunikace a aby v takovém případě přístup k provozním a lokalizačním údajům odepřely.

82. Ústavní soud s ohledem na uvedené neshledal důvody pro vyhovění návrhu pouze z principiálního důvodu, že by plošný a neadresný sběr provozních a lokalizačních údajů o uskutečněné komunikaci byl ve vztahu k ochraně soukromí *a priori* nepřiměřený. Jestliže tedy v navazujícím testu proporcionality budou podmínky uchovávání provozních a lokalizačních údajů a přístupu k nim shledány dostatečně přísnými a vyvažujícími omezení práva na soukromí podle čl. 10 odst. 2 a 3 ve spojení s čl. 13 Listiny, neshledává Ústavní soud ani tehdy prostor pro to, aby návrhu vyhověl.

Podmínky uchovávání provozních a lokalizačních údajů

Účel uchovávání a zpřístupňování provozních a lokalizačních údajů

83. V prvním kroku testu proporcionality je třeba zkoumat, zda zákonná úprava sleduje legitimní cíl a zda je touto úpravou vzniklý zásah do základního práva způsobilý vytýčeného cíle dosáhnout. Účel úpravy *data retention* nelze dovodit ze samotného znění § 97 odst. 3 ZEK, ale až v kombinaci s § 88a odst. 1 trestního řádu a dalšími předpisy, na něž je odkazováno při stanovení pravomoci jednotlivých orgánů. Pro vymezení cíle napadené právní úpravy je tak nutno zároveň zohlednit, kdo má k uchovávaným údajům oprávněný přístup, neboť tato skutečnost je vázána k účelu, k jakému mohou příslušné orgány přístup žádat.

84. Cílem shromažďování provozních a lokalizačních údajů je podle důvodové zprávy jejich následné využití pro odhalování vybrané trestné činnosti (§ 88a odst. 1 trestního řádu), pátrání po osobách pohřešovaných či ztracených (§ 68 odst. 2 ZPol), pro boj s terorismem [§ 71 písm. a) ZPol], činnost zpravodajských služeb (získávání, shromažďování a vyhodnocování informací důležitých pro ochranu ústavního zřízení, významných ekonomických zájmů, bezpečnosti a obrany České republiky – viz § 2 zákona č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů) a pro dohled nad kapitálovým trhem (§ 8 zákona č. 15/1998 Sb., o dohledu v oblasti kapitálového trhu a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů).

85. Všechny uvedené cíle sledují silný veřejný zájem (ochrana bezpečnosti a zdraví obyvatel, ekonomických zájmů státu) a jako takové je lze označit za legitimní. Informace, které uvedené oprávněné orgány z vyžádaných provozních a lokalizačních údajů získávají, jsou nepochybně způsobilé posunout je v jejich činnosti vpřed a nasměrovat je o krok blíže k naplnění uvedeného účelu, ať už je jím (zjednodušeně a obrazně řečeno) objasnění trestné činnosti, nalezení ztraceného seniora či odvrácení teroristické hrozby.

86. Dále je nutno zabývat se otázkou potřebnosti, tj. nezbytnosti omezování práva na soukromí ve vztahu ke sledovanému cíli. Ústavní soud zkoumal, zda existují mírnější a méně invazivní prostředky, které jsou též schopny dosáhnout vytýčeného cíle, a dospěl k závěru, že využití provozních a lokalizačních údajů skutečný ekvivalent nemá – neexistují prostředky, s nimiž by bylo možné zkoumaný nástroj porovnávat. Byť Ústavní soud na více místech tohoto i dřívějších nálezů přirovnává využití provozních a lokalizačních údajů v trestním řízení z hlediska intenzity zásahu do soukromí jednotlivých osob k odposlechu, nejde o totéž. Zatímco nařízením odposlechu lze podezřelou osobu monitorovat do budoucna, provozní a lokalizační údaje umožňují oprávněným orgánům získat informace o skutku, který se již stal – k takovým informacím se oprávněné orgány jinak nedostanou. Stejně nepřiléhavé by bylo přirovnání ke sledování osob a věcí podle § 158d trestního řádu, neboť i zde oprávněný orgán získává maximálně informace o pohybu a komunikaci sledované osoby v reálném čase, nikoli však do minulosti. Z uvedených důvodů nelze za adekvátní a méně invazivní náhradu považovat ani výše zmíněný mechanismus tzv. „*data freeze*“ (bod 75), kterým některé státy (např. Slovensko) nahradily princip *data retention* zcela nebo jej podstatně omezily za současného doplnění mechanismu „*data freeze*“ (např. Německo) – i zde totiž oprávněný orgán získává přístup pouze k údajům následujícím po vydání příslušného příkazu, nikoli k údajům minulým. Jelikož tedy neexistuje prostředek, který by umožňoval získání stejných poznatků, jaké lze vyčíst z provozních a lokalizačních údajů, není možné u druhého kroku testu proporcionality skončit, neboť i ten napadená právní úprava splňuje.

87. Ústavní soud proto přesunul těžiště své pozornosti k poslednímu kroku testu proporcionality, kterým je poměřování – proporcionalita omezení základního práva na soukromí ve prospěch sledovaných cílů, naplňujících veřejný zájem, v užším slova smyslu. Je třeba zodpovědět, zda je dotčený veřejný zájem natolik důležitý, aby ospravedlnil rozsah omezení práva na soukromí sledováním elektronické komunikace téměř celé české populace po dobu šesti měsíců „do zásoby", komerčními subjekty, zda nemohla napadená právní úprava omezit zásah do práva na soukromí více, tedy zda je zákonné nastavení podmínek dostačující, a zda poskytuje dostatek záruk proti zneužití tohoto významného nástroje, aby omezení vyvážila.

88. Ústavní soud se zaměřil na dílčí problémy, které ve svém souhrnu mají vliv na posouzení přiměřenosti napadené úpravy v užším smyslu. Je především třeba zabývat se zákonnou dobou, po kterou se povinné údaje uchovávají. Dále je třeba vyřešit, zda není příliš široce nastaven okruh orgánů oprávněných k přístupu k zadržovaným údajům (ve vazbě na cíl a podmínky, za nichž údaje mohou získat). A konečně je důležité, zda jsou jednotlivci poskytnuty dostatečné prostředky ochrany před zneužitím uchovaných údajů (jak z hlediska zabezpečení uchovaných údajů a neoprávněného přístupu k nim, tak i nástrojů procesní obrany jednotlivce v případě podezření, že jeho údaje skutečně byly zneužity).

Doba uchovávání provozních a lokalizačních údajů

89. Ve vztahu k době šesti měsíců, po kterou jsou provozní a lokalizační údaje podle § 97 odst. 3 ZEK uchovávány, vyšel Ústavní soud z toho, že její délka představuje nejmírnější variantu z možností stanovených směrnicí o *data retention*, která byla v době přijetí napadené právní úpravy ještě platná. Je nicméně nutno se ptát, zda je šestiměsíční doba v dnešních podmínkách přiměřená. Z výslechu informované osoby z řad operátorů bylo zjištěno, že maximální doba, po kterou operátor potřebuje předmětná metadata uchovávat pro vlastní potřeby, nepřekračuje dva měsíce. Zároveň však operátor vybrané údaje (v rozsahu nikoli totožném s rozsahem stanoveným zákonem) uchovává pro marketingové účely i po dobu šesti měsíců na základě souhlasu uděleného zákazníkem. V uvedeném režimu souhlasu uchovává např. společnost T-Mobile Czech Republic a. s. v současné době údaje cca 70 % zákazníků.

90. Na tomto místě je třeba zejména v souvislosti s vyšetřováním trestné činnosti odlišit, že údaje jsou vyžadovány v zásadě dvojím způsobem. Buď má oprávněný orgán k dispozici údaje ke konkrétnímu uživateli (číslo jeho mobilní linky, pevné linky, IP adresu, IMEI, apod.) a v takovém případě se zajímá o výpis hlasových nebo datových služeb – kontakty, činnost, případně pohyb uživatele (jeho telefonu, počítače apod.), nebo tyto údaje nezná, disponuje ale informacemi, kde se zájmový uživatel pohyboval, případně kde byl spáchán trestný čin. V druhém případě se oprávněný orgán zajímá zejména o údaje z jednotlivých stanic BTS (buněk), které určí například, jaké mobilní telefony se v danou chvíli k dané buňce připojovaly.

91. Z výpovědi plk. Ing. Šibora při veřejném ústním jednání Ústavní soud zjistil, že většina dotazů se týká právě výpisů BTS stanic, které nebývají starší několika dní; starší dotazy na tento druh výpisu není ani technicky možný. Dále z výpovědi plk. Ing. Bc. Mareše vyplynulo, že v případě výpisů hlasových či datových služeb konkrétního uživatele orgán činný v trestním řízení využívá zpravidla maximální možný

rozsah šesti měsíců. Na informace získané z jednoho výpisu o telekomunikačním provozu se často nabalují další poznatky, umožňující například odhalení sítě pachatelů či organizované skupiny. Nelze proto bez přihlédnutí ke konkrétním skutkovým okolnostem vyšetřovaného případu přijmout zobecňující závěr, nakolik jsou pro orgány činné v trestním řízení informace získané za celé období šesti měsíců pro naplnění sledovaného účelu potřebné či užitečné – lze jen konstatovat, že oprávněné orgány v případě znalosti identifikačních údajů konkrétního uživatele využívají maximální dobu, kterou jim zákon umožňuje. Jelikož však četnost dotazů na základnové stanice oproti výpisům konkrétních účastnických čísel či mobilních zařízení mnohonásobně převažuje, platí z pohledu celkového součtu všech dotazů závěr, že většina vyžadovaných údajů není starší než tři měsíce (viz také výpověď Mgr. Kellerové).

92. Přestože se provozní a lokalizační údaje starší tří měsíců využívají pouze v omezené míře, nelze podle Ústavního soudu učinit závěr, že by starší metadata v konkrétních případech (zejména při aplikaci § 88a trestního řádu) nebyla potřebná a užitečná, a tedy nepřiměřená sledovanému cíli. Zákonodárce v reakci na nález sp. zn. Pl. ÚS 24/10 zvolil šestiměsíční „retenční dobu“ jako nejkratší možnou podle tehdy ještě platné směrnice o *data retention*. Nepřijal-li Ústavní soud závěr, že by princip *data retention* byl protiústavní sám o sobě, a nebylo-li v řízení před Ústavním soudem prokázáno, že by uchované údaje nebyly využívány nebo naopak byly nadužívány, tj. nebylo šetřeno právo na soukromí ze strany oprávněných orgánů, nelze dospět k závěru o nepřiměřenosti takto nastavené retenční doby. Nikdy neexistuje jediné správné řešení, jak určitou oblast společenských vztahů právně regulovat. Jistě si lze z hlediska minimalizace zásahu do soukromí účastníků telekomunikačního provozu představit úpravu přísnější, např. – jak vypověděl doc. Polčák – rozlišit a odstupňovat přístup k provozním a lokalizačním údajům podle cíle, jehož naplnění oprávněný orgán sleduje, a od toho odvozené reálné potřeby získání právě tak starých údajů (srov. právní úpravu Belgie, Německa). 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.

Zabezpečení uchovávaných provozních a lokalizačních údajů

93. Na právní úpravu šetřící právo na soukromí v maximální míře je dále třeba klást požadavek stanovení jasných a detailních pravidel při zabezpečení uchovávání údajů a záruk proti jejich zneužití (neoprávněný či svévolný přístup k nim). Zejména v případě *data retention* jsou kvanta údajů o všech uživatelích elektronické komunikace soustřeďována u soukromých subjektů, a proto musí být zákonodárce přísný dvojnásob. Je třeba jasně stanovit, že provozní a lokalizační údaje musí být uchovávány bezpečně a nesmí bez výslovného souhlasu klientů ve smyslu platné úpravy ochrany osobních údajů sloužit marketingovým účelům povinných subjektů. Dynamický vývoj oblasti informačních technologií však zároveň způsobuje, že zákonodárce bude vždy o několik kroků pozadu; proto může být dokonce ku prospěchu věci, je-li zabezpečení údajů na zákonné úrovni formulováno obecněji a jsou-li technické detaily ponechány prováděcímu předpisu, který na změny praxe může reagovat pružněji a operativněji.

94. Zabezpečení uchovávaných údajů obsahují §§ 87 a násl. ZEK (jež představují implementaci e-privacy směrnice) spolu s obecnými předpisy ochrany osobních údajů –

GDPR (s výhradou čl. 95, vymezujícího vztah nařízení a e-privacy směrnice) a transpozičním zákonem č. 110/2019 Sb., o zpracování osobních údajů. Přestože uvedená pasáž ZEK upravující zabezpečení údajů nebyla napadena, Ústavní soud nemůže na hodnocení tohoto aspektu rezignovat, neboť způsob zabezpečení uchovaných (poskytnutých) provozních a lokalizačních údajů s přezkumem přiměřenosti principu *data retention*, a tedy i ústavnosti napadených § 97 odst. 3 a 4 ZEK, úzce souvisí.

95. V obecné rovině lze konstatovat, že úroveň zabezpečení provozních a lokalizačních údajů není nižší než úroveň zabezpečení jiných údajů, jež jsou v režimu ZEK zpracovávány – viz § 88a ZEK (doplněný stejně jako napadená ustanovení zákonem č. 273/2012 Sb. v reakci na nález sp. zn. Pl. ÚS 24/10), v jehož důsledku jsou provozní a lokalizační údaje z bezpečnostního hlediska explicitně řazeny na úroveň osobních údajů. Zákon ukládá operátorům povinnost zabezpečení uchovávaných provozních a lokalizačních údajů a upravuje i mechanismus přezkumu a kontroly dodržování stanovených povinností ze strany nezávislých institucí. Konkrétně je operátor jako zpracovatel údajů povinen: zajistit technicky a organizačně bezpečnost poskytované služby a zpracovat pro zajištění ochrany údajů a důvěrnosti komunikací (včetně důvěrnosti s komunikací spojených provozních a lokalizačních údajů) vnitřní technickoorganizační předpis [§ 88 odst. 1 písm. b) ve spojení s § 89 ZEK]; informovat účastníky komunikace o riziku porušení bezpečnosti služeb, ochrany osobních údajů a důvěrnosti komunikací [§ 88 odst. 1 písm. c) ZEK]; vytvořit vnitřní postupy pro vyřizování žádostí uživatelů o přístup k jejich osobním údajům [§ 88 odst. 1 písm. d) ZEK]; informovat Úřad pro ochranu osobních údajů o případech porušení ochrany osobních údajů včetně způsobu řešení a vést evidenci takových případů (§ 88 odst. 4-7 ZEK); nezpracovávat provozní a lokalizační údaje pro marketingové účely bez souhlasu dotčené osoby (§ 90 odst. 6 ZEK); omezit na nezbytné minimum jak rozsah uchovávaných údajů, tak i okruh osob (pověřených zaměstnanců) oprávněných k přístupu k uchovávaným údajům a jejich dalšímu zpracování (§ 90 odst. 9 a § 91 odst. 4 ZEK); zachovávat mlčenlivost o vyžádání a poskytnutí údajů podle § 97 odst. 3 ZEK (§ 97 odst. 8 ZEK); vést evidenci případů zpřístupnění provozních a lokalizačních údajů a pravidelně ji „reportovat“ Českému telekomunikačnímu úřadu (§ 97 odst. 10 a 11 ZEK).

96. Porušení kterékoli z výše uvedených povinností ze strany operátora je přestupkem [viz zejména § 118 odst. 12 písm. a), d) a odst. 14 písm. b)-h), k), z), aa), ae) a odst. 15 ZEK], za jehož spáchání hrozí v některých případech pokuta až 50 000 000 Kč nebo do výše 10 % z čistého obratu [§ 118 odst. 23 písm. c) ZEK], což je nepřísnější kategorie sankcí v režimu přestupků podle ZEK. K projednávání přestupků podle tohoto zákona je příslušný Český telekomunikační úřad, který má ve vztahu k operátorům i řadu dalších dozorových oprávnění. Dodržování obecných předpisů ochrany osobních údajů při jejich zpracování ze strany operátorů pak i v oblasti *data retention* podléhá zároveň dohledu Úřadu pro ochranu osobních údajů (§ 87 odst. 3, § 88 odst. 4-7 ZEK).

97. Jak je zřejmé z uvedeného výčtu, v právním řádu se podle Ústavního soudu nachází řada záruk proti zneužití uchovaných údajů, úroveň zabezpečení shromažďovaných údajů je dostačující; uvedený aspekt zkoumané problematiky tak neústavní nepřiměřenost napadené právní úpravy *data retention* (zejména § 97 odst. 3 a 4 ZEK a vyhlášky) nezakládá. Bez významu v tomto ohledu nezůstávají ani podmínky

přístupu oprávněných orgánů k vyžádaným údajům (viz dále) a skutečnost, že oprávněné orgány nedisponují žádnou databází údajů, v níž by mohly libovolně vyhledávat.

Podmínky přístupu k provozním a lokalizačním údajům

98. Ustanovení § 97 odst. 3 ZEK obsahuje taxativní výčet orgánů oprávněných k přístupu k provozním a lokalizačním údajům. Ve spojení se zvláštními předpisy, jimiž se činnost oprávněných orgánů řídí, je stanoven vždy rovněž účel, k jakému orgány mohou provozní a lokalizační údaje žádat. Bližší podmínky, za nichž oprávněné orgány mohou přístup získat, jsou dále upraveny těmito zvláštními předpisy, z nichž některé byly projednávaným návrhem napadeny, jiné nikoli. Ústavní soud zkoumal přiměřenost zásahu do práva na soukromí jen aplikací napadené právní úpravy.

Využití provozních a lokalizačních údajů v trestním řízení

99. Podle § 97 odst. 3 ZEK ve spojení s § 88a odst. 1 trestního řádu mohou orgány činné v trestním řízení žádat provozní a lokalizační údaje v souvislosti se stíháním trestných činů sankcionovatelných trestem odnětí svobody s horní hranicí trestní sazby nejméně tři roky, a dalších konkrétně vyjmenovaných trestných činů, u nichž hrozí trest mírnější (primárně souvisejících s „počítačovou kriminalitou“).

100. Ústavní soud již v nálezu sp. zn. Pl. ÚS 24/10 ve vztahu k přiměřenosti omezení základního práva v kontextu *data retention* vyslovil, že „*je nezbytné, aby s ohledem na závažnost a míru zásahu do základního práva jednotlivců na soukromí v podobě práva na informační sebeurčení (ve smyslu čl. 10 odst. 3 a čl. 13 Listiny), jež použití uchovávaných údajů představuje, zákonodárce omezil možnost použití uchovávaných údajů jen pro účely trestních řízení vedených pro zvlášť závažné trestné činy a jen pro případ, že nelze sledovaného účelu dosáhnout jinak*“ (podobně k tomu viz také SDEU v citovaném rozsudku *Digital Rights Ireland*). V porovnání s institutem odposlechu dále Ústavní soud zákonodárci vytýkal neodůvodněné odchýlení, rozporné s jeho judikaturou. V nálezu sp. zn. Pl. ÚS 24/11 k tomu dále uvedl: *„Jinými slovy, tomuto veřejnému zájmu [na předcházení a postihování trestných činů] nelze ani za splnění výše uvedené podmínky potřebnosti přiznat přednost v předmětné kolizi pokaždé. Je naopak třeba vždy zvažovat, zda vzhledem k významu objektu určitého trestného činu, jenž měl být spáchán, převáží zájem na jeho stíhání nad právem jednotlivce rozhodovat sám o tom, zda a komu zpřístupní svá osobní data. Je věcí zákonodárce, aby určil, v případě kterých trestných činů tento veřejný zájem převažuje, přičemž ve svém rozhodnutí musí, obdobně jako např. v případě stanovení výše trestních sazeb, zohlednit jejich závažnost. Zbývá dodat, že ze stejných zásad vychází i omezení možnosti vydat příkaz k odposlechu a záznamu telekomunikačního provozu podle § 88 odst. 1 trestního řádu pouze na trestní řízení pro zvlášť závažný zločin nebo pro jiný úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva…“*

101. V tomto ohledu lze zaznamenat pozitivní posun. Nynější právní úprava již nepracuje s neurčitým pojmem *„objasňování trestné činnosti“*, nýbrž nabízí konkrétní výčet trestných činů. Ke zvolené kategorizaci vedlejší účastnice jako předkladatelka návrhu zákona č. 273/2012 Sb., kterým byla napadená právní úprava do právního řádu vnesena, uvádí: „*Pokud jde o kategorii úmyslných trestných činů, za něž zákon stanoví*

trest odnětí svobody s horní hranicí trestní sazby nejméně tři roky, vychází se analogicky z právní úpravy institutu vazby, tj. závažnost činu je odvozena od možnosti vzetí osoby do vazby. Jestliže se pro trestné činy s uvedenou trestní sazbou umožňuje vzetí osoby do vazby, což je nejinvazivnější prostředek trestního práva vedoucí ke zbavení její osobní svobody, pak je namístě, aby u takové kategorie trestných činů bylo možné získávat provozní a lokalizační údaje podle § 88a trestního řádu.“

102. Ústavní soud trvá na tom, že povinnost uchovávání a poskytování provozních a lokalizačních údajů je nutné vnímat jako zásah svou intenzitou srovnatelný s nařízením odposlechu a je k němu tak třeba i přistupovat. Uvedenou optikou by tak neměl být za přiměřené omezení práva na soukromí vnímán plošný sběr provozních a lokalizačních údajů „do zásoby“ a využití těchto údajů pro cca 90 % skutkových podstat trestných činů, na něž se ve skutečnosti § 88a odst. 1 trestního řádu vztahuje. V řízení před Ústavním soudem bylo nicméně zjištěno, že dřívější způsoby páchání (a tedy i objasňování) trestné činnosti bez využití služeb elektronických komunikací si dnes lze jen stěží představit. Vznikají-li stále nové formy páchání trestné činnosti a služby elektronických komunikací jsou k tomu využívány stále více, nepřikládá Ústavní soud váhu statistikám objasněnosti trestné činnosti z let 2010-2014, předkládaným navrhovatelkou již jen z tohoto důvodu – uvedené roky nelze s rokem 2019 z hlediska forem kriminality a vyšetřovacích metod využívaných k jejímu odhalení srovnávat (viz výpověď JUDr. Bradáčové). Předkládané statistiky však nemají vypovídací hodnotu ani z dalšího důvodu: V jejich případě jde pouze o informaci, kolik případů vyšetřované trestné činnosti bylo v daném roce ukončeno, tedy objasněno; na uvedenou skutečnost má přitom vliv celá řada faktorů a jasnou korelaci mezi dostupností či nedostupností provozních a lokalizačních údajů, zvolenými vyšetřovacími metodami a jejich úspěšností, z nich podle Ústavního soudu průkazně vyvodit nelze. Nelze proto ani učinit závěr, zda se orgány činné v trestním řízení bez využití provozních a lokalizačních údajů (na základě principu *data retention*) dokáží obejít či nikoli.

103. Stejně tak jsou neprůkazné i statistiky vykazující počet uskutečněných žádostí o výpisy telekomunikačního provozu, které uvádí navrhovatelka na podporu tvrzení o nadužívání provozních a lokalizačních údajů v trestním řízení. Rozdíl mezi výstupy statistik, zpracovávaných nezávisle na sobě Českým telekomunikačním úřadem a policií s rozdílnými výstupy, lze vysvětlit odlišnou metodikou, jak ve svém vyjádření vysvětlila vedlejší účastnice. Zatímco ČTÚ zaznamenává každý uskutečněný dotaz na každého operátora, policie uvádí počet žádostí podle počtu případů, pro něž byly uskutečněny. Podle potřeby přitom policie v jednom případě musí uskutečnit hned několik dotazů, jednak z hlediska časového (např. výpis BTS stanice pokrývající období 12 hodin vyžaduje čtyři dotazy), jednak z hlediska adresáta dotazu (nelze předem odhadnout, který operátor drží pro policii relevantní data), jak vyplynulo zejména z výpovědi JUDr. Bradáčové a plk. Šibora. Nadužívání provozních a lokalizačních údajů orgány činnými v trestním řízení v řízení před Ústavním soudem nebylo prokázáno.

104. Z výpovědí informovaných osob opakovaně vyplynulo, že absence principu *data retention* neznamená, že by provozní a lokalizační údaje nebyly při vyšetřování trestné činnosti využívány. Orgány činné v trestním řízení při jeho absenci pouze volí jiné dostupné prostředky, což vede Ústavní soud k závěru, že důsledkem chybějící úpravy *data retention* je jednak menší transparentnost postupu vyšetřujících orgánů, a dále paradoxně vyšší riziko zneužití údajů, jež má operátor o uskutečněném

telekomunikačním provozu k dispozici. Je nutno zdůraznit, že veškeré vyšetřovací metody trestního řízení z povahy věci představují (větší či menší) zásah do soukromí vyšetřovaných osob; zůstává proto otázkou, zda i při absenci principu *data retention* jsou skutečně šetřena základní práva jednotlivce, volí-li vyšetřující orgány alternativní metody. Jinými slovy, nelze zaručit, že soukromí jednotlivce je více šetřeno tím, že zákonodárce nepřijal princip *data retention*, neboť je možné, že v případě nedostupnosti provozních a lokalizačních údajů zvolí vyšetřující orgán z hlediska ochrany soukromí invazivnější vyšetřovací metody (vždy nějakou zákonnou cestu k obstarání potřebných údajů najde).

105. Neobstojí ani argument navrhovatelky, že využití provozních a lokalizačních údajů je neefektivní nástroj, protože pachatelé trestné činnosti jsou si vědomi svého jednání a dokáží se elektronickým stopám vyhnout. Vyšetřování trestné činnosti a vztah mezi vyšetřovateli a pachateli je charakteristický tím, že vyšetřovatelé by měli být pokud možno krok před pachateli a jejich metodami, aby mohli trestnou činnost účinně odhalovat, což platí beze zbytku pro všechny vyšetřovací metody a neexistuje snad žádná, kterou by se pachatelé nepokoušeli obcházet. To však není argument pro zavržení konkrétní vyšetřovací metody jako neefektivní či neúčinné (bez dalšího).

106. Soudní dvůr Evropské unie považuje za legitimní cíl využití provozních a lokalizačních údajů v souvislosti s odhalováním trestné činnosti pouze vyšetřování „závažné trestné činnosti“ – tento pojem nicméně nedefinuje a ponechává členským státům prostor pro uvážení (v kontextu *data retention* příkladmo uvádí organizovaný zločin a terorismus). Přestože pojetí závažné trestné činnosti obsažené v napadeném ustanovení § 88a odst. 1 trestního řádu je široké, s ohledem na výsledky dokazování je Ústavní soud shledává přiměřeným. V řízení nebylo prokázáno, že by využití provozních a lokalizačních údajů jako vyšetřovací metoda bylo zbytečné, či že by bylo nadužíváno. Z výpovědi JUDr. Bradáčové vyplynulo, že z ročního nápadu trestních věcí se žádosti o záznam telekomunikačního provozu týkají 3 % případů, což nepřímo potvrdil ve své výpovědi také JUDr. Sokol z Unie obhájců. S ohledem na společenský i technologický vývoj je zároveň stále více trestné činnosti (a to nejen kybernetické) pácháno prostřednictvím nebo za přispění služeb elektronické komunikace – kde dříve vyšetřovatelé nacházeli stopy „v blátě“, nacházejí nyní zejména stopy elektronické. Rozsah stanovený napadeným § 88a trestního řádu proto z pohledu Ústavního soudu lze odůvodnit potřebou rychlého a efektivního odhalování a objasňování v něm uvedené trestné činnosti. V případě zařazení taxativního výčtu trestných činů páchaných v převážné míře ve virtuálním prostředí elektronických zařízení je zřejmé, že bez přístupu k provozním a lokalizačním údajům by tento druh kriminality (kyberkriminality) byl prakticky nepostižitelný a stát, jehož úkolem je zajištění bezpečnosti a stíhání trestné činnosti, by se v tomto ohledu stal „bezzubým“.

107. Napadenou úpravu lze považovat za přiměřenou i z pohledu procesních záruk proti případnému zneužití této pravomoci orgánů činných v trestním řízení. Ustanovení § 88a odst. 1 výslovně žádá, aby jeho aplikace bylo využito pouze v případě, *„nelze-li sledovaného účelu dosáhnout jinak, nebo bylo-li by jinak jeho dosažení podstatně ztížené“*, čímž je dodržen požadavek minimalizace zásahu do základního práva. K vyžádání provozních a lokalizačních údajů je třeba souhlasu soudu (v přípravném řízení k návrhu státního zástupce) a soudní příkaz je podle citovaného ustanovení třeba i řádně odůvodnit. Dotčený jednotlivec má tedy záruku, že oprávněnost vyžádání jeho telekomunikačních údajů bude posouzena nezávislým

soudním orgánem a v případě neodůvodněnosti žádosti nebude vyhověno. Podobnou záruku považují ve shodě s Ústavním soudem ve své rozhodovací činnosti za stěžejní také SDEU i ESLP (viz výše rozhodnutí citovaná v bodech 57-62).

108. Aby mohly být záruky proti zneužití uchovaných údajů efektivní, musí existovat nástroje zpětné kontroly oprávněnosti získaného přístupu ke konkrétním provozním a lokalizačním údajům. Dalším opatřením vyvažujícím intenzitu zásahu do soukromí jednotlivce ve prospěch sledovaného veřejného zájmu je proto v § 88a odst. 2 trestního řádu (s výjimkami odůvodněných případů stanovených v odst. 3 téhož ustanovení) upravená povinnost oprávněného orgánu informovat dotčeného jednotlivce o získání jeho provozních a lokalizačních údajů. Se získanou informací se pak jednotlivec může obrátit na Nejvyšší soud, který přezkoumá soulad postupu orgánů činných v trestním řízení se zákonem; jednotlivec je tak vůči případné svévoli orgánu veřejné moci nadán účinným prostředkem obrany. V řízení před Ústavním soudem nebylo v tomto ohledu prokázáno žádné systémové selhání.

109. Ústavní soud v této části přezkumu s ohledem na uvedené uzavírá, že úprava obsažená v § 88a trestního řádu je z hlediska proporcionality zásahu do práva na soukromí osoby, jejíž údaje si orgán činný v trestním řízení vyžádá, přijatelné ve všech ohledech – co do rozsahu trestné činnosti, přísnosti podmínek přístupu k požadovaným údajům i co do procesních záruk, které má dotčená osoba na svou obranu k dispozici.

Využití provozních a lokalizačních údajů v režimu zákona o policii

110. Napadená ustanovení ZPol jsou součástí právního řádu od počátku jeho účinnosti, tedy od 1. 1. 2009, a dosud předmětem přezkumu Ústavního soudu (na rozdíl od ostatních napadených ustanovení) nebyla. Provozní a lokalizační údaje v režimu zákona o policii lze za stávající (napadené) právní úpravy využít v případě pátrání po konkrétní hledané nebo pohřešované osobě a za účelem zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly (§ 68 odst. 2 ZPol), nebo v souvislosti s bojem proti terorismu [§ 71 písm. a) ZPol]. Rozsah uvedených oprávnění co do účelu hodnotí Ústavní soud jako odpovídající sledovanému cíli. Zákon nicméně nestanoví nad přístupem policie k uchovávaným údajům kontrolu nezávislého orgánu (soudu), jak v obecné rovině pro využití provozních a lokalizačních údajů vyžaduje Ústavní soud, ale i SDEU a ESLP, což by mohlo evokovat, že záruky proti zneužití a možnost jednotlivce bránit se případné svévoli nejsou z hlediska proporcionality řešeny uspokojivě a zásah do práva na soukromí tak není dostatečně vyvážen. Je však třeba si uvědomit, že Ústavní soud měl dosud příležitost vyjádřit se k přiměřenosti právní úpravy přístupu k uchovávaným provozním a lokalizačním údajům pouze v kontextu trestního řízení, jemuž také přizpůsoboval svoji argumentaci; východiska režimu zákona o policii jsou však jiná než u vyšetřování trestné činnosti.

111. Policie je při výkonu své činnosti jednak vázána zákonem o policii (v daném kontextu jsou zásadní zejména § 2 a § 11 ZPol), dále se ve vztahu k projednávané problematice řídí interními akty řízení [zde zejména závazný pokyn policejního prezidenta č. 215/2008, kterým se stanoví některé bližší podmínky a postupy pro zpracování osobních údajů (o ochraně osobních údajů), závazný pokyn policejního prezidenta č. 109/2009, o operačních střediscích, závazný pokyn policejního prezidenta č. 186/2011, o vyžadování odposlechu a záznamu telekomunikačního provozu a údajů

o uskutečněném telekomunikačním provozu, závazný pokyn policejního prezidenta č. 222/2011, kterým se vydává spisový řád Policie České republiky, závazný pokyn policejního prezidenta č. 66/2014, o informačním systému ETŘ (evidence trestního řízení), a závazný pokyn policejního prezidenta č. 53/2015, o pátrání].

112. Pátrání po osobách je organizovaná činnost policie prováděná s využitím pátracích prostředků; pátrání je formalizovaný proces, který nelze zahájit bez konkrétního podnětu. Aby bylo možné lokalizační údaje v režimu „pátracího" ustanovení § 68 ZPol vyžádat neoprávněně, bylo by nejprve nutné neoprávněně zahájit pátrání po konkrétní osobě. Tento postup však má konkrétní hierarchická pravidla, stanovená výše citovanými interními akty řízení, a podléhá vnitřní kontrolní činnosti. Lokalizační údaje lze u operátora vyžádat pouze za účelem pátrání po konkrétní hledané nebo pohřešované osobě (zákonem definované pojmy – viz dále) a za účelem zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly, pouze prostřednictvím Útvaru zvláštních činností či Operačního střediska Policejního prezidia na základě žádosti schvalované přímým nadřízeným a vedoucím příslušného útvaru. Při zahájení pátrání se vytváří elektronický spis, v němž je žádost o výpis lokalizačních údajů založena. Veškerý postup je dokumentován a je zpětně verifikovatelný – přezkoumatelný (s možností vyvodit důsledky v případě podezření ze zneužití vyžádaných údajů). V praxi tak nemůže nastat situace, v níž by se jednomu konkrétnímu policistovi bez přičinění dalších osob podařilo svévolně lokalizační údaje zájmové osoby získat. V řízení před Ústavním soudem nebylo v tomto ohledu prokázáno žádné systémové selhání (viz výpověď plk. Habady).

113. Podle § 111 písm. c) ZPol se hledanou osobou ve smyslu zákona o policii rozumí fyzická osoba, u které je dán některý ze zákonných důvodů omezení její osobní svobody, místo jejího pobytu není známo a policii bylo po ní vyhlášeno pátrání; podmínky musí být splněny kumulativně, aby mohla být konkrétní osoba označena za hledanou a mohly tak být aktivovány související postupy podle zákona o policii. Obecně lze konstatovat, že hledaná osoba se z nějakého důvodu vyhýbá plnění svých povinností, stanovených zákonem či soudním rozhodnutím (podle vyjádření vedlejší účastnice jde nejčastěji o odsouzené osoby, které nenastoupily výkon trestu odnětí svobody).

114. Pohřešovanou osobou se pak podle písm. d) téhož ustanovení rozumí fyzická osoba, o níž se lze důvodně domnívat, že je ohrožen její život nebo zdraví, místo jejího pobytu není známo a policii po ní bylo vyhlášeno pátrání. U pohřešované osoby se předpokládá, že je určitým způsobem ohrožena a její situace je naléhavá. Úkony policie jsou činěny v řádu hodin (minut) a zpravidla ve prospěch dotčené osoby (či k dosažení jiného legitimního zájmu, např. vypátrání dítěte, s nímž se jeden z rodičů skrývá). Ústavní soud zejména po provedeném dokazování přisvědčil argumentaci vedlejší účastnice, konkrétně obavám z následků časového prodlení v případě, že by bylo nutné soudní souhlas obstarat. Také Soudní dvůr Evropské unie v rozsudku *Tele 2 Sverige AB* uvádí, že jím jmenované záruky přístupu k údajům prostého libovůle (řádné odůvodnění žádosti a přezkum nezávislého orgánu) jsou vyžadovány s výjimkou naléhavých případů (bod 120).

115. Dalším prvkem vyvažujícím zásah do soukromí je v trestním řízení povinnost dodatečně vyrozumět dotčené osoby, že jejich údaje byly poskytnuty (viz § 88a odst. 2 trestního řádu). Je však nutno přisvědčit argumentaci, podle které by

stanovení uvedené povinnosti v intencích § 68 odst. 2 ZPol působilo absurdně, neboť hledaná a nalezená osoba se o zpracování svých údajů policií dozví právě tím, že je policií nalezena. V režimu § 68 ZPol lze navíc žádat a získat pouze lokalizační údaje vztahující se ke zjištění doby a místa pobytu osoby, po níž se pátrá (§ 68 odst. 4 ZPol). Rozsah údajů, k nimž může mít policie podle tohoto ustanovení přístup, je tak v porovnání s režimem § 88a trestního řádu zákonem výrazně omezen, a to pouze na nezbytnou míru.

116. Záruky jednotlivce před zneužitím pravomoci podle § 68 odst. 2 ZPol tak představuje jednak vnitřní kontrolní činnost a sankce plynoucí případnému pachateli protiprávního jednání buď v rovině služebního poměru nebo v rovině trestněprávní, jednak má jednotlivec i možnost bránit se proti neoprávněně zahájenému pátrání (a tedy neoprávněnému vyžádání lokalizačních údajů) žalobou na ochranu před nezákonným zásahem ve správním soudnictví (§ 82 a násl. zákona č. 150/2002 Sb., soudní řád správní, ve znění pozdějších předpisů), nebylo-li pátrání zahájeno v intencích trestního řízení.

117. Ani v případech odvracení akutní teroristické hrozby zákon [konkrétně napadené ustanovení § 71 písm. a) ZPol] nevyžaduje zákon k přístupu oprávněného orgánu předchozí souhlas soudu ani jeho následnou kontrolu. V důvodové zprávě je uvedeno, že se získávání poznatků podle § 71 písm. a) ZPol blíží činnosti zpravodajských služeb a příslušným k uvedené činnosti bude pouze útvar zabývající se předcházením a odhalováním terorismu. Absenci soudního dohledu lze v tomto výjimečném případě odůvodnit jednak časovou naléhavostí, jež může příslušný policejní orgán při aplikaci uvedeného ustanovení svazovat, jednak utajenou povahou činnosti tohoto útvaru. Ústavní soud proto neshledává intenzitu zásahu do soukromí, odůvodňující jeho derogační výrok, ani zde. Chybějící povinnost informovat dotčenou osobu o přístupu k jejím provozním a lokalizačním údajům lze s ohledem citlivost a závažnost činnosti, kterou policejní orgány při odhalování teroristických hrozeb vykonávají, aprobovat též (podobně jako u činnosti zpravodajských služeb či v trestním řízení za splnění podmínek podle § 88a odst. 3 trestního řádu).

Další využití provozních a lokalizačních údajů

118. Dalšími oprávněnými orgány, jež § 97 odst. 3 ZEK jmenuje, jsou Bezpečnostní informační služba, Vojenské zpravodajství a Česká národní banka. Jelikož nebyla napadena zvláštní právní úprava, na kterou § 97 odst. 3 ZEK odkazuje a která s přezkumem otázky přiměřenosti tohoto oprávnění a podmínek, za nichž uvedené orgány mohou přístup k provozním a lokalizačním údajům získat, úzce souvisí (§ 6-10 zákona č. 154/1994 Sb., o Bezpečnostní informační službě; § 7-10 zákona č. 289/2005 Sb., o Vojenském zpravodajství; § 8 zákona č. 15/1998 Sb., o dohledu v oblasti kapitálového trhu a o změně a doplnění dalších zákonů), Ústavnímu soudu na tomto místě nepřísluší přiměřenost úpravy ve vztahu k uvedeným orgánům veřejné moci hodnotit.

119. V obecné rovině lze konstatovat, že je-li cíl, který je propůjčením tohoto oprávnění sledován, legitimní (viz výše body 81-83), jsou-li zvláštní právní úpravou nastavené podmínky přístupu k provozním a lokalizačním údajům, jakož i záruky účinné ochrany jednotlivce, dostatečně přísné a budou-li se nést v duchu závěrů tohoto

nálezu, pak není co vytknout samotné skutečnosti, že § 97 odst. 3 ZEK uvádí mezi oprávněnými orgány mimo jiné i orgány v předchozím odstavci uvedené.

Prováděcí předpis

120. K provedení všech výše popsaných zákonných mechanismů uchovávání a zpřístupňování provozních a lokalizačních údajů byla Ministerstvem průmyslu a obchodu přijata vyhláška, která je navrhovatelkou rovněž napadena. Předchozí prováděcí předpis byl nálezem sp. zn. Pl. ÚS 24/10 zrušen primárně proto, že byla zrušena zákonná úprava, k jejímuž provedení sloužil, aniž by se Ústavní soud k samotnému obsahu 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, podrobněji vyjadřoval.

121. Vyhláška upravuje v souladu se zákonným zmocněním obsaženým v § 97 odst. 4 ZEK rozsah uchovávaných provozních a lokalizačních údajů, formu a způsob jejich předávání oprávněným orgánům a způsob jejich likvidace. Z mezí zákonnosti tak napadená vyhláška nevybočuje. Ústavní soud dále posoudil obsah vyhlášky v duchu výše učiněných závěrů a dospěl k závěru, že vyhláška nepřekračuje ani meze ústavnosti (stejně jako napadená zákonná úprava). Vyhláška představuje typický podzákonný právní předpis technického charakteru, která neukládá adresátům žádné nové, zákonem nestanovené povinnosti (viz *a contrario* výhrada zákona podle čl. 4 odst. 1 Listiny). Nyní účinná zákonná úprava je z pohledu Ústavního soudu oproti předchozí podrobnější a přísnější, naplňující požadavky nálezů sp. zn. Pl. ÚS 24/10 a Pl. ÚS 24/11. Pojmy provozní údaje a lokalizační údaje jsou zákonem definovány (viz § 90 a § 91 ve spojení s § 97 odst. 4 ZEK), vyhláška jejich zákonem definovaný obsah pouze blíže konkretizuje (§ 1 a § 2 vyhlášky). Tentýž závěr lze přijmout ohledně úpravy způsobu předávání údajů (§ 3 a příloha vyhlášky). Ustanovením § 4 vyhlášky je konečně operátorům konkretizována povinnost uchované údaje po uplynutí retenční doby likvidovat, stanovenou § 97 odst. 3, poslední věta, ZEK. V situaci, kdy Ústavní soud nepovažuje napadenou zákonnou úpravu za neproporcionální, nemá důvod vyhovět ani tomuto bodu projednávaného návrhu.

VII. Shrnutí

122. Spolu s rostoucí hrozbou teroristických útoků se vyvinul logický trend posilovat pravomoci a nástroje vyšetřujících orgánů veřejné moci na úkor zachování dosavadního standardu základních práv jednotlivců. Uvedený trend se však postupně mění v čase, a také v důsledku rozhodnutí ústavních soudů, ESLP či SDEU začínají politické reprezentace chápat potřebu hledání rovnováhy, při jejímž zachování by státy byly schopny účinně a efektivně dostát pozitivním závazkům, aniž by přitom do základních práv jednotlivců, v tomto kontextu zejména práva na soukromí a informační sebeurčení podle čl. 10 odst. 2, odst. 3 a čl. 13 Listiny, zasahovaly více, než je v demokratické společnosti nezbytně nutné. Změnu trendu směrem k posílení ochrany osobních údajů, či spíše znovunalezení ztracené rovnováhy, demonstruje mimo jiné přijetí GDPR či příprava přijetí tzv. *e-privacy* nařízení, upravujícího oblast soukromí a elektronických komunikací namísto dosavadní stejnojmenné směrnice. Překotný vývoj informačních technologií nelze zastavit či zbrzdit žádnou právní úpravou; dosah internetu a dalších sítí umožňujících elektronickou komunikaci se neomezují na hranice jednotlivých států, jde o globální jev, celosvětový fenomén, který

vnitrostátní zákonodárci řeší různě a obtížně. Je třeba se vypořádat se skutečností, že aktivním přičiněním jednotlivců vzniká nepřeberné množství nejrůznějších dat (metadat) a riziko jejich zneužití exponenciálně narůstá – tomu je třeba prostředky ochrany osobních údajů přizpůsobit.

123. Ústavní soud dospěl k závěru, že v podmínkách dnešní informační společnosti, v níž běžný jednotlivec využívá služeb elektronické komunikace takřka na každém kroku a dobrovolně přijímá, že se o něm ukládají kvanta dat, bylo by nemoudré tolerovat stav, v němž by poskytovatelé služeb údaji uživatelů disponovali, a státní aparát (v odůvodněných případech) nikoli. Plošné uchovávání provozních a lokalizačních údajů představuje snahu státu *„neztratit v době informační společnosti krok“* a mít v rukou efektivní nástroje k plnění svých úkolů – zde zejména v oblasti bezpečnosti státu a jeho obyvatel. Principiálně proto z pohledu Ústavního soudu nelze *data retention* zavrhovat. Z hlediska práva na soukromí není šetrnější varianta, v níž by stát využíval dostupných údajů netransparentním, „pokoutným“ způsobem; takový důsledek však bez jasné právní úpravy nelze vyloučit.

124. V každém případě však shromažďování a zadržování provozních a lokalizačních údajů znamená zvlášť závažný zásah do soukromí prakticky všech obyvatel České republiky. Princip *data retention* spočívá v plošném, nevýběrovém sběru významného množství dat o každé uskutečněné elektronické komunikaci, čímž je intenzivně omezeno soukromí jednotlivce, které je mu na ústavní úrovni garantováno čl. 10 odst. 2 Listiny, potažmo i čl. 10 odst. 3 Listiny ve spojení s čl. 13 Listiny. Tak závažné omezení proto jednak musí být prospěšné silnému veřejnému zájmu, a zároveň je nutno je v maximální možné míře minimalizovat, aby mezi ním a naplněním sledovaných cílů existovala spravedlivá rovnováha. Minimalizace zásahu lze dosáhnout omezením využití dat telekomunikačního provozu jen pro nejnutnější okruhy případů, stanovením přísných podmínek, za kterých jsou data jednak uchovávána, jednak zpřístupňována, a vytvořením záruk každému jednotlivci, že v případě využití jeho údajů bude mít k dispozici účinné prostředky obrany proti případnému zneužití. Na provozní a lokalizační údaje je třeba nahlížet jako na cenný zdroj informací o osobním životě dotčené osoby, jehož zneužití může mít v soukromí jednotlivce značné dopady. Údaje o telekomunikačním provozu mohou mít mnohdy větší vypovídající hodnotu než znalost obsahu komunikace a připodobnění k odposlechům (§ 88 trestního řádu) je zde proto namístě; provozní a lokalizační údaje zasluhují z hlediska ochrany základních práv podobnou míru regulace.

125. Povinnost sběru a uchovávání provozních a lokalizačních údajů lze tolerovat pouze po přiměřenou dobu. Ústavní soud dospěl k závěru, že není-li období šesti měsíců dobou zjevně nepřiměřenou, což nebylo v řízení z hlediska aplikační praxe ani srovnáním s evropským standardem prokázáno, není jeho úlohou suplovat roli zákonodárce a určovat, že by stačila doba kratší a o kolik kratší doba by byla jediná přiměřená. Jde o lhůtu nejkratší z rozmezí, jaké předepisovala (dnes již neplatná) směrnice o *data retention*, a z evropského standardu nevybočuje.

126. Dalším aspektem posouzení přiměřenosti úpravy *data retention* v užším smyslu je úroveň zabezpečení uchovávaných údajů. Ustanovení týkající se zabezpečení nebyla napadena, Ústavní soud se nicméně musel zabývat i touto otázkou. Přestože si lze představit úpravu přísnější, jdoucí nad rámec obecného standardu ochrany osobních údajů stanoveného § 87 a násl. ZEK, nelze z této skutečnosti dovodit závěr, že by

úroveň zabezpečení byla nedostatečná a omezovala by tak soukromí jednotlivce nepřiměřeným způsobem. Citovaná ustanovení ZEK stanovují operátorům řadu povinností, jejichž dodržování podléhá kontrole nezávislých orgánů – dohled nad plněním zákonných povinností vykonává jak Český telekomunikační úřad, tak i Úřad pro ochranu osobních údajů, který v tomto ohledu nevyslovuje žádné konkrétní výtky. V řízení před Ústavním soudem nebylo prokázáno, že by v praxi docházelo k systémovému selhání. Ústavní soud proto nepřisvědčil tvrzení navrhovatelky, že by úroveň zabezpečení provozních a lokalizačních údajů byla z hlediska ochrany soukromí jednotlivců nedostatečná.

127. Ustanovení § 88a trestního řádu nebylo shledáno nepřiměřeným zejména s ohledem na kontext dnešního digitálního věku. Pachatelé trestné činnosti za sebou v dnešní době zanechávají téměř vždy (a často výhradně) elektronickou stopu, a to i tehdy, nepáchají-li trestnou činnost přímo prostřednictvím služeb elektronických komunikací. Stát má pro naplnění veřejného zájmu na zajištění bezpečnosti obyvatel a majetkových hodnot za úkol trestnou činnost odhalovat, objasňovat a předcházet jí; aby mohl tento úkol plnit efektivně, nesmí za pachateli ve svých vyšetřovacích metodách „pokulhávat“ a musí mít k dispozici odpovídající technické prostředky. V řízení nebylo prokázáno, že by byl § 88a trestního řádu nadužíván, ani že by výčet trestných činů, na něž se vztahuje, byl zbytečný. Nastavené podmínky přístupu k údajům i procesní záruky proti zneužití jsou dostatečně přísné a vyvažují zásah do soukromí dotčeného jednotlivce.

128. Napadená ustanovení ZPol byla předmětem přezkumu Ústavního soudu poprvé; je z nich patrné, že zcela neodpovídají požadavkům vysloveným v nálezu sp. zn. Pl. ÚS 24/10. V citovaném nálezu se však Ústavní soud nezabýval využitím provozních a lokalizačních údajů mimo trestní řízení. Obě ustanovení předvídají situace, kdy jakékoli časové prodlení může způsobit nevratnou újmu na životě či zdraví – absence soudního dohledu je zde proto ospravedlnitelná. Totéž se týká procesních záruk proti zneužití, jež by měl mít jednotlivec k dispozici, počínaje povinností jej o využití jeho údajů informovat.

VIII. Závěr

129. Ústavní soud proto podle § 70 odst. 2 zákona o Ústavním soudu návrh skupiny poslanců zamítl. Požadavek přiměřenosti zásahu do práva na soukromí ve světle čl. 10 odst. 2 ve spojení s čl. 10 odst. 3 a čl. 13 Listiny a navazující judikatury Ústavního soudu právní úprava v kontextu dnešního společenského i technologického vývoje naplňuje a lze ji vyložit ústavně konformním způsobem. Každou žádost a odůvodněnost jejího podání je třeba ze strany oprávněného orgánu důkladně zvážit a ze strany soudu pečlivě přezkoumat s ohledem na konkrétní okolnosti posuzovaného případu, a neomezovat se pouze na posouzení splnění formálních náležitostí žádosti, tak jak současná právní úprava i judikatura Ústavního soudu vyžaduje.

Poučení: Proti rozhodnutí Ústavního soudu se nelze odvolat.

V Brně dne 14. května 2019

Pavel Rychetský
předseda Ústavního soudu

Odlišné stanovisko soudkyně Kateřiny Šimáčkové k výroku i odůvodnění nálezu Ústavního soudu sp. zn. Pl. ÚS 45/17 ze dne 14. 5. 2019

1. K zamítavému nálezu pléna zaujímám odlišné stanovisko, neboť se domnívám, že napadená právní úprava zákona o elektronických komunikacích („ZEK“) z ústavněprávního pohledu neobstojí, neboť neskýtá dostatečné záruky proti úniku či zneužití dat, jejichž sbírání stát ukládá, a tím i umožňuje, soukromým subjektům (mobilním operátorům). Jsem přesvědčena, že neobstojí ani napadená úprava zákona o Policii, protože zasahuje do soukromí jednotlivců neproporcionálním způsobem; zákonodárce totiž policii poskytl mimo trestní řízení příliš široký přístup k citlivým údajům bez náležitého odůvodnění a časového odstupňování podle jednotlivých situací příliš dlouhé „retenční doby“. To vše v kombinaci s nemožností jednotlivce sám kontrolovat rozsah shromažďování a využití údajů o své osobě prostřednictvím „data retention“ a případně podrobit neodůvodněné zásahy do svého soukromí kontrole soudní mocí či expertním orgánem.

2. Při posuzování úpravy „data retention“ je třeba vyjít ze skutečnosti vyjádřené i ve většinovém názoru pléna (v bodě 49), a sice že prostřednictvím shromažďovaných informací lze sestavit podrobný osobní a komunikační profil jednotlivce. A to včetně tak zásadních údajů jako jsou politická orientace, zdravotní stav, sexuální orientace, osobní vazby a společenské postavení. Z pohledu ústavněprávní ochrany se tedy jedná o mimořádně citlivá osobní data. I podústavní právo tyto osobní údaje považuje za tzv. zvláštní kategorie osobních údajů (či citlivé osobní údaje) a s jejich ochranou spojuje zvláštní povinnosti nad rámec ochrany ostatních osobních údajů pro všechny, kdo je zpracovávají. Většinový názor pléna (bod 50) připouští, že metadata o uskutečněné komunikaci mohou být pro soukromí jednotlivce „nebezpečnější“ než znalost samotného obsahu komunikace, neboť jsou snadno zpracovatelná a analyzovatelná, přičemž z výsledků takového zpracování pak lze usuzovat budoucí chování jednotlivce. Metadata, jež jsou předmětem uchovávání a předávání na základě napadené legislativy, tedy mohou o jednotlivci vypovědět velmi komplexní a nesmírně citlivé informace, jež zcela zásadním způsobem zasahují do jeho soukromé sféry, osobnostních práv a práva na informační sebeurčení.

3. Do jisté míry se ztotožňuji s názorem většiny, že není ústavně zcela nepřijatelné, aby metadata byla po určitou dobu uchovávána a předávána orgánům činným v trestním řízení, případně dalším specificky vymezeným subjektům, a to pouze za velmi přesně vymezenými účely. Většinový názor vychází z toho, že v rámci testu proporcionality nelze nalézt jiné opatření, které by bylo způsobilé dosáhnout stejného legitimního cíle, avšak za cenu nižšího zásahu do základních práv a svobod jednotlivců. S tímto závěrem většiny se neztotožňuji z důvodů, které později vyložím (viz bod 11 níže). Domnívám se, že i kdyby skutečně takové opatření neexistovalo, je třeba požadovat alespoň dodatečné záruky a pojistky minimalizující negativní dopady do základních práv a svobod. Dle mého názoru je tak pro ústavnost takovéhoto shromažďování, uchovávání a předávání metadat zcela zásadní a klíčové, aby byl poskytnut ucelený a koherentní systém záruk proti neoprávněnému zpracování takovýchto dat, jejich úniku, změně, poškození či zničení, a to jak nahodile, tak cíleně.

4. Jsem toho názoru, že napadená právní úprava, zejména pak napadená ustanovení ZEK, takovýto koherentní systém záruk neposkytují. Tyto záruky chybí o to více, vezmeme-li v potaz fakt, že jsou to právě mobilní operátoři a další soukromí poskytovatelé služeb, tedy subjekty s minimální veřejnou kontrolou sledující primárně

komerční, resp. soukromé zájmy, na které jsou bez důsledné a preventivní kontroly částečně přenášeny povinnosti náležející státu (získávání, uchovávání, zabezpečování a další nakládání s daty, které mají sloužit např. ke stíhání trestné činnosti).

5. Ochrana dat, resp. osobních údajů, kterými metadata jistě mohou být a zpravidla budou (konec konců účelem jejich zpracování v kontextu napadené právní úpravy je zejména identifikovat konkrétní osobu, např. pachatele trestné činnosti), má již velmi dlouho obecnou úpravu, která dříve byla obsažena v zákoně č. 101/2000 Sb., o ochraně osobních údajů, a relativně nově pak zejména v obecném nařízení o ochraně osobních údajů (dále jen „GDPR“), které je nyní s ročním odstupem konečně doplněno implementačním zákonem č. 110/2019 Sb., o zpracování osobních údajů, jež nahradil zákon o ochraně osobních údajů. Jelikož GDPR představuje provedení práva na informační sebeurčení na podústavní úrovni, a tedy specifikuje jeho nuance, je potřeba tuto obecnou úpravu vzít v potaz, pokud Ústavní soud provádí test proporcionality a zvažuje, zda nejsou dostupné jiné nástroje k dosažení legitimního cíle, jež by méně zasahovaly do základních práv a svobod, případně, jestli nemají být z hlediska přezkumu ústavnosti požadovány dodatečné záruky a technická a organizační opatření pro zajištění bezpečnosti předmětných dat (a pokud ano, tak jaká).

6. Ve vztahu k výše uvedenému závěru, že z metadat je možné sestavit komplexní komunikační a sociální profil jednotlivce včetně jeho politických názorů, sexuální orientace apod., není možné pominout, že dle čl. 22 odst. 1 GDPR má každý právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něj právní účinky nebo se ho obdobným způsobem významně dotýká. Ustanovení čl. 22 odst. 2 písm. b) GDPR sice stanoví výjimku pro takovéto zpracování, pokud probíhá na základě zákona, nicméně požaduje, aby tato zákonná úprava stanovila vhodná opatření zajišťující ochranu práv a svobod a oprávněných zájmů subjektu údajů. I podústavní obecná úprava tak vyžaduje dodatečné záruky.

7. Pro inspiraci týkající se konkrétních dodatečných záruk, jež dle mého přesvědčení chybí v napadené právní úpravě, resp. nejsou v ní stanoveny dostatečně určitě a není tak zaručen minimální standard ochrany uchovávaných dat a záruk pro jejich bezpečné předávání, považuji za vhodné použít zejména čl. 32 GDPR, jež mezi příslušnými opatřeními stanovuje např. pseudonymizaci a šifrování dat, schopnost zajištění neustálé důvěrnosti, integrity, dostupnosti a odolnosti systémů tím, že bude např. vyžadováno minimální odpovídající technické zařízení a programové vybavení, zabezpečení objektů a místností, zabezpečení serverů, minimální požadavky na přístupové kódy a hesla, atp. Samozřejmostí by měly být rovněž požadavky na okamžitou obnovitelnost dat v případě bezpečnostních incidentů stejně jako požadavky na pravidelné testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování dat. Zákonodárce by měl též vyžadovat od mobilních operátorů pečlivý dohled nad osobami, které mají k citlivým datům přístup, a tyto jejich postupy preventivně průběžně kontrolovat. Veškeré procesy zpracování dat související s ukládáním a předáváním příslušných metadat by měly rovněž podléhat posouzení vlivu na ochranu osobních údajů ve smyslu zmíněné legislativy a pravidelnému přezkumu z tohoto hlediska.

8. Ve vztahu k zajištění dostatečných záruk pak považuji na napadené legislativě dále problematické zejména předávání dat orgánům veřejné moci, které je potřeba z tohoto pohledu odlišit od samotného uchovávání, což vyjádřil ve své výpovědi rovněž

doc. Radim Polčák. Zatímco samotné uložení dat se děje i za čistě soukromými účely poskytovatelů příslušných služeb (např. marketingové aktivity telefonního operátora) a definováním tohoto účelu je také omezen rozsah zpracovávaných dat a délka jejich uchování, předávání dat se děje výhradně za účelem zásahu do soukromí jednotlivce (byť sledující legitimní cíl), a představuje tak výrazně vyšší riziko z hlediska zneužití či úniku dat. Napadená legislativa v tomto ohledu dle mého názoru neposkytuje dostatečné obecně platné záruky. Ústavně konformní právní úprava (a jedno zda na zákonné či podzákonné úrovni) by měla obsahovat konkrétní technická opatření jako třeba nástroje pro ověřování identity uživatelů, nástroje pro řízení přístupových oprávnění, nástroje pro zaznamenání činnosti informačních systémů, jejich uživatelů a administrátorů, nástroje pro identifikaci a vyhodnocení bezpečnostních incidentů, nástroje pro zajištění přenosu dat pomocí neveřejné zabezpečené sítě a organizační opatření jako např. minimální požadavky na řízení rizik a bezpečnostní politiku, bezpečnostních požadavků na dodavatele, řízení provozu příslušně infrastruktury, atd.

9. Domnívám se tedy, že aby mohlo být požadavku ústavnosti přezkoumávané právní úpravy učiněno zadost, záruky ve smyslu výše uvedeného by měly být upraveny výslovně, dostatečně určitě a s možností (resp. nezbytností) jejich veřejné kontroly specificky v kontextu „data retention“, a to samozřejmě nad rámec obecné úpravy obsažené v GDPR nebo v jiné podústavní právní úpravě, která kvůli citlivosti sbíraných dat, jejich rozsahu, způsobu užití a závažnosti účelů, pro něž jsou data sbírána, může posloužit pouze jako výchozí bod a soubor základních principů.

10. Jedině dostatečně konkrétní a všeobecně platné povinnosti poskytovatelů elektronických služeb i oprávněných orgánů veřejné moci zajistit tyto záruky mohou vyvážit zásadní zásah do základních práv a svobod, který přezkoumávaná legislativa umožňuje. Bez takovýchto explicitních záruk v rámci „data retention“ se domnívám, že nelze shledat napadenou legislativu jako ústavně souladnou.

11. Poučené osoby, jež byly vyslechnuty, zejména pak doc. Radim Polčák, uvedly, že v jiných evropských zemích je úprava odlišná, přičemž plní kýžený cíl s obdobnou efektivitou. Zejména se tedy lze zamyslet, zda by nebylo možné příslušná metadata uchovávat kratší dobu v kombinaci se „zmrazovacím příkazem“, případně uchovávat po dobu 6 měsíců pouze některá metadata v menším rozsahu, než je tomu dnes (z výpovědi dalších poučených osob vyplývá, že Policie a další orgány činné v trestní řízení ponejvíce využívají jen některé druhy osobních údajů a po kratší dobu), metadata předávat příslušným orgánům v rozsahu dle závažnosti příslušné trestné činnosti, přístupu jednotlivých osob či orgánů dle závažnosti příslušných případů, resp. založit a odstupňovat přístup k metadatům podle cíle, jehož dosažení oprávněný orgán sleduje, případně zvolit jakoukoliv kombinaci uvedených omezení plošného „data retention“. Již samotná existence těchto alternativních řešení (a jejich úspěšná aplikace v každodenní praxi v dalších evropských zemích, například v Německu či na Slovensku), jež více šetří základní práva a svobody, poukazuje na neudržitelnost tvrzení, že současná úprava „data retention“ v České republice nemá alternativu a je jediným vhodným a nezbytným prostředkem k dosažení příslušného legitimního cíle. Z tohoto důvodu tedy nesouhlasím s výsledkem testu proporcionality, jak je proveden v plenárním nálezu. Shora uvedené minimalizační principy (omezení účelem, minimalizace rozsahu zpracovávaných údajů, omezení doby uložení apod.) jsou ostatně základními zásadami při jakémkoliv zpracování osobních údajů a musí se vztahovat také na „data retention“. Osobní údaje musí být zpracovávány na základě principu nezbytnosti pro dosažení cíle (need to know) nikoliv proto, že by mohly příslušnému orgánu potenciálně přijít vhod a ulehčit

práci (nice to have). V demokratickém právním státě založeném na úctě k právům a svobodám jednotlivce musí zákonná úprava v prvé řadě ctít soukromí a svobodu jednotlivce a pouze výjimečně a v nejmenší možné míře do ní může být za určitých okolností zasaženo. Referenčním bodem je tak jednotlivec a jeho přirozená práva, nikoliv potřeba orgánů veřejné moci v tomto případě užívat metadata.

12. Domnívám se, že uvedené požadavky nejsou samoúčelným omezováním orgánů činných v trestním řízení v naplňování jejich důležité role v každé demokratické společnosti. Většinový názor je, zdá se, založen na premise, již vyjádřila jedna ze zainteresovaných stran – konkrétně vrchní státní zástupkyně Lenka Bradáčová – že vzhledem k čím dál většímu přesouvání lidského života (a tedy mimo jiné i kriminality) do „světa dat“ je nezbytné, aby stát disponoval čím dál většími pravomocemi pro potírání trestné činnosti i právě ve „světě dat“ (na úkor svobody jednotlivce, samozřejmě). Tento závěr však nepovažuji za nevyhnutelný. Posilování pravomocí orgánů činných v trestním řízení na úkor svobody jednotlivce je v jakémkoliv okamžiku a za všech okolností hodnotovou volbou. Nelze tedy tvrdit, že pokud čím dál více osoby žijí „online“ a páchají tam také trestnou činnost, tím více pravomocí na kontrolu těchto našich životů stát musí mít. Stejně tak by se totiž dalo tvrdit přesně opačně, že čím více se náš život přesouvá do virtuálního světa, tím více by se ochrana práv jednotlivců a jejich osobnosti a soukromí měla vztahovat také na virtuální kontext, jehož jsou metadata nedílnou součástí. Právě tento druhý výklad spíše odpovídá tomu, jak by měl k ochraně lidských práv přistupovat Ústavní soud jako strážce ústavnosti a základních práv a svobod jednotlivce, a touto optikou pak provádět vyvažování mezi ochranou práva jednotlivce a veřejným zájmem.

13. Přestože principiálně nerozporuji uchovávání a předávání metadat, chtěla bych vyjádřit nesouhlas se závěrem obsaženým v bodě 76, 89 a na jiných místech, kde dochází dle mého názoru k nepřípustnému zjednodušení celé problematiky. Princip „data retention“ je plénem akceptován s argumentem všeobecné ochoty sdílet osobní údaje pro marketingové účely. Tento názor však pomíjí zásadní rozdíl mezi dobrovolným sdílením dat, které subjekty údajů mohou ovlivnit, a které probíhá za účelem, o jehož dosažení sami stojí (obdržení obchodních nabídek), a které mohou navíc kdykoliv ukončit (odvoláním souhlasu, odchodem ze sociální sítě, smazáním účtu, …). Naproti tomu „data retention“ je zákonem vynucené plošné sbírání všech dat (krom obsahu), na základě kterých je možné vytvořit velmi podrobné profily daných jednotlivců, a to zcela nezávisle na vůli nebo alespoň vědomí subjektů údajů. Nadto souhlas se shromažďováním těchto údajů operátorům neudělují zdaleka všichni jejich zákazníci (viz bod 89 nálezu uvádějící, že je to asi 70 % zákazníků), přičemž Ústavní soud má za povinnost chránit základní práva všech jednotlivců, tedy i těch, kteří nejsou ochotni odsouhlasit operátorovi své sledování.

14. Většina pléna vychází z přesvědčení, že zrušení napadené úpravy by vyvolalo jakýsi chaos, menší transparentnost, vyšší riziko zneužití dat, případně by situaci uvrhlo do „legislativního stínu“. Nedomnívám se, že tyto obavy jsou namístě. Zrušení napadené právní úpravy by samozřejmě vyvolaly naléhavou potřebu přijetí úpravy nové, nicméně Ústavní soud mohl zvolit např. dlouhý odklad vykonatelnosti a naznačit, že nerozporuje sám systém, ale pouze nedostatek záruk a ochrany dat a rozsah jejich využití.

15. Neobstojí ani argumenty o zajištěných institucionálních zárukách prostřednictvím pokut od existujících orgánů, majících velké množství jiných úloh,

nebo tvrzení, že se před Ústavním soudem neprokázala žádná zneužití systému. Riziko třeba i vysoké sankce má minimální odstrašující potenciál, je-li toto riziko nepravděpodobné (není přece důležitá výše trestu, ale jeho neodvratitelnost). Ještě efektivnější pak je takové nastavení systému, aby k zneužívání nemohlo docházet. Většině však postačila potenciální možnost sankcí pro případné narušitele soukromí nad rámec zákonných limitů a přesvědčivé vystoupení tří osobností české policie a státního zastupitelství při ústním jednání.

16. Další důležitý důvod pro větší kontrolu dat shromážděných soukromými společnostmi na základě povinností, stanovených v ZEK, a větší míru obezřetnosti s jejich sbíráním a používáním je nejen ochrana soukromí jednotlivce, ale i možnost zneužitelnosti mimo rámec trestních řízení. V obdobném kontextu sociálních sítí lze sledovat, jak jsou v jednotlivých politických kampaních využívána data, která o sobě jednotlivci sami zveřejňují a která jsou provozovateli těchto sítí zpeněžována, a jak tento způsob zneužití takto shromážděných dat může vést k zásahům do svobodné soutěže politických sil. Už na přelomu tisíciletí varoval Paul Schwartz, že sbírání osobních údajů v kyberprostoru ohrožuje nejen individuální možnost sebeurčení jednotlivých lidí, ale rovněž zhoršuje kvalitu deliberativní demokracie (SCHWARTZ, Paul M. Privacy and Democracy in Cyberspace. *Vanderbilt Law Review*, 1999, vol. 52, s. 1609). Eliška Wagnerová to obecně vystihla názvem svého příspěvku o ochraně soukromí: „Kde má být svoboda, tam musí být soukromí." (Právo na soukromí: Kde má být svoboda, tam musí být soukromí. In: ŠIMÍČEK, Vojtěch (ed.). *Právo na soukromí*. Brno: Masarykova univerzita, 2011, s. 49). Boehme-Neßler v textu z roku 2016 varuje, že v dlouhodobém horizontu nebude existovat žádná demokracie, nebude-li zajištěna ochrana soukromí (Boehme-Neßler Volker. Privacy: a matter of democracy. Why democracy needs privacy and data protection. *International Data Privacy Law*. 2016, vol. 6, no. 3, s. 222-229).

17. Závěrem tedy shrnuji, že napadená právní úprava ve světle nedostatečných záruk před zneužitím shromážděných dat neobstojí, a to nejen z hlediska ochrany práv jednotlivců, ale též celého systému naší demokracie. Naše úprava „data retention" i ve srovnání s jinými státy Evropy metadata jednotlivců dostatečně nechrání ani dostatečně nekontroluje, co se s metadaty děje u operátora, který je shromažďuje, a jakým způsobem jsou následně předávány a využívány samotnou státní mocí. Stát, ukládající a povolující soukromé společnosti tato data shromažďovat, nevyužívá všech možností pro to, aby nemohla být zneužita. Nadto zákonodárce nedává jednotlivci možnost, aby měl kontrolu nad tím, v jakém rozsahu jsou jeho metadata státem využívána, a tak je jednotlivec připraven o možnost bránit se proti takovému zásahu.

V Brně dne 14. května 2019

Kateřina Šimáčková