Jan Vobořil
Advokát

O----------

Ústavní soud České republiky

Joštova 8

660 83 Brno 2

V Praze dne 15. prosince 2017

Návrh na zrušení § 97 odst. 3 a 4 zákona č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů

Návrh na zrušení § 68 odst. 2 a § 71 písm. a) zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů

Návrh na zrušení § 88a zákona č. 141/1961 Sb., trestního řádu, ve znění pozdějších předpisů

Návrh na zrušení vyhlášky č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů

Navrhovatel:

Skupina 58 poslanců dle ust. čl. 88 odst. 1 Ústavy ve spojení s ust. § 64 odst. 1 písm. b) zákona o Ústavním soudu

Právně zastoupena:

Mgr. et Mgr. Janem Vobořilem, advokátem ev. č. 15017, se sídlem U Smaltovny 1115/32, Praha 7, 170 00

Účastníci řízení:

1. Poslanecká sněmovna Parlamentu ČR, se sídlem Sněmovní 4, 118 26, Praha 1

2. Senát Parlamentu ČR, se sídlem Valdštejnské náměstí 17/4, 118 01 Praha 1

Datovou schránkou

Příloha: Podpisová listina k návrhu a plná moc pro řízení před Ústavním soudem

I.

Navrhovatel

Níže podepsaná skupina poslanců Poslanecké sněmovny Parlamentu České republiky využívá tímto svého práva daného ustanovením § 64 odst. 1 písm. b) zákona č. 182/1993 Sb. o Ústavním soudu, ve znění pozdějších předpisů (dále „zákon o Ústavním soudu“) a podává návrh na zrušení části zákona a prováděcí vyhlášky dle čl. 87 odst. 1 písm. a) a b) a č. 88 odst. 1 ústavního zákona č. 1/1993 Sb., Ústavy České republiky, ve znění pozdějších předpisů (dále „Ústava“).

II.

Účastník řízení

Na výše uvedeném ustanovení zákona se usnesl Parlament České republiky, který má tímto postavení účastníka řízení dle § 69 odst. 1 zákona o Ústavním soudu.

III.

Napadená ustanovení

Tento návrh směřuje proti ustanovení § 97 odst. 3 a 4 zákona č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů (dále „ZEK“) a prováděcí vyhlášce č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů (dále „Vyhláška“). Jakož i proti § 68 odst. 2 a § 71 písm. a) zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů (dále „PolZ“) a § 88a zákona č. 141/1961 Sb., trestního řádu, ve znění pozdějších předpisů (dále „TŘ“)

Ustanovení ***§ 97 odst. 3***, jehož zrušení je navrhováno, zní:

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).

Ustanovení ***§ 97 odst. 4***, jehož zrušení je navrhováno, zní:

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.

Podrobný popis provozních a lokalizačních údajů, které mají být uchovávány, obsahuje § 2 **Vyhlášky**. Vzhledem k rozsáhlosti napadené vyhlášky navrhovatelé uvádí příkladný výčet nejdůležitějších údajů, které jsou uchovávány a ve zbytku odkazuje na její znění vyhlášené ve Sbírce zákonů.

U veřejných **telefonních sítí s přepojováním okruhů** se uchovávají tyto provozní a lokalizační údaje

a) telefonní číslo volajícího a volaného, telefonní čísla, která se zúčastnila konferenčního volání, identifikátor telefonní karty použité ve veřejném telefonním automatu,

b) datum a čas zahájení komunikace,

c) délka komunikace,

d) datum a čas odeslání textové zprávy SMS,

e) použitá telefonní služba (např. přesměrování hovoru, hlasová schránka apod.)

f) stav komunikace

U veřejných **mobilních telefonních sítí** se uchovávají údaje uvedené výše a dále

a) identifikátor IMSI[1] volajícího a volaného,

b) identifikátor mobilního přístroje volajícího a volaného,

c) datum a čas odeslání multimediální zprávy MMS,

d) označení základnové stanice Start a základnové stanice Stop[2],

U služby **přístupu k internetu z pevného připojení**

a) typ připojení,

b) telefonní číslo nebo označení uživatele,

c) identifikátor uživatelského účtu,

d) adresa MAC zařízení uživatele služby[3],

e) datum a čas zahájení a ukončení připojení k internetu,

f) označení přístupového bodu u bezdrátového připojení k internetu,

g) adresa IP a číslo portu, ze kterých bylo připojení uskutečněno;

U služby **přístupu k internetu z mobilního připojení**

a) typ připojení,

b) telefonní číslo uživatele,

c) identifikátor mobilního zařízení,

d) datum a čas zahájení a ukončení připojení k internetu,

e) označení základnové stanice Start a základnové stanice Stop,

f) adresa IP a číslo portu, ze kterých bylo připojení uskutečněno;

[1] Identifikátor IMSI je dle §1 písm. d) Vyhlášky mezinárodní identifikátor účastníka veřejné mobilní komunikační sítě přidělený operátorem
[2] Jedná se o základnové stanice prostřednictvím nichž je uživatel připojen do veřejné telefonní sítě (viz § 1 písm. b), c) Vyhlášky).
[3] Adresou MAC je dle § 1 písm. f) Vyhlášky identifikátor síťového zařízení uživatele na spojové vrstvě.

U služby **přístupu ke schránce elektronické pošty**

a) adresa IP a číslo portu, ze kterých bylo připojení uskutečněno,

b) identifikátor uživatelského účtu,

c) datum a čas zahájení připojení ke schránce elektronické pošty,

d) datum a čas ukončení připojení ke schránce elektronické pošty,

e) identifikátor protokolu elektronické pošty;

U služby **přenosu zpráv elektronické pošty**

a) adresa IP a číslo portu zdroje a cíle přenášené zprávy,

b) datum a čas odeslání zprávy,

c) adresa elektronické pošty odesílatele,

d) adresy elektronické pošty příjemců,

e) stav přenosu zprávy,

f) identifikátor protokolu elektronické pošty;

U služby **IP telefonie**

a) adresa IP a číslo portu zdrojového zařízení,

b) adresa IP a číslo portu cílového zařízení,

c) transportní protokol,

d) datum a čas zahájení a ukončení komunikace,

U služby **přístupu k internetu podle písmene z pevného či mobilního připojení s překladem adres IP**

a) privátní adresa IP,

b) veřejná adresa IP a číslo portu, nebo přidělený rozsah portů,

c) datum a čas zahájení překladu adres,

d) datum a čas ukončení překladu adres.

Ve všech výše uvedených případech se dále uchovávají také údaje jako jméno, příjmení a adresa účastníka nebo registrovaného uživatele uvedená ve smlouvě nebo adresa umístění telekomunikačního koncového zařízení. Dle § 2 odst.4, odst. 5, odst. 6 Vyhlášky se uchovávají také údaje o všech telefonních automatech, údaje o všech základnových stanicích (tzv. BTS) včetně geografických souřadnic, údaje o vzájemných vazbách mezi telefonními čísly a identifikátory IMSI, jakož i identifikátory mobilních zařízení, údaje o aktivaci u předplacených služeb či údaje o poskytovatelích služeb.

Z důvodu chybějícího nezávislého soudního přezkumu při žádostech o poskytnutí provozních a lokalizačních údajů je dále navrhováno zrušení § 68 odst. 2 a § 71 písm. a) PolZ.

Ustanovení **§ 68 odst. 2 PolZ**, jehož zrušení je navrhováno, zní:

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 předpisů jinak. Informace se poskytne ve formě a v rozsahu stanoveném jiným právním předpisem.

Ustanovení **§ 71 písm. a) PolZ**, jehož zrušení je navrhováno, zní:

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[20)] jinak; informace se poskytne ve formě a v rozsahu stanoveném jiným právním předpisem.

Z důvodu příliš šiokého vymezení okruhu trestných činů a nedostatečného omezení využívání provozních a lokalizačních údajů na nezbytné případy je navrhováno zrušení ustanovení § 88a TŘ.

Ustanovení § 88a TŘ, jehož zrušení je navrhováno, zní:

(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.

IV.

Rozpor s ústavním pořádkem

Navrhovatel namítá rozpor napadených ustanovení s těmito ustanoveními ústavního pořádku ČR:

a) čl. 7 odst. 1 Listiny základních práv a svobod, vyhlášené usnesením předsednictva České národní rady č. 2/1993 Sb. jako součást ústavního pořádku České republiky (dále jen „Listina“):

„*Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem.*“

b) čl. 10 odst. 2 a 3 Listiny:

„*(2) Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.*

(3) Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.“

c) čl.13 Listiny:

„Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.“

d) čl. 8 Úmluvy o ochraně lidských práv a základních svobod (dále „EÚLP“):

„(1) Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence.

(2) Státní orgán nemůže do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, ochrany pořádku a předcházení zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.“

V.
Prejudikatura Ústavního soudu

Ústavní přezkum § 97 odst. 3 a 4 zákona o elektronických komunikacích, jakož i jeho tehdejší prováděcí vyhlášky č. 485/2005 Sb. byl iniciován v březnu 2010 skupinou 51 poslanců. Ústavní soud návrhu na zrušení této právní úpravy, která v roce 2005 s předstihem implementovala do českého právního řádu evropskou směrnici č. 2006/24/ES, o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES (dále jen „směrnice o data retention“), vyhověl nálezem **sp. zn. Pl. ÚS 24/10 ze dne 31. 3. 2011**. Ústavní soud se zabýval tím, jestli uchovávání a využívání provozních a lokalizačních údajů představuje zásah do práva na soukromí jedince, i když nedochází přímo k uchovávání obsahu komunikace. Došel k závěru, že jde o významný zásah do soukromí (bod 44) zejména proto, že **lze data propojovat a vytvářet tak profily jednotlivých osob**, z nichž lze zjistit osobnostní charakteristiky jednotlivých osob. Ústavní soud dále posuzoval ospravedlnitelnost takové právní úpravy, pokud jde o zásah do práva na soukromí, respektive práva na informační sebeurčení. Soud kritizoval zejména velkou nejasnost a neurčitost právní úpravy, jakož i **absenci striktních limitů tohoto zásahu** do základních práv. Předně ÚS kritizoval nejasné vymezení účelů,

pro které mají být údaje poskytovány, což dle ÚS znemožňuje posouzení napadené úpravy z hlediska její skutečné potřebnosti. (bod 47) Dále ÚS kritizuje nejasné vymezení orgánů, které jsou oprávněny data vyžadovat (bod 46) nebo absenci pravidel, která by dovolovala využívat údaje pouze v úzce vymezených případech vyšetřování zvlášť závažných trestných činů, což mělo v praxi za následek, že údaje byly využívány i při vyšetřování běžné, méně závažné kriminality. (body 48 a 49) Dále ÚS upozorňuje na absenci jasných a detailních pravidel pro zabezpečení osobních údajů u operátorů, kteří mají povinnost data uchovávat. (bod 50)

Jako **obiter dictum** (body 55-59) pak ÚS vyslovil pochybnosti, **„***zda* ***samotný nástroj plošného a preventivního uchovávání provozních a lokalizačních údajů téměř o veškeré elektronické komunikaci je z hlediska intenzity zásahu do soukromé sféry nepřeberného množství účastníků elektronické komunikace nástrojem nezbytným a přiměřeným***." (bod 55) Tuto pochybnost pak zasadil do kontextu širší evropské debaty, řešení otázky ústavní konformity národních implementací směrnice o data retention v dalších evropských státech, jakož i kritických ohlasů ze strany Evropského parlamentu či evropského inspektora osobních údajů. Soud vyslovil také **pochybnost o efektivitě data retention** zejména s ohledem na možnost využívání anonymních SIM karet. V neposlední řadě pak vyjádřil pochybnost o tom, zda by vůbec poskytovatelé služeb měli jakožto soukromé osoby disponovat takovým objemem informací o uživatelích služeb.

Vzhledem k tomu, že návrh přímo napadal pouze shromažďování provozních a lokalizačních údajů a jejich uchovávání a nikoli využívání ze strany oprávněných orgánů v trestním řízení a výtky Ústavního soudu přitom částečně směřovaly i proti § 88a trestního řádu, který upravuje využívání provozních a lokalizačních údajů v trestním řízení a Ústavní soud explicitně vyzval zákonodárce, aby se ústavní konformitou tohoto ustanovení také zabývali (bod 54), obrátil se na soud s návrhem na zrušení § 88a trestního řádu Obvodní soud pro Prahu 6. Ústavní soud svým nálezem **sp. zn. Pl. ÚS 24/11 ze dne 20. 12. 2011** zrušil s účinností k 30. 9. 2012 napadené ustanovení trestního řádu. Důvodem pak byla zejména skutečnost, že právní úprava nereflektovala požadavek proporcionality zásahu do základního lidského práva, v právní úpravě se nijak nepromítl požadavek omezení využití těchto údajů v rámci trestních řízení na nezbytné případy, přičemž tento nedostatek nelze dle ÚS odstranit ani prostřednictvím stanovené soudní kontroly, protože ani soudní kontrola nemůže nahradit absenci dostatečně určité zákonné právní úpravy, jež je ve smyslu čl. 4 odst. 2 Listiny předpokladem omezení základních práv a svobod v obecné rovině.

Na derogaci výše uvedených ustanovení zákona o elektronických komunikacích, trestního řádu a prováděcí vyhlášky reagovala vláda přípravou nové právní úpravy (konkrétně zákona č. 273/2012 Sb., kterým novelizovala několik zákonů a Vyhlášky), která měla zohlednit výhrady ústavního soudu. Argumentem pro její

přijetí, pak byla zejména nutnost implementovat směrnici o data retention, jakož i tvrzená potřebnost těchto údajů pro dokazování v rámci trestních řízení. Takto přijatá právní úprava je nyní napadena tímto návrhem.

VI.

Prejudikatura Soudního dvora EU

Vedle výše uvedené judikatury je třeba v rámci posouzení ústavní konformity brát v potaz i judikaturu Soudního dvora Evropské unie, který se hned dvakrát zabýval otázkou souladu směrnice o data retention, jakož i samotného principu plošného shromažďování provozních a lokalizačních údajů, a jejich souladu s Listinou základních práv EU.

Navrhovatelé mají za to, že Listinu základních práv EU, jakož i navazující judikaturu Soudního dvora Evropské unie je třeba brát nejen jako interpretační vodítko při výkladu vnitrostátních norem, zejména Listiny základních práv a svobod, ale i jako aplikovatelný zdroj subjektivních práv, čemuž přisvědčil Ústavní soud i v tzv. prvním lisabonském nálezu **sp. zn. Pl. ÚS 19/08**. (bod 201) Jak konstatoval Ústavní soud v dalším svém nálezu **sp. zn. Pl. ÚS 14/14**: *„Jelikož přijímání vnitrostátních implementačních předpisů k Aktu, včetně vyplnění jím poskytnutého prostoru pro legislativní uvážení národního zákonodárce, je „uplatňováním" unijního práva ve smyslu čl. 51 odst. 1 Listiny základních práv Evropské unie, mohou se na přezkumu ústavnosti těchto předpisů v členských státech spolu s referenčními kritérii ústavního pořádku v zásadě podílet – podle své povahy – také ustanovení LZPEU, ať už „prostupováním" do ústavního pořádku nebo přímou aplikací v případě vyšší úrovně jimi poskytované ochrany (čl. 53 LZPEU) [...]."*

Na nezbytnost aplikace Listiny základních práv EU včetně níže zmíněné judikatury poukazuje i slovenský ústavní soud ve svém rozhodnutí, kterým zrušil slovenskou právní úrpavu data retention, jedná se konkrétně o nález **Ústavného súdu Slovenskej republiky, Pl. ÚS 10/2014-78 ze dne 29. 4. 2015**. [4] Slovenský ústavní soud zde již v době po zrušení směrnice o data retention Soudním dvorem EU (viz níže) konstatoval, že ať už jde o právní úpravu, která implementovala zrušenou směrnici, nebo o právní úpravu, která se opírala o čl. 15 odst. 1 evropské směrnice č. 2002/58/ES, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (dále jen „e-privacy směrnice") a šlo tedy o výjimky z unijních předpisů, je ji v každém případě nezbytné považovat za sféru působnosti práva EU a to včetně ustanovení dalších zákonů, které vycházejí z dané směrnice a umožňují využívat telekomunikační data například v trestních řízeních či při práci policie mimo trestní řízení (k tomu viz bod 68 nálezu).

[4] Dostupné zde: http://www.eisionline.org/images/Data_retention_rozhodnutie_PL_US_10_2014.pdf

První rozhodnutí SDEU ve spojených věcech **C-293/12 a C 594/12 ze dne 8. 4. 2014 (dále jen "rozhodnutí Digital Rights Ireland")**[5] došlo ke zrušení směrnice o data retention z důvodu, že tato směrnice byla v rozporu s Listinou základních práv EU. Konkrétně podle Soudního dvora EU unijní zákonodárce překročil přijetím směrnice o data retention meze, jež ukládá požadavek na dodržování zásady proporcionality z hlediska článků 7 a 8 a čl. 52 odst. 1 Listiny základních rpáv EU (bod 69). SDEU byl v projednávaných věcech požádán ze strany ústavních soudů Irska (Highcourt) a Rakouska (Verfassungsgerichtshof) o rozhodnutí o dvou sadách předběžných otázek týkajících se posouzení platnosti směrnice 2006/24/ES.

Pokud jde o uchovávání provozních a lokalizačních údajů, tak toto SDEU označil za velmi vážný zásah do práva na ochranu soukromí, přičemž toto **sledování u lidí vytváří oprávněný pocit, že jsou pod konstantním dohledem** (bod 37). Z dat lze zjistit velmi podrobné informace o každodenním soukromém životě, místech pobytu, či sociálních vztazích sledovaných osob (bod 27). Sledování se týká celé evropské populace, přičemž míra využívání prostředků elektronické komunikace roste, čímž **roste i dopad do základních práv lidí** (bod 56). Uchovávání údajů požadované směrnicí na druhou stranu podle Soudního dvora není takové povahy, aby nepříznivě ovlivnilo samu podstatu základních práv na respektování soukromého života a právo na ochranu osobních údajů (bod 39). SDEU přiznává, že uchovávání dat sleduje účel veřejného zájmu, kterým je stíhání závažných zločinů a boj proti terorismu (bod 44).

SDEU konstatuje, že zásah do práva na ochranu soukromí a ochranu osobních údajů musí být v souladu s konstantní judikaturou omezen na nezbytné minimum (bod 52). Dále dovozuje, že v daném případě tomu tak není a směrnice tyto limity neobsahuje.

SDEU uvádí v bodě 58, že napadená směrnice se „*týká globálně všech osob, které využívají služeb elektronických komunikací, aniž se však osoby, jejichž údaje jsou uchovávány, nachází byť nepřímo v situaci, která může vést k trestnímu stíhání. Vztahuje se tedy i na osoby, v jejichž případě neexistuje žádný důvod se domnívat, že by jejich chování mohlo byť nepřímo nebo vzdáleně souviset se závažnou trestnou činností*." SDEU zde upozorňuje i na to, že jsou uchovávány i údaje o komunikaci osob, které mají ze zákona **zachovávat profesní tajemství**, jako jsou advokáti, poskytovatelé zdravotních nebo sociálních služeb apod. V bodě 59 pak na toto soud navazuje: „*Uvedená směrnice, jejímž cílem je přispět k boji proti závažné trestné činnosti, dále nevyžaduje žádnou souvislost mezi údaji, jejichž uchovávání je stanoveno, a ohrožením veřejné bezpečnosti a zejména se neomezuje na uchovávání údajů vztahujících se buď k určitému časovému období*

[5] Dostupné zde: http://curia.europa.eu/juris/liste.jsf?num=C-293/12&language=cs

či určité zeměpisné oblasti či okruhu určitých osob, které mohou být jakýmkoli způsobem zapojeny do závažné trestné činnosti, anebo k osobám, které by prostřednictvím uchovávání jejich údajů mohly z jiných důvodů přispívat k předcházení, odhalování nebo stíhání závažných trestných činů."

SDEU v této formulované první výtce proti směrnici tedy říká, že **plošné a nevýběrové uchovávání údajů je nepřijatelné, protože neminimalizuje zásah do základních práv**. Plošnost tohoto zásahu nezohledňuje žádné souvislosti mezi uchovávanými údaji a účelem směrnice, tedy bojem proti závažné kriminalitě. SDEU v bodě 59 naznačuje, že pokud by k uchovávání mělo docházet, mělo by být **vázáno na určité rizikové faktory a omezeno buď časově, místně nebo co do okruhu sledovaných osob**. SDEU tak odmítá stávající koncept plošného a nevýběrového sledování komunikace celé populace bez jakéhokoli časového nebo místního omezení.

Členské státy, včetně České republiky, odmítaly i po tomto rozhodnutí SDEU od plošného sběru údajů upustit a právní základ plošného sběru dat nově spatřovaly v čl. 15 odst. 1 e-privacy směrnice, který zakotvuje možnost členských států přijmout právní úpravu omezující práva vyplývající ze směrnice včetně práva na zachování důvěrnosti komunikace mimo jiné z důvodu zajištění bezpečnosti a pro prevenci či odhalování trestné činnosti. To ovšem pouze v případě, pokud je to v demokratické společnosti nezbytné, přiměřené a úměrné.

Právě k souladu principu plošného uchovávání provozních a lokalizačních údajů se vyjádřil SDEU v dalším rozhodnutí ve spojených věcech **C 203/15 a C 698/15 ze dne 21. 12. 2016 (dále jen „rozhodnutí Tele2/Watson")[6],** kde SDEU konstatuje, že uvedený čl. 15 odst. 1 e-privacy směrnice musí být vykládán tak, že **brání vnitrostátní právní úpravě zavést plošné a nerozlišující uchovávání provozních a lokalizačních údajů všech účastníků**. SDEU konstatoval, že uvedený článek směrnice umožňuje členským státům omezit dosah základních povinnosti, podle které musí být zajištěna důvěrnost osobních údajů a souvisejících provozních údajů. Toto omezení ale musí být vykládáno striktně a takovým ustanovením tak nelze odůvodnit, aby se výjimka stala pravidlem. (bod 89) Vnitrostátní právní úprava, která stanoví plošné a nerozlišující uchovávání veškerých provozních a lokalizačních údajů všech účastníků a registrovaných uživatelů, které se vztahuje na veškeré prostředky elektronické komunikace, a ukládá poskytovatelům služeb elektronických komunikací povinnost uchovávat tyto údaje systematicky a průběžně bez jakékoli výjimky, představuje zásah do základních práv zakotvených v článcích 7 a 8 Listiny základních práv EU, který je třeba považovat za zvlášť

[6] Dostupné zde: http://curia.europa.eu/juris/document/document.jsf?docid=186492&doclang=CS

závažný.(body 97 a 100) Skutečnost, že uživatelé jsou pod neustálým dohledem pak má vliv i na výkon svobody projevu, kterou zaručuje čl. 11 Listiny základních práv EU. (bod 101)

Jako problematické SDEU uvádí, že **plošné a nevýběrové shromažďování údajů představuje pravidlo a nikoli výjimku z pravidla důvěrnosti informací**. Vztahuje se na osoby, u nichž neexistuje důvod se domnívat, že by jejich chování mohlo, byť nepřímo nebo vzdáleně, souviset se závažnou trestnou činností, stejně jako na osoby, jejichž činnost je dle vnitrostátního práva předmětem profesního tajemství. Stejně jako v bodě 59 předchozího rozhodnutí SDEU považuje za problematické, že uchovávání údajů se neomezuje na případy omezené časově, zeměpisně nebo okruhem osob, které mohou být jakýmkoli způsobem zapojeny do trestné činnosti. Taková vnitrostátní právní úprava pak „*překračuje meze toho, co je naprosto nezbytné a nelze ji v demokratické společnosti považovat za odůvodněnou*“. (bod 107)

S ohledem na výše uvedené v závěru SDEU konstatuje, že čl. 15 odst. 1 e-privacy směrnice ve spojení s čl. 7, 8, 11 a čl. 52 odst. 1 Listiny základních práv EU musí být vykládán v tom smyslu, že brání vnitrostátní právní úpravě, která za účelem boje proti trestné činnosti stanoví plošné a nerozlišující uchovávání veškerých provozních a lokalizačních údajů všech účastníků a registrovaných uživatelů, které se vztahují na veškeré prostředky elektronické komunikace. (bod 112)

Kromě výše uvedeného odsudku principu plošného uchovávání dat SDEU rovněž hodnotil podmínky přístupu k těmto údajům, přičemž konstatoval, že by tento **přístup měl být možný výlučně za účelem boje proti závažné trestné činnosti** a přístup by měl být podmíněn **přezkumem soudního** nebo nezávislého správního orgánu, jakož by mělo být i zajištěno, aby údaje byly uchovávány na území EU. (bod 125)

Navrhovatelé mají za to, že je třeba výše zmíněnou judikaturu Soudního dvora Evropské unie, která ještě nebyla známa v době vydání prvních nálezů Ústavního soudu ve věcech sp. zn. Pl. ÚS 24/10 a sp. zn. Pl. ÚS 24/11 zohlednit zejména při hodnocení ústavní konformity samotného principu plošného a nevýběrového shromažďování a uchovávání provozních a lokalizačních údajů a navázat tak na zpochybnění tohoto principu v rámci obiter dictum nálezu sp. zn. Pl. ÚS 24/10, neboť Listina základních práv a svobod a Listina základních práv EU vycházejí z hodnotově shodných základů a judikatura SDEU je tak relevantním zdrojem pro posouzení ústavní konformity i předpisů vnitrostátních.

VII.
Podrobné odůvodnění

Mezi podstatné náležitosti demokratického právního státu při hodnocení konfliktů základních práv a veřejných zájmů bezpochyby patří zásada uvedená v hlavě I. Listiny, čl. 4 odst. 4, a to **zásada proporcionality**, která se vztahuje na zákonná omezení základních práv a svobod, dle které *„Při používání ustanovení o mezích základních práv a svobod musí být šetřeno jejich podstaty a smyslu. Taková omezení nesmějí být zneužívána k jiným účelům, než pro které byla stanovena.“* Napadená ustanovení dle navrhovatelů představují zásah do uvedených základních práv, který není v souladu s čl. 4 Listiny, a který lze proto považovat za **ohrožení podstatných náležitosti demokratického právního státu**.

Jak konstatoval Ústavní soud v nálezu ve věci sp. zn. Pl. ÚS 24/10, tak *„zásah do základního práva jednotlivce na soukromí v podobě práva na informační sebeurčení ve smyslu čl. 10 odst. 3 a čl. 13 Listiny z důvodu prevence a ochrany před trestnou činností je tak možný jen skrze imperativní zákonnou úpravu, která musí především odpovídat nárokům plynoucím z principu právního státu a která naplňuje požadavky vyplývající z testu proporcionality, kdy v případech střetů základních práv či svobod s veřejným zájmem, resp. s jinými základními právy či svobodami je třeba posuzovat účel (cíl) takového zásahu ve vztahu k použitým prostředkům, přičemž měřítkem pro toto posouzení je zásada proporcionality (v širším smyslu). Taková právní úprava musí být přesná a 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, aby případně mohli upravit své chování tak, aby se nedostali do konfliktu s omezující normou. Rovněž musí být striktně definovány i pravomoci udělené příslušným orgánům, způsob a pravidla jejich provádění tak, aby jednotlivcům byla poskytnuta ochrana proti svévolnému zasahování. Posouzení přípustnosti daného zásahu z hlediska zásady proporcionality (v širším smyslu) pak zahrnuje tři kritéria. Prvním z nich je posouzení způsobilosti naplnění účelu (nebo také vhodnosti), přičemž je zjišťováno, zda je konkrétní opatření vůbec schopno dosáhnout zamýšleného cíle, jímž je ochrana jiného základního práva nebo veřejného statku. Dále se pak jedná o posouzení potřebnosti, v němž je zkoumáno, zda byl při výběru prostředků použit ten prostředek, který je k základnímu právu nejšetrnější. A konečně je zkoumána přiměřenost (v užším smyslu), tj., zda újma na základním právu není nepřiměřená ve vazbě na zamýšlený cíl, tzn. že opatření omezující základní lidská práva a svobody nesmějí, jde-li o kolizi základního práva či svobody s veřejným zájmem, svými negativními důsledky převyšovat pozitiva, která představuje veřejný zájem na těchto opatřeních.“*

VII.1

Vhodnost právní úpravy

V prvním kroku testu proporcionality je třeba posuzovat **způsobilost k naplnění účelu**, tedy je zjišťováno, zda konkrétní opatření je vůbec způsobilé daný účel naplnit.

Účel uchovávání těchto údajů ve vztahu ke konkrétním činnostem orgánů oprávněných tyto údaje vyžadovat nevyplývá z textu napadených ustanovení zákona o elektronických komunikacích, ani z Vyhlášky, ale ze zvláštních zákonů, které upravují oprávnění těchto orgánů. Obecně lze říci, že údaje mají sloužit ke zvýšení efektivity činnosti těchto orgánů.

V případě oprávnění orgánů činných v trestním řízení, které vyplývá z § 88a TŘ je účelem uchovávání dat možnost jejich **vyžádání a využití v rámci trestních řízení** vedených pro okruh trestných činů definovaných v § 88a TŘ. V případě dalších oprávnění Policie ČR je účelem možné využití údajů pro účely **zahájeného pátrání po konkrétní hledané nebo pohřešované osobě** a za účelem **zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly** (§ 68 odst. 2 PolZ) či pro **účely předcházení a odhalování konkrétních hrozeb v oblasti terorismu** (§ 71 PolZ) či **prověřování chráněné osoby** a při splnění podmínek stanovených zvláštním právním předpisem (§ 10a zákona č. 137/2001 Sb., o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízením a o změně zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů).

V případě Bezpečností informační služby a Vojenského zpravodajství je účel možno dovodit z ustanovení § 8a zákona č.154/1994 Sb., o Bezpečnostní informační službě, ve znění pozdějších předpisů (dále jen „ZoBIS“) a z § 8a zákona č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů (dále jen „ZoVZ“)., kde je shodně řečeno, že údaje lze vyžadovat v rozsahu pro **plnění konkrétního úkolu, myšleno úkolu patřícího do působnosti těchto zpravodajských služeb** dle § 5 zákona č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů (dále jen „ZoZS“).

V posledním případě České národní banky je pak účelem uchovávání zajištění možnosti vyžádání údajů pro účelu zajištění dohledu nad kapitálovým trhem dle § 8 odst. 1 písm. d) zákona č. 15/1998 Sb., o **dohledu v oblasti kapitálového trhu** o změně a doplnění dalších zákonů (dále jen „ZDKT“).

Z výše uvedeného je zřejmé, že **vymezení účelů, pro něž jsou údaje uchovávány je velmi široké**. V některých případech (např. oprávnění ČNB či Policie ČR dle § 68 PolZ) pak je minimálně sporné, zda vůbec stanovené účely mohou odpovídat účelům stanoveným v čl. 15 odst. 1 e-privacy směrnice, kde je řečeno, že

porušení tajemství dopravovaných zpráv národní legislativou je možné pouze, pokud je to nezbytné, přiměřené a úměrné opatření pro zajištění národní bezpečnosti (tj. bezpečnosti státu), obrany, veřejné bezpečnosti a pro prevenci, vyšetřování, odhalování a stíhání trestných činů.

Stávající systém uchovávání provozních a lokalizačních údajů je nastaven tak, že jsou uchovávány údaje definované v prováděcí Vyhlášce, a to o všech provedených komunikacích, které spadají do dané kategorie. Údaje jsou následně **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 **kontakty, činnost, případně pohyb** tohoto konkrétního uživatele (jeho telefonu, počítače apod.) nebo tyto údaje nezná, disponuje ale informacemi, kde se zájmový uživatel pohyboval, případně kde došlo k trestnému činu. V těchto případech se oprávněný orgán zajímá zejména o údaje z jednotlivých **stanic BTS**, které určí například jaké mobilní telefony se v danou chvíli k dané buňce připojovaly.[7]

Teoreticky platí, že uchovávané údaje v případě jejich vyžádání mohou posloužil k naplňování stanovených účelů. V trestních řízeních může jít o zvýšení možností při objasňování trestné činnosti atd. Problémem nicméně je, že na to, o jak masivní nástroj sledování jde a jak masivním způsobem jsou údaje vyžadovány, tak zároveň není zřejmé, že by došlo ke zlepšení stavu.

Většina států se podle názoru Evropské komise, které Komise shrnula pro Evropský parlament v Hodnotící zprávě o směrnici o uchovávání údajů (směrnice 2006/24/ES) z 18. 4. 2011[8], shodla, že využívání provozních a lokalizačních údajů je potřebné při odhalování trestné činnosti. Jak ale poukázal **Evropský inspektor osobních údajů**, tak se k otázce této potřebnosti vyjádřilo pouze 9 států z 27 a interpretovat jejich pohled jako názor většiny států je tedy chybné.[9] Státy, které se k potřebnosti data retention vyjádřily uvedly konkrétní případy, kdy byly údaje využity a přispěly k vyšetření trestného činu. Zároveň konstatovaly, že v řadě případů došlo k vyloučení podezření ze spáchání trestného činu, aniž by musely být využity invazivnější zásahy do soukromí, jako domovní prohlídky nebo odposlechy. **Prezentovány ze strany členských států byly nicméně zejména případy, kdy provozní a lokalizační údaje byly důležité při objasnění trestné činnosti, spíše než o případy, kdy jejich využití bylo pro vyšetření daného trestných činů nezbytné** a nenahraditelné a

[7] K tomu viz Jan Vobořil: Data retention (nejen) v policejní praxi, Analýza postupů Policie ČR a dalších orgánů při vyžadování a využívání provozních a lokalizačních údajů o elektronických komunikacích v České republice, Praha 2012, dostupné zde: http://www.slidilove.cz/sites/default/files/dr-analyza-final2.pdf

[8] Hodnotící zpráva o směrnici o uchovávání údajů (2006/24/ES), Brusel 18.4.2011, dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:CS:PDF

[9] Stanovisko evropského inspektora ochrany údajů k Hodnotící zprávě Komise Radě a Evropskému parlamentu o směrnici o uchovávání údajů (směrnice 2006/24/ES) , Brusel 31.5.2011, s. 8, dostupné zde: https://edps.europa.eu/sites/edp/files/publication/11-05-30_evaluation_report_drd_cs.pdf

mohlo tak jedině splňovat zásadu proporcionality zásahu do práva na soukromí. Na možnost zaměnění této dvojí role provozních a lokalizačních údajů upozornila v předvečer zveřejnění zprávy Komise ve své stínové zprávě nevládní organizace EDRi[10] nebo ve svém Stanovisku Evropský inspektor osobních údajů Peter Hustinx.

Statistiky trestné činnosti navíc dokládají, že využívání provozních a lokalizačních údajů nemělo na snížení míry kriminality nebo na zvýšení její objasněnosti zásadní vliv. Za příklad lze vzít využívání údajů ze statistik Policie ČR týkajících se trestních řízení, což je jednoznačně dominantní oblast, v níž jsou provozní a lokalizační údaje využívány. **Z čísel o množství a objasněnosti trestných činů je zřejmé, že to, zda údaje byly nebo nebyly plošně uchovávány, nemělo prakticky vliv ani na množství trestných činů, ani na jejich objasněnost**. Z následující tabulky, která vychází z policejních statistik za roky 2011, 2012 a 2013 je zřejmé, že ačkoli v roce 2012, kdy po většinu roku neplatila povinnost operátorů uchovávat provozní a lokalizační údaje v důsledku nálezu ÚS sp. zn. 24/10 Sb. **došlo k významnému poklesu žádostí o tyto údaje, tak se to nijak neodrazilo v množství trestných činů ani v jejich objasněnosti zejména v porovnání s rokem 2013, kdy po celý rok trvala znovuzavedená povinnost uchovávat provozní a lokalizační údaje a počet žádostí stoupl na více než pětinásobek**.

Počty trestných činů, jejich objasněnost ve vztahu k počtu žádostí o provozní a lokalizační údaje v letech 2011 - 2013

Rok	Počet trestných činů	Počet objasněných TČ	Počet žádostí o údaje dle § 88a TŘ
2011	**317 177**	**122 238**	43 976
2012	**304 528**	**120 168**	9 946
2013	**325 366**	**129 181**	54 560

Zdroj: Policie ČR: Statistiky kriminality za roky 2011-2013[11], Policie ČR: Analýzy odposlechů a sledování osob a věcí dle trestního řádu za roky 2011-2013[12]

[10] EDRi, Shadow evaluation report on the Data Retention Directive (2006/24/EC), Brusel 17. 4. 2011, s. 11, dostupné z: http://www.edri.org/files/shadow_drd_report_110417.pdf

[11] Statistiky jsou dostupné zde: http://www.policie.cz/statistiky-kriminalita.aspx

[12] Analýzy jsou dostupné zde: http://www.mvcr.cz/clanek/analyza-odposlechu-a-sledovani-osob-a-veci-dle-trestniho-radu-za-rok-2011.aspx,http://www.mvcr.cz/clanek/analyza-odposlechu-a-sledovani-osob-a-veci-dle-trestniho-radu-za-rok-2012.aspx, http://1url.cz/ht0CN

Obdobné závěry lze vysledovat i ze **statistik Spolkového úřadu vyšetřování SRN**, které ukazují, že po zavedení plošného uchovávání provozních a lokalizačních údajů rovněž nedošlo k pozitivním změnám v úrovni kriminality či její objasněnosti. Z dat je zřejmé, že po zavedení plošného sledování komunikace v letech 2008 a 2009 nedošlo k poklesu míry kriminality u závažných trestných činů a dokonce lehce poklesla jejich objasněnost.[13] Na nedostatečnost důkazů prokazujících přínosy data retention poukázal Evropský inspektor ochrany údajů ve svém kritickém vyjádření k evaluační zprávě Komise.[14]

Přínosem provozních a lokalizačních údajů pro míru objasněnosti trestných činů se v roce 2011 zabýval rovněž v kriminologické studii „Schutzlücken durch Wegfall der Vorratsdatenspeicherung?" Institutu Maxe Plancka pro zahraniční a mezinárodní trestní právo.[15] Z klíčových pasážích na str. 218 a následujících studie vyplývá mimo jiné, že pokud jde o **závažné trestné činy, ale i trestné činy, které lze nazvat kyberkriminalitou, tak nejsou prokazatelné žádné změny pokud jde o míru objasněnosti trestných činů** mezi lety, kdy byla data plošně uchovávána a kdy k plošnému uchovávání nedocházelo.

Z výše uvedeného lze dovodit, že uchovávané provozní a lokalizační údaje jsou sice při vyšetřování trestné činnosti hojně využívány, ale toto nemá vliv na množství trestných činů či míru jejich objasněnosti. Policie tak byla zjevně i v období, kdy neplatila pro operátory povinnost data plošně uchovávat, schopna vyšetřovat trestné činy stejně efektivně a **chybějící důkazy v podobě výpisů provozních a lokalizačních údajů tak byla zjevně schopna nahradit důkazy jinými.**

Malý dopad na objasněnost trestných činů i míru kriminality lze přičíst i možnosti obcházení plošného sledování pomocí různých nástrojů. **Paradoxně potom oprávněné orgány často nemají k dispozici relevantní údaje, protože osoby, které například páchají závažnou trestnou činnost, mají vyšší motivaci k využití těchto mechanismů zajišťujících důvěrnost komunikace, než běžná populace, která se ničeho protiprávního nedopouští, ale jejíž komunikace je plošně uchovávána**.

Vedle služeb elektronických komunikací lze dnes komunikovat i prostřednictvím různých služeb vymezených v zákoně č. 480/2004, o některých službách informační společnosti. Může jít například o komunikaci prostřednictvím **sociálních sítí**, běžných **šifrovaných komunikačních aplikací**, jako je například WhatsApp nebo Signal. Zmínit je třeba také využití **předplacených telefonních služeb a anonymních SIM karet**, které neumožňují přímouidentifikaci osoby. Navíc v kriminální praxi jsou předplacená čísla často měněna. Tento

[13] Dostupné z: http://www.vorratsdatenspeicherung.de/images/schaubilder_wirksamkeit_vorratsdatenspeicherung_2011-01-26.pdf
[14] Stanovisko evropského inspektora ochrany údajů k Hodnotící zprávě Komise Radě a Evropskému parlamentu o směrnici o uchovávání údajů (směrnice 2006/24/ES) , Brusel 31.5.2011, s. 9
[15] Studie je dostupná zde: https://www.mpg.de/5000721/vorratsdatenspeicherung.pdf

případ zmiňuje v obiter dictum rovněž Ústavní soud v nálezu sp. zn. Pl. ÚS 24/10. Další možností je anonymizace komunikace prostřednictvím **proxy serverů** (využití prostředníka mezi klientem a cílovým počítačem, vůči němuž vystupuje sám jako klient), systému **TOR** (umožňuje šifrovaný přenos dat prostřednictvím sítě routerů, kde je odesílatel prakticky nedohledatelný) apod.

Pokud tedy cílem takto plošného uchovávání údajů mělo být zefektivnění boje se závažnou kriminalitou, tak k tomuto cíli zavedení takto invazivního nástroje zjevně nevedlo. **Uvedený nástroj se tedy nejeví jako vhodný pro naplnění stanoveného účelu vyšetřování závažné trestné činnosti.**

VII.2

Potřebnost a přiměřenost právní úpravy uchovávání údajů

Druhým stupněm testu proporcionality je otázka potřebnosti. V tomto kroku je zkoumáno, zda byl při výběru prostředků použit takový prostředek, který je k základnímu právu nejšetrnější. Třetím stupněm testu je potom zkoumání přiměřenosti v užším slova smyslu, tedy otázky, zda újma na základním právu není nepřiměřená ve vazbě na zamýšlený cíl.

V dané problematice je **nezbytné oddělit dva aspekty problému spojeného se shromažďováním a dalším využíváním provozních a lokalizačních údajů**, ačkoli jsou oba úzce provázány. Jednak jde o otázku ústavnosti samotného **shromažďování a následného uchovávání údajů**, jehož pravidla jsou upravena v napadených ustanovení zákona o elektronických komunikacích a ve Vyhlášce. Druhým aspektem je pak **vyžadování a využívání těchto údajů** ze strany oprávněných orgánů, což je materie upravená zejména ve zvláštních zákonech, jako je trestní řád, pro orgány činné v trestním řízení, ale i zákon o Policii ČR pro jiná oprávnění policie, zákony upravující činnost zpravodajských služeb, či zákon o dohledu v oblasti kapitálového trhu upravující oprávnění České národní banky.

Navrhovatelé se domnívají, že **hlavním problémem, který vede k neústavnosti napadené právní úpravy je právě samotné plošné a nevýběrové shromažďování provozních a lokalizačních údajů**, které se týká všech osob, neboť v současném světě je prakticky nemožné fungovat a udržovat sociální vztahy bez interakce s dalšími lidmi prostřednictvím nástrojů elektronické komunikace. V této souvislosti je vhodné ocitovat z prejudikaturního nálezu sp.zn. Pl. ÚS 24/10, kde Ústavní soud shrnul význam práva na respekt k soukromému životu zejména pokud jde o právo na informační sebeurčení a konstatoval, že ačkoli nejsou shromažďovány obsahy komunikace, tak zásah do těchto práv je v případě provozních a lokalizačních údajů obdobný.

Ústavní soud ve zmíněném nálezu uvádí: *„primární funkcí práva na respekt k soukromému životu je zajistit prostor pro rozvoj a seberealizaci individuální osobnosti… právo na soukromí garantuje rovněž právo jednotlivce rozhodnout podle vlastního uvážení zda, popř. v jakém rozsahu, jakým způsobem a za jakých okolností mají být skutečnosti a informace z jeho osobního soukromí zpřístupněny jiným subjektům. Jde o aspekt práva na soukromí v podobě práva na informační sebeurčení, výslovně garantovaný čl. 10 odst. 3 Listiny.*

Právo na informační sebeurčení je tak nezbytnou podmínkou nejen pro svobodný rozvoj a seberealizaci jednotlivce ve společnosti, nýbrž i pro ustavení svobodného a demokratického komunikačního řádu. Zjednodušeně řečeno, v podmínkách vševědoucího a všudypřítomného státu a veřejné moci se svoboda projevu, právo na soukromí a právo svobodné volby chování a konání stávají prakticky neexistujícími a iluzorními.

Ačkoliv se stanovená povinnost uchovávat provozní a lokalizační údaje nevztahuje na obsahy jednotlivých sdělení, tak z uvedených údajů o uživatelích, adresátech, přesných časech, datech, místech a formách telekomunikačních spojení, budou-li sledovány po delší časový úsek, lze v jejich kombinaci sestavit detailní informace o společenské nebo politické příslušnosti, jakož i o osobních zálibách, sklonech nebo slabostech jednotlivých osob“.

Tento názor koresponduje jak s konstantní judikaturou Ústavního soudu, tak i s výše uvedenými rozhodnutími Soudního dvora Evropské unie, či s judikaturou **Evropského soudu pro lidská práva**, kde z klíčových judikátů lze zmínit zejména rozhodnutí ve věci Amann v. Švýcarsko ze dne 16. 2. 2000, Leander v. Švédsko ze dne 26. 3. 1987, Kopp v. Švýcarsko ze dne 25. 3. 1998 či Copland v. Spojené království ze dne 3. 4. 2007, v nichž bylo konstatováno porušení čl. 8 Úmluvy o ochraně lidských práv a základních svobod a bylo judikováno, že **již samotné uchovávání údajů týkajících se soukromého života jednotlivce je zásahem do práva dle č. 8 Úmluvy**, bez ohledu na to, zda k těmto údajům měl někdo přístup nebo byly jinak využity. Podobně jako Ústavní soud hodnotil i Evropský soud pro lidská práva **uchovávání informací o uskutečněné komunikaci na roveň uchovávání obsahu komunikace** (viz Amann v. Švýcarsko či Copland v. Spojené království).

Jak vyplývá z judikatury Evropského soudu pro lidská práva například ve věci Kruslin v. Francie, Huvig v. Francie ze dne 24. 4. 1990 či Zakharov proti Rusku ze dne 4. 12. 2015 tak jedním ze základních požadavků ESLP vyvinutých výkladem podmínky zákonného podkladu státních zásahů do soukromého života je **předvídatelnost a dostupnost tohoto zákonného podkladu**. Důvodem je legitimní a logický požadavek, aby

lidé znali předem okolnosti, kdy stát může výjimečně do jejich soukromého života zasáhnout, a mohli přizpůsobit své jednání tak, aby se tomuto vyhnuli. **Plošný charakter uchovávání provozních a lokalizačních údajů však možnost reálné volby osob omezuje až vylučuje**, protože základní lidská potřeba, tedy komunikovat mezi sebou, která se v dnešní době převážně realizuje prostřednictvím nástrojů elektronické komunikace, je podrobena plošnému sledování bez ohledu na další okolnosti, jako je například relevance údajů pro trestní vyšetřování.

Jak konstatoval Soudní dvůr Evropské unie, tak míra sledování dosahuje takové intenzity, že je možno dokonce dojít k závěru, že může mít vliv na využívání prostředků elektronické komunikace, a v důsledku toho **na výkon svobody projevu** zaručenou v čl. 11 Listiny základních práv EU ze strany uživatelů těchto prostředků.[16]

Soudní dvůr Evropské unie proto v rozhodnutí Digital Rights Ireland i Tele2/Watson konstatoval nepřijatelnost principu plošného uchovávání údajů, když kritizoval, že se uvedený princip neomezuje na uchovávání údajů vztahujících se buď k určitému časovému období či určité zeměpisné oblasti či okruhu určitých osob, které mohou být jakýmkoli způsobem zapojeny do závažné trestné činnosti.

Dále je třeba upozornit, že plošné sledování provozních a lokalizačních údajů vede fakticky nejen ke sledování interakce mezi lidmi, ale i **fyzického pohybu jednotlivců**. Od rozhodování Ústavního soudu v roce 2011 se výrazně zvýšilo využívání datových služeb v mobilních telefonech, které umožňují získat mnohem ucelenější a komplexnější přehled o pohybu osob vzhledem k připojování mobilních telefonů s datovým připojením k základnovým stanicím. Fakticky tak p**ři využívání nástrojů elektronické komunikace dnes vzniká násobně více údajů, než tomu bylo v roce 2011**. Pro představu, jak komplexní může být sledování pohybu je vhodné se seznámit s dvěma případy osob, které si vyžádali lokalizační údaje, které na základě napadené právní úpravy o nich operátoři uchovávají, a následně získané údaje zveřejnili. V prvním případě tak učinil německý poslanec Malte Spitz a závěry včetně vizualizace jsou shrnuty v článku z roku 2011 na internetovém serveru Zeit Online[17], v druhém případě pak o totéž požádal český novinář Jan Cibulka a podobnou vizualizaci pak uveřejnil na serveru iHned v roce 2013.[18]

Dalším problematickým aspektem je skutečnost, že údaje jsou uchovávány **i o komunikaci osob, které jsou vázány z různých důvodů povinností mlčenlivosti.** Což vede k ohrožení profesního tajemství. Týká se to jak advokátů tak např. sociálních pracovníků či různých poradců (po telefonu, anonymní poradny pro

[16] Rozhodnutí SDEU ve spojených věcech C 203/15 a C 698/15 ze dne 21. 12. 2016, bod 101
[17] Dostupné zde: http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz
[18] Dostupné zde: https://ihned.cz/c3-59259950-000000_d-59259950-data-retention-zivot-v-zaznamech-mobilniho-operatora

alkoholiky, manželské poradny, poradny pro HIV pozitivní, těhotenské poradny, krizové linky, atd.), lékařů a psychoterapeutů nebo novinářů (právo na ochranu zdroje). Uchovávání a možné využívání provozních a lokalizačních údajů o jejich telekomunikaci je přímo limituje ve výkonu jejich povolání, čímž vedle práva na ochranu soukromí či informačního sebeurčení může docházet i **k zásahům do svobody projevu.**

Plošné uchovávání údajů s sebou nese i značná **rizika jejich zneužití**, a to ať už ze strany třetích osob, které například neoprávněně získají přístup k údajům uchovávaným operátory, tak ze strany státu, operátorů či jejich zaměstnanců. V této souvislosti je možné zmínit několik případů zneužití takto uchovávaných údajů. V **České republice došlo k neoprávněnému vyžádání osobních údajů desítek osob, zejména politiků nebo podnikatelů, včetně předsedy Ústavního soudu nebo osob z okolí prezidenta republiky, příslušníkem cizinecké policie v roce 2011**.[19] Podobně o rok později byla obviněna elitní policistka ÚOOZ, protože si neoprávněně opatřovala provozní a lokalizační údaje osob konkurujících bezpečnostní agentuře ABL.[20] V Polsku policie a tajné služby **neoprávněně vyžadovaly údaje o telekomunikaci nezávislých žurnalistů**.[21] V Německu neoprávněně v**yužíval uchovávané údaje o desítkách osob Deutsche Telekom**.[22] Na možnost zneužití lokalizačních údajů ukazuje případ z Běloruska, kdy si policie od operátorů vyžádala výpis z BTS stanic v místě protivládních demonstrací a takto **zjišťovala totožnost osob, které se těchto demonstrací účastnily** a následně byly vyšetřovány.[23] Na řadu nových rizik spojených s uchováváním údajů a nejednotnost přijatých opatření pro zabezpečení údajů upozornila například pracovní skupina pro ochranu údajů WP 29. Řada bezpečnostních děr byla odhalena například u malých providerů. WP 29 upozornila také na nebezpečí využívání údajů poskytovateli pro další invazivnější účely.[24]

Je třeba zdůraznit, že přestože Ústavní soud kritizoval nedostatečné požadavky na zabezpečení uchovávaných údajů zejména pokud jde o zamezení přístupu třetích osob, zabezpečení celistvosti a důvěrnosti údajů, jakož i procesu jejich ničení, tak **legislativní změny přijaté v reakci na rozhodnutí Ústavního soudu otázky zabezpečení dat nijak neřešily**, takže situace se nezměnila. Zejména pak nejsou

[19]Policista nelegálně sháněl výpisy mobilů, špehoval i Rychetského, iDnes 18.6.2011, dostupné z: http://zpravy.idnes.cz/policista-nelegalne-shanel-vypisy-mobilu-spehoval-i-rychetskeho-phy-/krimi.aspx?c=A110617_225431_krimi_abr
[20] Inspekce odhalila další policisty, kteří nelegálně odposlouchávali, iDnes 12. 3. 2012, dostupné zde: https://zpravy.idnes.cz/inspekce-odhalila-dalsi-policisty-kteri-nelegalne-odposlouchavali-1fq-/domaci.aspx?c=A120311_210203_domaci_brm
[21]Arbeitskreis Vorratsdatenspeicherung, There is no such things as secure data, s.32, dostupné z: http://wiki.vorratsdatenspeicherung.de/images/Heft_-_es_gibt_keine_sicheren_daten_en.pdf
[22]Evropská komise, Hodnotící zpráva o směrnici o uchovávání údajů (2006/24/ES), Brusel 18.4.2011, s. 26
[23]Dostupné zde: http://charter97.org/en/news/2011/1/12/35161/
[24]WP29, Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive, Brusel 13.7.2010, s. 11, dostupné zde: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf

data dostatečně zabezpečena proti jejich využívání ze strany operátorů i k jiným účelům, než je jejich uchovávání pro potřeby oprávněných orgánů, například k marketingovým účelům.

Pro hodnocení přiměřenosti plošného uchovávání údajů je vhodné rovněž upozornit na **možné alternativy**, které se uplatňují například ve státech, v nichž došlo ke zrušení plošného uchovávání těchto dat a nebyla přijata nová právní úprava, která by operátorům ukládala tuto povinnost. Možnost využívání provozní a lokalizační údaje se zde obvykle opírá o data, která jsou operátory uchovávána za účelem vyúčtování služeb, případně jako doplněk je zde upravena možnost tzv. **quick freeze**, tedy operativní zabránění likvidaci určitého druhu údajů např. o konkrétních osobách. Přičemž tato data jsou následně využitelná při trestních vyšetřováních. Toto se týká v rámci EU zejména pěti států, v nichž došlo ke zrušení právní úpravy plošného a nevýběrového uchovávání provozních a lokalizačních údajů ze strany ústavních soudu, a zároveň nebyla přijata nová právní úprava, která by ho opět zaváděla.[25]

Příkladem je například **Slovensko**. Zde v dubnu 2015 zrušil slovenský Ústavní soud nálezem sp. zn. Pl. ÚS 10/14 národní úpravu data retention v reakci na derogaci směrnice o data retention.[26] Nová právní úprava plošného uchovávání dat zde přijata nebyla a platí tak zde quick freeze systém, neboli zajišťování údajů, jehož postup je upraven v § 63 odst. 5 – 8 Zákona č. 351/2011 Z. z., o elektronických komunikaciách. Zajišťování údajů se liší od uchovávání údajů zejména tím, že při něm nejsou uchovávány plošně údaje o veškeré komunikaci, ale jsou uchovávány pouze údaje o komunikaci podezřelých osob, které jsou vyžádány ze strany oprávněných orgánů a se souhlasem soudu. Uchovávání tak začíná až ve chvíli, kdy o toto požádá oprávněný orgán, podobně jako je tomu například u odposlechů, případně lze vyžádat i údaje uchovávané operátory za účelem vyúčtování služeb. Podobně v **Rakousku** ústavní soud zrušil v roce 2014 národní právní úpravu. V současné době je zde připravován quick freeze systém, kde by byla možnost, aby státní zástupce zažádal v souvislosti s podezřením o další uchovávání některých dat, kterými operátoři disponují v souvislosti se zajištěním poskytování služeb, tato data by pak mohla být uchovávána ze strany operátorů až po dobu 12 měsíců a sloužit pro účely vyšetřování.[27] Podobně ani v **Nizozemsku** v současné době není účinný žádný zákon, který by upravoval povinné uchovávání provozních a lokalizačních údajů. Původní národní úprava byla

[25] K tomu viz Eurojust, Data retention regimes in Europe in light of the CJEU ruling of 21 December 2016 in Joined Cases C-203/15 and C-698/15, 7. 11. 2017, s. 6, dostupné zde: http://statewatch.org/news/2017/nov/eu-eurojust-data-retention-MS-report-10098-17.pdf

[26] Dostupné zde: http://www.eisionline.org/images/Data_retention_rozhodnutie_PL_US_10_2014.pdf

[27] Privacy International, National Data Retention Laws since the CJEU's Tele-2/Watson Judgment, September 2017, s. 15n., dostupné zde: https://privacyinternational.org/sites/default/files/Data%20Retention_2017.pdf

zrušena v roce 2015 v reakci na zrušení data retention směrnice.[28] Dalším případem je pak **Slovinsko**, kde došlo v roce 2014 ke zrušení národní právní úrpavy data retention a data jsou tam dnes uchovávána pouze za účelem, v rozsahu a po dobu nezbytnou pro vyúčtování služeb.[29] Pětici států, kde v současné době nefunguje plošný sběr dat potom uzavírá rumunko, kde došlo ke zrušení národní právní úpravy rovněž v roce 2011.

Za méně invazivní alternativu, byť z hlediska navrhovatelů i tak za nevyhovující, lze považovat například i kratší dobu uchovávání provozních a lokalizačních údajů. To je případ **Německa**, kde rovněž došlo v roce 2011 ke zrušení národní úpravy data retention. Nová právní úprava zde vstoupila v účinnost až po více než šesti letech v červenci 2017.[30] Na rozdíl od české právní úpravy jsou zde podstatně kratší doby uchovávání dat, kdy lokalizační dat se uchovávají 4 týdny, provozní data potom 10 týdnů. V České republice se shodně jedná o 6 měsíců.

Přestože ve většině členských států EU je stále princip plošného sběru provozních a lokalizačních údajů uplatňován, tak Česká republika je dle aktuální zprávy Eurojustu jednou z pouhých čtyř zemí, v nichž neprobíhají a ani nejsou plánovány ze strany vlád žádné změny v reakci na judikaturu Soudního dvora EU.[31]

VII.3

Potřebnost a přiměřenost právní úpravy využívání údajů

Vedle otázky uchovávání údajů je dále třeba posuzovat i potřebnost a přiměřenost právní úpravy využívání údajů. Navrhovatelé mají předně za to, že v řadě aspektů stávající právní **úprava nenaplňuje požadavky formulované ze strany Ústavního soudu v nálezu sp. zn. Pl. ÚS 24/10**. Předně je třeba konstatovat, že u napadených ustanovení **§ 68 odst. 2 a § 71 písm. a) PolZ není upravena nezávislá kontrola ze strany soudní moci**. K žádosti o provozní a lokalizační údaje tak policejní orgán nepotřebuje souhlas soudu, což zvyšuje riziko zneužití údajů či nadužívání žádostí. Přitom požadavek na soudní přezkum žádostí o poskytnutí dat je jedním z klíčových bodů relevantní judikatury a soudní přezkum se objevuje u všech dalších oprávněných orgánů. Jak konstatoval Ústavní soud v nálezu ve věci sp. zn. Pl. ÚS 24/10 (bod 36) s odkazem na ustálenou judikaturu: *„K omezení osobní integrity a soukromí osob (tj. k prolomení respektu k nim) tak ze*

[28] Privacy International, National Data Retention Laws since the CJEU's Tele-2/Watson Judgment, September 2017, s. 30, dostupné zde: https://privacyinternational.org/sites/default/files/Data%20Retention_2017.pdf
[29] Privacy International, National Data Retention Laws since the CJEU's Tele-2/Watson Judgment, September 2017, s. 36, dostupné zde: https://privacyinternational.org/sites/default/files/Data%20Retention_2017.pdf
[30] Privacy International, National Data Retention Laws since the CJEU's Tele-2/Watson Judgment, September 2017, s. 23, dostupné zde: https://privacyinternational.org/sites/default/files/Data%20Retention_2017.pdf
[31] Eurojust, Data retention regimes in Europe in light of the CJEU ruling of 21 December 2016 in Joined Cases C-203/15 and C-698/15, 7. 11. 2017, s. 9, dostupné zde: http://statewatch.org/news/2017/nov/eu-eurojust-data-retention-MS-report-10098-17.pdf

strany veřejné moci může dojít jen zcela výjimečně, 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. Esenciální předpoklady spravedlivého procesu totiž vyžadují, aby byl jednotlivec vybaven dostatečnými garancemi a zárukami proti možnému zneužití pravomoci ze strany veřejné moci. Ony ***nezbytné záruky sestávají z odpovídající právní úpravy a z existence účinné kontroly jejich dodržování, kterou představuje především kontrola těch nejintenzivnějších zásahů do základních práv a svobod jednotlivců nezávislým a nestranným soudem****, neboť je povinností soudů poskytovat ochranu základním právům a svobodám jednotlivců*."

Podobně i Soudní dvůr EU rozhodl ve výrokovém bodě 2 rozhodnutí Tele 2/Watson takto*: „Článek 15 odst. 1 směrnice 2002/58, ve znění směrnice 2009/136, ve spojení s články 7, 8, 11 a čl. 52 odst. 1 Listiny základních práv, musí být vykládán v tom smyslu, že brání vnitrostátní právní úpravě, která upravuje ochranu a bezpečnost provozních a lokalizačních údajů, zejména přístup příslušných vnitrostátních orgánů k uchovávaným údajům, a která v rámci boje proti trestné činnosti neomezuje tento přístup tak, aby byl umožněn výlučně pro účely boje proti závažné trestné činnosti, a nepodmiňuje* ***tento přístup předchozím přezkumem ze strany soudu nebo nezávislého správního orgánu****, a která nevyžaduje, aby dotčené údaje byly uchovávány na území Unie."*

Vedle chybějící předběžné soudní kontroly je nezbytné zdůraznit, že **PolZ neukládá policii ani povinnost následného informování o vyžádání si údajů o konkrétní osobě**, která je v případě trestního řádu upravena v § 88a odst. 2 trestního řádu. PolZ umožňuje sice získat informace o zpracovávaných osobních údajích na základě písemné žádosti dle § 83 PolZ, nicméně jednak je zde upravena řada výjimek, kdy se informace neposkytují a zároveň k podání takové žádosti sledovaná osoba nemá důvod, pokud se nedozví o tom, že její údaje byly ze strany policie využívány.

Z toho důvodu je vedle úpravy plošného sběru a uchovávání dat navrhováno i zrušení zmíněných ustanovení PolZ.

Dalším důležitým aspektem je otázka **zajištění vyžadování provozních a lokalizačních údajů** pouze v případech, kdy je to nezbytné a nelze stanoveného účelu docílit jinak. K vyžadování údajů a tím i k prolamování práva na soukromí a informačním sebeurčení by se mělo v souladu s nálezem sp. zn. Pl. ÚS 24/10 sahat "*jen zcela výjimečně, 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*." Ačkoli v důsledku tohoto nálezu Ústavního soudu byla do ustanovení § 88a

trestního řádu zařazeno omezení trestných činů v souvislosti s jejichž vyšetřováním je možno o údaje žádat, jakož i podmínka vyžadování dat pouze v případech "nelze-li sledovaného účelu dosáhnout jinak nebo bylo-li by jinak jeho dosažení podstatně ztížené", je **z počtu žádostí o provozní a lokalizační údaje, že zejména posuzování nezbytnosti podání žádosti o výpisy dat není v praxi respektováno** a k vyžadování dat dochází v obrovském množství případů. Zásada omezení využívání těchto údajů na nezbytné případy se pak **nijak nepromítá v právní úpravě oprávnění policie využívat data mimo trestní řízení či v oprávnění zrpavodajských služeb**.

Jestliže ve svém nálezu sp. zn. Pl ÚS 24/10 konstatoval Ústavní soud jako důkaz nadužívání žádostí o provozní a lokalizační údaje, že v roce 2008 bylo ze strany oprávněných orgánů dle statistik, kterými disponovala Evropská komise na základě hlášení Českého telekomunikačního úřadu, který shromažďoval údaje od operátorů, zažádáno o údaje v **131 560** případech, tak je nezbytné zdůraznit, že počet žádostí dle hlášení ČTÚ se od té doby zvedl několikanásobně, navzdory omezením v trestním řádu. **V roce 2016 bylo kladně vyřízeno celkem 487 289 žádostí, z nichž drtivá část se týkala mobilních telefonů**. Toto byl zároveň i rekordní nárůst oproti roku 2015, kdy bylo kladně vyřízeno "pouze" 230 124 žádostí.[32]

Ústavní soud ve svých nálezech týkajících se uchovávání a využívání provozních a lokalizačních údajů v trestním řízení dále vyslovil požadavek, aby údaje byly využívány v obdobném režimu jako jsou nařizovány odposlechy. Využití údajů by tak mělo být dle Ústavního soudu možné pouze v případech „**zvlášť závažných trestných činů"**. Vzhledem k tomu, že Ústavní soud například v nálezu sp. zn. Pl. ÚS 24/10 **přímo odkazuje na úpravu odposlechů** (bod 48), je dle navrhovatelů nezbytné tento pojem „zvlášť závažné trestné činy" vykládat právě v souvislosti s úpravou odposlechů v § 88 TŘ. **Je zřejmé, že zákonodárce při přípravě nové právní úpravy nerespektoval toto vymezení přípustnosti zásahu do práva na informační sebeurčení v případě žádostí orgánů činných v trestním řízení o provozní a lokalizační údaje**, když odposlechy dle § 88 je možné nařídit v případech trestných činů s horní hranicí minimálně 8 let a dalších uvedených trestných činů, zatímco provozní a lokalizační údaje lze vyžadovat u trestných činů s horní hranicí trestní sazby 3 roky a dalších vymezených trestných činů včetně například hojného trestného činu podvodu dle § 209, kde je horní hranice základní trestní sazby v odst. 1 dva roky. Navrhovatelé mají za to, že uvedená úprava neodpovídá požadavkům formulovaným ze strany Ústavního soudu a je tedy rovněž v rozporu s Listinou.

[32] Tisková zpráva ČTÚ: Případů provozních a lokalizačních údajů předaných operátory na žádost oprávněných orgánů meziročně přibylo, 9. 3. 2017, dostupné zde: https://www.ctu.cz/tiskova-zprava-pripadu-provoznich-lokalizacnich-udaju-predanych-operatory-na-zadost-opravnenych

Je tedy zřejmé, že údaje jsou zejména v trestním řízení vyžadovány zcela rutinně. Navrhovatelé mají za to, že stávající právní úprava **zjevně neposkytuje efektivní záruku toho, aby nedocházelo k nadužívání žádostí o provozní a lokalizační údaje.** Absenci dostatečné právní úpravy, jež je ve smyslu ustanovení čl. 4 odst. 2 Listiny předpokladem omezení základních práv a svobod v obecné rovině, přitom nelze nahradit ani soudním přezkumem (k tomu viz Nález ÚS ve věci sp. zn. Pl. ÚS 24/11) a **dle navrhovatelů nelze tento problém vyřešit ani ústavně konformním výkladem. Proto je dle navrhovatelů na místě zrušit i napadené ustanovení § 88a TŘ.**

VIII.

Shrnutí

Uchovávání a následné plošné a nevýběrové využívání provozních a lokalizačních údajů je s rozvojem elektronických komunikací a zejména využívání datových služeb **stále masivnějším zásahem do práva na soukromí** i práva na informační sebeurčení. Tento masivní nástroj na jedné straně shromažďuje data o všech, kteří komunikují, včetně například osob, které jsou ze zákona povinny dodržovat **profesní tajemství**, na druhé straně je ale **možno tento invazivní nástroj obcházet**, což vede k tomu, že nemíří na ty, kvůli nimž byl zaveden, tedy zejména osoby dopouštějící se závažné trestné činnosti. Přestože je tento nástroj masivně využíván a jen v roce 2016 bylo o údaje zažádáno téměř v 500 000 případech, tak například využívání provozních a lokalizačních údajů v trestních řízeních **nevedlo ani k poklesu kriminality, ani ke zvýšení její objasněnosti**. Policie i v době, kdy neplatila povinnost data uchovávat byla schopna vyšetřovat trestné činy se stejnou úspěšností a chybějící údaje tak byla schopna nahrazovat jinými důkazy.

Napadená ustanovení nereflektují judikaturu, která se týká dané problematiky, ať už jde o **nálezy Ústavního soudu** nebo o **rozhodnutí Soudního dvora EU**, který označil **samotný princip plošného uchovávání dat za nepřijatelný**. Pokud jde o otázku využívání údajů, tak ačkoli došlo v důsledku nálezů Ústavního soudu vztahujících se k dané problematice k částečné novelizaci napadených ustanovení, tak lze konstatovat, že **nebyly reflektovány všechny výtky, které Ústavní soud k napadeným ustanovením měl** (chybějící soudní přezkum v PolZ, právní úprava, která nebrání nadužívání údajů ze strany oprávněných orgánů, neprovedení změn týkajících se zabezpečení údajů).

Shromažďování a využívání provozních a lokalizačních údajů o telekomunikačním provozu je tedy z výše zmíněných důvodů **v rozporu s čl. 7 odst. 1, čl. 10 odst. 2 a 3 a čl. 13 Listiny, jakož i čl. 8 EÚLP.**

IX.

Návrh

Na základě výše uvedených skutečností navrhovatelé navrhují, aby Ústavní soud vydal podle ustanovení § 70 odst. 1 zákona č. 182/1993 Sb., o Ústavním soudu, ve znění pozdějších předpisů, nález,

1. **kterým se § 97 odst. 3 a 4 zákona č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, zrušuje.**
2. **kterým se § 68 odst. 2 a § 71 písm. a) zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů, zrušují.**
3. **kterým se § 88a zákona č. 141/1961 Sb., trestního řádu, ve znění pozdějších předpisů, zrušuje.**
4. **kterým se vyhláška č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů, zrušuje.**

Jan Vobořil, advokát

jako právní zástupce navrhovatele – skupiny poslanců