SLOVENSKÁ REPUBLIKA

NÁLEZ

Ústavného súdu Slovenskej republiky

V mene Slovenskej republiky

PL. ÚS 10/2014-78

Ústavný súd Slovenskej republiky na neverejnom zasadnutí 29. apríla 2015 v pléne zloženom z predsedníčky Ivetty Macejkovej a zo sudcov Jany Baricovej (sudkyňa spravodajkyňa), Petra Brňáka, Ľubomíra Dobríka, Sergeja Kohuta, Milana Ľalíka, Lajosa Mészárosa, Marianny Mochnáčovej a Rudolfa Tkáčika prerokoval návrh skupiny 31 poslancov Národnej rady Slovenskej republiky, zastúpených poslancom Národnej rady Slovenskej republiky Martinom Poliačikom, na začatie konania o súlade § 58 ods. 5 až 7 a § 63 ods. 6 zákona č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov, § 116 zákona č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov a § 76a ods. 3 zákona Národnej rady Slovenskej republiky č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov s čl. 13 ods. 4, čl. 16 ods. 1, čl. 19 ods. 2 a 3, čl. 22 a čl. 26 Ústavy Slovenskej republiky, čl. 7 ods. 1, čl. 10 ods. 2 a 3, čl. 13 a čl. 17 Listiny základných práv a slobôd, čl. 8 a čl. 10 Dohovoru o ochrane ľudských práv a základných slobôd a čl. 7, čl. 8, čl. 11 a čl. 52 ods. 1 Charty základných práv Európskej únie a takto

r o z h o d o l :

1. Ustanovenia § 58 ods. 5 až 7 a § 63 ods. 6 zákona č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov, § 116 zákona č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov a § 76a ods. 3 zákona Národnej rady Slovenskej republiky č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov n i e s ú v súlade s čl. 13 ods. 4, čl. 16 ods. 1, čl. 19 ods. 2 a 3 a čl. 22 Ústavy Slovenskej republiky, čl. 7 ods. 1, čl. 10 ods. 2 a 3 a čl. 13 Listiny základných práv a slobôd a čl. 8 Dohovoru o ochrane ľudských práv a základných slobôd.

2. Vo zvyšnej časti návrhu n e v y h o v u j e .

O d ô v o d n e n i e :

I.

1. Ústavnému súdu Slovenskej republiky (ďalej len „ústavný súd“) bol 10. októbra 2012 doručený návrh skupiny 31 poslancov Národnej rady Slovenskej republiky (ďalej len „skupina poslancov“ alebo „navrhovatelia“) na začatie konania podľa čl. 125 ods. 1 písm. a) Ústavy Slovenskej republiky (ďalej len „ústava“) o súlade § 58 ods. 5 až 7 a § 63 ods. 6 zákona č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov (ďalej len „zákon o elektronických komunikáciách“), § 116 zákona č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov (ďalej len „Trestný poriadok“) a § 76a ods. 3 zákona Národnej rady Slovenskej republiky č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov (ďalej len „zákon o Policajnom zbore“) s čl. 13 ods. 4, čl. 16 ods. 1, čl. 19 ods. 2 a 3, čl. 22 a čl. 26 ústavy, čl. 7 ods. 1, čl. 10 ods. 2 a 3, čl. 13 a čl. 17 Listiny základných práv a slobôd (ďalej len „listina“), čl. 8 a čl. 10 Dohovoru o ochrane ľudských práv a základných slobôd (ďalej len „dohovor“) a čl. 7, čl. 8, čl. 11 a čl. 52 ods. 1 Charty základných práv Európskej únie (ďalej len „charta“).

I.1 Odôvodnenie návrhu skupiny poslancov

2. V úvodnej časti svojho návrhu skupina poslancov uvádza, že napadnuté ustanovenia zákona o elektronických komunikáciách ukladajú poskytovateľom elektronických komunikácií povinnosť uchovávať prevádzkové údaje, lokalizačné údaje a údaje komunikujúcich strán odo dňa uskutočnenia komunikácie počas 6 mesiacov, ak ide o pripojenie k internetu, internetovú elektronickú poštu a telefonovanie prostredníctvom internetu, a počas 12 mesiacov, ak ide o ostatné druhy komunikácie. Poukazujú, že predmetom uchovávania je niekoľko desiatok údajov, ktoré príloha č. 2 zákona o elektronických komunikáciách pre ich nepreberné množstvo ďalej rozdeľuje do kategórií identifikácia zdroja komunikácie; identifikácia adresáta komunikácie; identifikácia dátumu, času a trvania komunikácie; identifikácia typu komunikácie; identifikácia použitého komunikačného zariadenia a identifikácia polohy komunikujúceho. V rovnakom rozsahu majú poskytovatelia elektronických komunikácií uchovávať aj údaje súvisiace s neúspešnými pokusmi o volanie.

3. Podľa názoru skupiny poslancov *„zavedenie povinnosti uchovávať údaje podľa vyššie uvedených ustanovení predstavuje citeľný zásah do súkromného života, keďže ide o plošne sledovanie všetkých obyvateľov Slovenska, bez ohľadu na ich bezúhonnosť a čestnosť. Každý deň je o každom obyvateľovi Slovenska povinne zaznamenané to s kým telefonoval, komu posielal textové správy a emaily, kedy tak urobil, kde sa vtedy nachádzal, aký telefón alebo službu použil, ako dlho trvala predmetná komunikácia a mnoho ďalších. Kombináciou týchto informácií dokážeme opísať pohyb každého obyvateľa na Slovensku, ktorý používa mobilný telefón či internet, predpovedať jeho správanie, okruh známych, záľuby, zdravotný stav, sexualitu, či iné osobné údaje a tajomstvá... Na základe údajov, ktoré sa takto uchovávajú, je možné zostaviť dokonalý osobnostný, komunikačný a pohybový profil jednotlivca, odhaľujúci radu podstatných charakteristík jeho identity a chovania, inými slovami odhaľujú podstatnú časť jeho súkromia.“*.

4. Vo svojom návrhu skupina poslancov ďalej poukazuje na skutočnosť, že *„ako zásah do súkromného života je podľa judikatúry ESĽP potrebné chápať ako kontrolu obsahu*

pošty a telefónnych hovorov (Rozsudok ESĽP vo veci Klaas proti Nemecku), tak aj zisťovanie telefónnych čísel telefonujúcich osôb, či uchovávanie informácií, že daná osoba telefonovala s určitou osobou. Nie je pri tom rozhodujúce, či uchovávané údaje boli nejakým spôsobom použité alebo zverejnené (najmä Rozsudok ESĽP vo veci Copland proti Spojenému kráľovstvu). Zásahom do základných práv, a teda aj do súkromného života, sa rozumie nie len bezprostredný zásah (napr. oboznámenie sa s uchovávanými údajmi), ale aj také opatrenia štátnych orgánov, z ktorých možno predvídať, že ich následkom bude obmedzenie základných práv a slobôd.“.

5. V súvislosti so zásahom napadnutých ustanovení zákona o elektronických komunikáciách do práva na súkromie skupina poslancov vo svojom návrhu uvádza, že *„uchovávanie údajov po dobu 6, resp. 12, mesiacov znamená latentné nebezpečenstvo ďalších bezprostredných zásahov štátnych orgánov. Navyše, štát neuchováva prevádzkové a lokalizačné údaje sám, ale používa k tomu súkromné osoby poskytujúce telekomunikačné služby, pričom riziko možného zneužitia uchovávaných údajov je vyššie ako pri ich uchovávaní štátom, a to v dôsledku veľkého počtu súkromných osôb poskytujúcich telekomunikačné služby, a taktiež väčšieho počtu zamestnancov týchto súkromných osôb, ktorí prichádzajú do styku s uchovávanými údajmi... Preventívne plošné uchovávanie telekomunikačných údajov predstavuje vážny zásah, resp. obmedzenie základných práv.“. Skupina poslancov ďalej dodáva, že „z ústavného poriadku plynie, že k obmedzeniu osobnej integrity a súkromia (t. j. k prelomeniu ochrany) môže zo strany verejnej moci dôjsť iba celkom výnimočne, a to iba vtedy, keď je to nevyhnutné a účel sledovaného verejného záujmu nemožno dosiahnuť inak. Pri nedodržaní niektorej podmienky ide o zásah, ktorý je protiústavný. Zásah do súkromia je teda v zásade obmedzený predovšetkým nevyhnutnosťou takéhoto postupu. K tomu, aby neboli prekročené medze nevyhnutnosti, musí existovať systém adekvátnych a dostatočných záruk skladajúci sa z tomu zodpovedajúcich právnych predpisov a účinnej kontroly ich dodržiavania. Skryté sledovanie orgánmi verejnej moci, s ohľadom na vyššie uvedené základné právo na ochranu súkromia, je preto možné vždy iba v legitímnom záujme a na základe zákona.“.*

6. Podľa navrhovateľov sú napadnuté ustanovenia zákona o elektronických komunikáciách *„v priamom rozpore so zásadou, že pri obmedzovaní základných práv a slobôd sa musí dbať na ich podstatu a zmysel, pričom obmedzenia možno použiť len na ustanovený cieľ (čl. 13 ods. 4 Ústavy)“*. Ďalej konštatujú, že *„opodstatnenosť každého zásahu do základných práv a slobôd sa v demokratickom a právnom štáte posudzuje na základe kumulatívneho splnenia troch základných kritérií, a to legality, legitimity a proporcionality takéhoto zásahu (Nálezy Ústavného súdu SR, sp. zn. I. ÚS 117/07, PL. ÚS 23/06, PL. ÚS 3/09, PL. ÚS 3/00, PL. ÚS 67/07)“*.

7. Skupina poslancov v podanom návrhu tvrdí, že napadnutá právna úprava ohrozuje samotnú podstatu *„práva na nedotknuteľnosť súkromia, súkromný život, ochranu pred neoprávneným zhromažďovaním údajov o svojej osobe a tajomstva dopravovaných správ“*. V návrhu skupina poslancov uvádza, že príslušné základné práva jednotlivca prostredníctvom napadnutej právnej úpravy štát obmedzuje spôsobom, ktorý *„najmä ohrozuje ich samotnú podstatu“*, keďže *„podľa posledných výskumov Inštitútu Maxa Plancka totiž zbieranie týchto údajov nemá žiadny pozitívny vplyv na odhaľovanie závažných trestných činov v Európe“*.

8. Skupina poslancov v návrhu konštatuje, že *„obmedzenie, ktoré znamená zásah do určitého práva, musí byť vždy primerané vzhľadom k významu tohto práva. Zásah je prípustný, len ak je to v demokratickej spoločnosti nevyhnutné v záujme dosiahnutia legitímneho cieľa... Obmedzenie základných práv je teda prípustné iba vtedy, pokiaľ je to k dosiahnutiu zamýšľaného cieľa vhodné a nevyhnutné, a s tým spojený zásah nie je vzhľadom na svoju intenzitu v nepomere k významu veci a ujme, ktorú spôsobí dotknutým osobám.“*.

9. V návrhu navrhovatelia podrobujú napadnuté ustanovenia zákona o elektronických komunikáciách testu proporcionality.

10. Pokiaľ ide o existenciu legálneho cieľa, ktorým možno odôvodniť zásah do základného práva, v návrhu skupina poslancov konštatuje: *„Uchovávaním údajov štát*

sleduje cieľ, ktorým je zaistenie národnej bezpečnosti, obrany a verejnej bezpečností. Úprava teda sleduje spoločenský významný cieľ.“

11. Pokiaľ ide o posúdenie vhodnosti napadnutej právnej úpravy na dosiahnutie sledovaného cieľa, navrhovatelia v návrhu uvádzajú: *„... sme presvedčení, že od predmetných údajov nemožno očakávať dlhodobý a pozitívny vplyv na zníženie kriminality a zvýšenie bezpečnosti v spoločnosti. Existuje totiž viacero spôsobov, ako sa vyhnúť uchovávaniu dát. Stačí si zvoliť iný spôsob komunikácie, ktorý nie je štátom zatiaľ monitorovaný.“ Ďalej navrhovatelia uvádzajú: «Vzhľadom na vymedzenie, resp. nevymedzenie pojmov „internetová elektronická pošta“ a „telefonovanie prostredníctvom internetu“ nebudú osobitne uchovávané údaje pri požití napr.: blogu, sociálnych sieti (napr. Facebook), webov umožňujúcich zdieľanie videí (napr. Youtube), rýchlych správ (IM), IRC (Internet relay chat), peer-to-peer (P2P) komunikácie, nakoľko tieto nepoužívajú protokoly predpokladané ZoEK, resp. šifrujú komunikáciu.»*

12. Vo svojom návrhu skupina poslancov uvádza aj ďalšie spôsoby, akými sa možno vyhnúť uchovávaniu údajov, v dôsledku čoho napadnutá právna úprava zákona o elektronických komunikáciách nemôže byť spôsobilá dosahovať zamýšľaný cieľ boja proti závažnej trestnej činnosti. Sú nimi napríklad *„... použitie telefónnej búdky alebo tzv. anonymných predplatených telefónnych kariet. Ide o také karty, pri kúpe ktorých nie je nevyhnutné preukazovať svoju totožnosť.“*. V návrhu skupina poslancov tiež uvádza: *„Vyhnúť sa uchovávaniu možno aj oveľa sofistikovanejším spôsobom, a to použitím komerčných služieb na anonymizáciu komunikácie alebo systému The Onion Rouler (TOR), či systému JAP (JonDo). Komerčné služby na anonymizáciu komunikácie sú založené prevažne na systéme proxy serverov.“* Napokon dodáva: *„Vzhľadom na množstvo uvedených, ale aj ďalších spôsobov, akými sa možno vyhnúť uchovávaniu údajov, je zrejme, že právna úprava nemôže dosahovať svoj cieľ, a to boj proti organizovanému zločinu a terorizmu, nakoľko práve tieto osoby najlepšie poznajú spôsoby ako sa takémuto uchovávaniu údajov efektívne vyhnúť. Zásah do súkromia sa tak paradoxne viac dotkne osôb, ktoré s trestnou činnosťou nemajú nič spoločné, ako osôb, ktoré ju páchajú a majú*

zvýšený záujem komunikovať anonymne. Tieto osoby totiž nemajú dôvod meniť svoje osobné návyky, keďže sú čestnými a bezúhonnými občanmi...“

13. Skupina poslancov v návrhu rovnako spochybňuje aj nevyhnutnosť napadnutej právnej úpravy pre dosiahnutie cieľa. Jej nevyhnutnosť spochybňujú navrhovatelia vzhľadom na súčasné štúdie, predovšetkým kriminologickú štúdiu Inštitútu Maxa Plancka *„Stutzlücken durch Wegfall der Vorratsdatenspeicherung?“ (Kriminologická štúdia Stutzlücken durch Wegfall der Vorratsdatenspeicherung* - http://vds.brauchts.net/MPI_VDS_Studie.pdf*)*, ktorá poukazuje na to, že zbieranie prevádzkových a lokalizačných údajov *„vôbec nevedie k lepšiemu odhaľovaniu závažnej trestnej činnosti“*, a to napríklad z dôvodu rozsahu dnes uchovávaných údajov či doby, po ktorú sa údaje majú uchovávať, ako aj z dôvodu existencie menej invazívnych, ale rovnocenne efektívnych spôsobov boja proti závažnej kriminalite (ako napr. § 90 Trestného poriadku).

14. V súvislosti s porovnaním miery zásahov do ústavou chránených hodnôt vyvolaných uplatnením napadnutej právnej úpravy navrhovatelia uvádzajú: „Závažnosť a rozsah zásahu je nutné posudzovať podľa toho, koľko a ktorí nositelia základných práv ním budú dotknutí a v akej intenzite. Intenzita zásahu závisí okrem iného od druhu, rozsahu a zamýšľaného použitia uchovávaných údajov. Pri zisťovaní možností použitia uchovaných údajov je treba zohľadniť aké negatívne dôsledky hrozia dotknutým osobám alebo akých sa môžu dôvodne obávať. Ďalej je dôležité posúdiť využiteľnosť a použiteľnosť údajov, a to najmä s ohľadom na skutočnosť, že získané údaje môžu byť kombinované s ďalšími údajmi, čím môžu byť získavané kvalitatívne hodnotnejšie údaje.

Pri posudzovaní závažnosti zásahu do práva na súkromie je nutné sa predovšetkým zaoberať tým, do akej miery je možná identifikácia alebo zachovanie anonymity dotknutej osoby s ohľadom na uchovávané údaje. Vzhľadom na to, že majú slúžiť hlavne na vyšetrovanie, odhaľovanie a stíhanie taxatívne vymenovaných trestných činov, nemožno predpokladať anonymitu týchto údajov, v opačnom prípade by uchovávanie nemalo v podstate žiaden zmysel.

Často sa uvádza, že uchovávanie toľko prevádzkových a lokalizačných údajov nepredstavuje tak vážny zásah do základných práv a slobôd ako prípadné uchovávanie obsahu telekomunikácie. Správnosť tohto tvrdenia však nemožno posudzovať iba podľa druhu uchovávaných údajov, ale i z hľadiska ich užitočnosti a ich možného použitia. To súvisí jednak s účelom ich uchovávania a ďalej aj s možnosťou ich spracovania a prepojenia s ďalšími údajmi. V konkrétnom prípade môže byť tak zásah do súkromia závažnejší pokiaľ pôjde o uchovávanie a využívanie prevádzkových a lokalizačných údajov, ako keby šlo o uchovávania obsahu komunikácie (porovnaj bod 27, Pl. ÚS 42/11, ÚS ČR). Ako príklad možno uviesť telefonát medzi dvoma osobami, ktorý nie je obsahovo dôležitý, avšak o súkromí týchto osôb nám môžu viac povedať údaje z hľadiska miesta, doby uskutočneného hovoru a identifikácie telefonujúcich osôb, ako z hľadiska predmetu samotného hovoru.

Ukladanie, triedenie a vyhodnocovanie prevádzkových a lokalizačných údajov a ich spájanie s ďalšími informáciami je možné vykonávať automaticky s pomocou vyhľadávača. Čo zvyšuje riziko zneužitia a závažnosť dopadu spracovania týchto údajov na súkromie jednotlivca.

Z vyššie uvedeného vyplýva, že hodnota informácií získaných na základe prevádzkových a lokalizačných údajov môže byť porovnateľná s hodnotou informácií získaných z obsahu komunikácie, ba niekedy môže byť dokonca aj vyššia. Z toho môžeme vyvodiť, že prevádzkové a lokalizačné údaje je potrebne chrániť rovnako dobre ako údaje o obsahu komunikácie.

Pri pospájaní jednotlivých uchovávaných údajov a pri spojení týchto údajov s ďalšími informáciami môžeme odhaliť podstatnú časť súkromia dotknutej osoby. Umožni to odhaliť kontakty dotknutej osoby. Na základe toho, ako často dotknutá osoba komunikuje s inými ľuďmi, je možné zostaviť sieť jej priateľov alebo aj jej pracovných vzťahov. Ak dotknutá osoba často volá s inou osobou počas určitého kratšieho časového obdobia môže to znamenať relatívnu dôležitosť volaného pre volajúceho. V rade prípadov sa dá z identity adresáta telefonátu alebo emailu odhaliť citlivý údaj o volajúcom či odosielateľovi. Ak je adresátom telefonátu lekár - špecialista, tak sa dá predpokladať, že volajúci bude mať zrejme zdravotný problém z oblasti, ktorej sa daný špecialista venuje. Taktiež pri emaily,

ktorého adresátom je niekto@anonymny-alkoholici.sk sa dá predpokladať, že dotyčný je alkoholik. Pri použití mobilného telefónu je zas možné zistiť napr. miesta pobytu a pohybu, kto sa kde a kedy s niekým stretol. Ak dvaja ľudia, ktorí medzi sebou zvyčajne komunikujú z určitej geografickej oblasti zrazu na pár dní zmenia oblasť, z ktorej zvyčajne komunikujú, tak sa dá predpokladať, že išli na dovolenku alebo na pracovnú cestu.“

15. Vyššiu mieru intenzity zásahu do práva na súkromie skupina poslancov vo svojom návrhu odôvodňuje aj rozsahom okruhu osôb, voči ktorým sa povinnosť uchovávať údaje vzťahuje. *„Z okruhu osôb, ktorých údaje sú takto preventívne uchovávané, nie sú dokonca vylúčené ani osoby, ktoré sú inak viazané povinnosťou mlčanlivosti (napr. advokáti, lekári). Z prevádzkových a lokalizačných údajov je totiž veľmi jednoduché zistiť množstvo údajov, ktoré inak podliehajú prísnej dôvernosti, ako napr. zoznamy klientov/pacientov určitého advokáta/lekára, či frekvenciu a intenzitu ich kontaktu. Ako sme už vyššie spomenuli, oproti iným inštitútom, nie sú z okruhu osôb, o ktorých sú údaje takto preventívne zbierané, dokonca vylúčené ani osoby, ktoré sú inak viazané povinnosťou mlčanlivosti (napr. advokáti, lekári), alebo ktoré nemožno sledovať alebo odpočúvať, ak vykonávajú určitú činnosť (vzťah obhajca a advokát). Vzniká teda absurdná situácia, a síce, že fyzicky sledovať (§ 113 ods. 3 TP) a odpočúvať (§ 115 ods. 1 TP) komunikáciu obvineného so svojím obhajcom nemožno, žiadne ustanovenie však nezakazuje použitie rovnakých informácií získaných na základe plošného monitoringu. Hoci všetky inštitúty rovnako „sledujú" predmetnú komunikáciu obvineného so svojím obhajcom.“*

16. Podľa navrhovateľov *„To, že uchovávanie údajov vnímajú aj ľudia ako výrazný zásah do práva na súkromný život dokazujú aj zahraničné prieskumy. Takéto zásahy do súkromia sú mimoriadne závažné, pretože jednotlivec nepredstavuje žiadnu charakteristiku odôvodňujúcu takýto zásah a pretože, aj keď sa správa zákonným spôsobom, môže byť zastrašený z dôvodu rizika zneužitia a z dôvodu pocitu, že je pod dohľadom (rozhodnutie nemeckého spolkového Ústavného súdu, sp. zn. 1 BvR 518/02, bod 117).“*.

17. Skupina poslancov vo svojom návrhu rovnako poukazuje, že napadnuté ustanovenia zákona o elektronických komunikáciách zasahujú aj do slobody prejavu a slobody tlače, *„... keďže novinári nemajú možnosť používať internetovú alebo telefónnu komunikáciu pri svojej práci bez toho, aby tak ohrozili svoje tajné zdroje, ktorých existencia vitálne podporuje obe tieto slobody. Každá priama komunikácia s takouto osobou, alebo všetka komunikácia súvisiaca s takýmito stretnutiami (napr. prezvonenie tesne pred, či po tajnom stretnutí odhaľujúce polohu stretnutia) spôsobuje, že novinár si musí nachádzať úplne odlišné spôsoby komunikácie. To iste platí aj pre iné profesie, ktoré sa musia vyhýbať elektronickej komunikácií, ak chcú v skutočnosti zachovať tajnosť svojho klienta (psychológovia, manželský poradcovia, psychoterapeuti, alkoholické liečebne a pod).“*.

18. Skupina poslancov napadnutej právnej úprave napokon vytýka neexistenciu adekvátnych a dostatočných záruk proti zneužitiu uchovávaných údajov a vo svojom návrhu ďalej uvádza: „Pokiaľ ide o bezpečnosť údajov, zákonodarca musí stanoviť vysoký štandard bezpečnosti, ktorý bude zodpovedať aktuálnemu stavu poznatkov na tomto úseku a nebude určovaný vlastným uvážením súkromných poskytovateľov, ktorí budú zohľadňovať predovšetkým ekonomické hľadisko.

Zákonodarca síce stanovil bezpečnostné opatrenia v § 64 ZoEK, avšak iba veľmi všeobecne a konkrétne opatrenia ponecháva na poskytovateľov. Pritom ak zoberieme do úvahy to, že zo strany štátu nie je poskytovaná žiadna finančná kompenzácia za uchovávanie údajov, tak potom dôjdeme k záveru, že podniky, ktoré sa snažia minimalizovať svoje náklady, nebudú chcieť a ani nebudú môcť urobiť dostatočné bezpečnostné opatrenia, ktoré sú dosť finančne náročné (porovnaj ústavnosť kompenzácie v prípade odpočúvania, Nález, sp. zn. PL ÚS 23/06). Navyše, k zneužitiu uchovávaných údajov môže dôjsť aj samotným poskytovateľom a to najmä za účelom marketingu svojich služieb.“

19. Podľa skupiny poslancov *„Zabezpečenie osobných údajov je všade v Európe problematické a úniky týchto údajov sú veľmi časté, Podľa spoločnosti Ponemon Institute, ktorá urobila výskum v 785 britských spoločnostiach zameraných na informačné*

technológie, priznalo celých 55 % týchto spoločností stratu údajov, 49 % z nich zaznamenalo viac ako dva prípady počas posledných dvoch rokov. Pri veľkom množstve spoločností zabezpečujúcich telekomunikáciu (najmä v prípade internetu) sa nedá očakávať u každého z nich zodpovedajúce zabezpečenia prevádzkových a lokalizačných údajov. V konečnom dôsledku by najefektívnejšou ochranou proti možnému zneužitiu údajov bolo, keby sa tieto údaje vôbec neuchovávali.“.

20. Záruky proti zneužitiu uchovávaných údajov je podľa skupiny poslancov potrebné posudzovať *«... nielen z hľadiska technických požiadaviek bezpečnosti, ale aj z hľadiska právnej „bezpečnosti“, a teda, či je na sprístupnenie takýchto údajov potrebný súdny príkaz vydaný v súlade s účelom uchovávania údajov a či sa pri uchovávaní a použití údajov zachováva transparentnosť».*

21. Skupina poslancov dodáva: *„Súdny príkaz je síce potrebný na sprístupnenie údajov, avšak je otázne, či je vydávaný na účely ustanovené v § 58 ods. 7 ZEK, nakoľko v § 116 TP, je ustanovené, že súdny príkaz možno vydať pre úmyselný trestný čin. Ak by sme uplatnili zásadu lex posterior derogat legi priori, tak pri výklade § 116 TP by súdy takýto príkaz mali vydať len pre trestné činy stanovené v § 58 ods. 7 ZoEK a nie pre každý úmyselný trestný čin. Ak však zoberieme do úvahy ročnú štatistiku žiadostí o sprístupnenie uchovávaných údajov (Tab. 1), tak vzhľadom na počet prípadov, v ktorých sa požadované údaje poskytli oprávneným orgánom štátu, môžeme dôvodne predpokladať, že sa súdny príkaz vydáva aj pre iné úmyselné trestné činy ako sú stanovené v § 58 ods. 7 ZoEK.“*

22. Podľa navrhovateľov *„Zákonodarca musí pri uchovávaní a použití údajov stanoviť jasné pravidla transparentnosti. Sem patrí najmä zásada otvorenosti pri zhromažďovaní a použití osobných údajov, a teda zhromažďovanie a použitie osobných údajov by sa malo diať s vedomím dotknutej osoby, okrem prípadu, ak by tým došlo k zmareniu vyšetrovania. Aj v prípade zhromaždenia alebo použitia údajov bez vedomia dotknutej osoby by mal zákonodarca stanoviť aspoň povinnosť dodatočného informovania. Avšak orgánom oprávneným k využitiu prevádzkových a lokalizačných údajov nebola stanovená povinnosť dodatočného informovania dotknutej osoby. Takáto povinnosť však*

podľa § 88 ods. 8 TP existuje pri vyhotovovaní obrazových, zvukových alebo obrazovo-zvukových záznamov, pričom tieto dva inštitúty predstavujú porovnateľný zásah do súkromia.“.

23. V súvislosti s napádanými ustanoveniam Trestného poriadku skupina poslancov vo svojom návrhu ďalej uvádza: „... hodnota informácií získaných z prevádzkových a lokalizačných údajov je porovnateľná s hodnotou informácií získaných z obsahu komunikácie, ba niekedy môže byť dokonca aj vyššia. Postup ustanovený Trestným poriadkom v súvislosti s príkazom na zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke na objasnenie skutočností dôležitých pre trestné konanie však túto skutočnosť ignoruje. Neobsahuje totiž žiadne garancie práv porovnateľné s tými, ktoré predpokladá Trestný poriadok v § 115 pre odpočúvanie a záznam telekomunikačnej prevádzky. Bez akéhokoľvek relevantného dôvodu sa procesný postup pri použití týchto dvoch, inštitútov značne líši. V prípade príkazu na zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke je priveľmi všeobecný a vágny, čo možno, vzhľadom na informácie, ktoré možno získať z daných údajov, považovať za ústavne neprijateľné (porovnaj bod 27, PL ÚS 42/11, ÚS ČR).

Údaje podľa § 116 TP môžu byť poskytnuté pre všetky trestné konania vedené pre akýkoľvek úmyselný trestný čin. Takéto všeobecné obmedzenie je v rozpore so znením ZoEK, ktoré je neporovnateľne užšie. Empirické údaje však naznačujú, že sudcovia uplatňujú rozsah trestných činov podľa § 116TP (viď Tab. 1).

Navyše k poskytovaniu týchto údajov nedochádza iba vtedy, ak účel trestného konania nemožno dosiahnuť inak a zákonná úprava neposkytuje dostatočné garancie na to, aby nedošlo k použitiu týchto údajov k inému než zákonom predpokladanému účelu - absentuje jasná a detailná úprava minimálnych požiadaviek na zabezpečenie uchovávaných údajov (postupy vedúce k ochrane ich celistvosti, dôvernosti ako aj k ich zničeniu). Napokon, účinná ochrana pred nezákonným zásahom do základných ľudských práv a slobôd dotknutých osôb by mala byť zaručená aj prostredníctvom povinnosti dodatočne informovať o tom, že jej prevádzkové a lokalizačné údaje boli poskytnuté orgánom činným v trestnom konaní.“

24. Navrhovatelia napokon dodávajú: *«Nehovoriac o tom, že podniky, ktoré takéto informácie sprístupňujú sú často veľmi malé spoločností (pripojenie na internet), u ktorých je „bezpodozrievavá úslužnosť“ voči štátnym orgánom pomerne vysoká. Predmet telekomunikačného tajomstva (§ 63 ZoEK) tak podľa bežnej praxe býva sprístupňovaný aj v priestupkovom konaní (viď príloha č. 1). Policajný zbor mimo trestného konania svoje protiprávne a protiústavné žiadostí odôvodňuje § 76a ods. 3 zákona č. 171/1993 Z. z. o Policajnom zbore (ZoPZ) alebo dokonca všeobecnou povinnosťou súčinnosti podľa § 76 ZoPZ, resp. § 76a ZoPZ. Generálny advokát Jäaskinen pritom v prípade Bonnier Audio C-461/10 výslovne pripomína, že: „k tomu, aby bylo zpřístupnění osobních údajů možné, vyžaduje unijní právo, aby povinnost uchovávaní byla stanovená vnitrostátními právními předpisy, které upřesni kategorie uchovávaných údajů, účel uchovávaní, dobu uchovávaní a osoby, které mohou mít k údajům přístup. Využívaní databází, které existují k jistým účelům, než které byly takto stanovený zákonodárcem, by bylo v rozporu se zásadami ochrany osobních údajů.“»*

I.2 Návrh na rozhodnutie

25. Na základe uvedenej argumentácie sa skupina poslancov domáha, aby ústavný súd prijal jej návrh na ďalšie konanie a následne o ňom v konaní vo veci samej nálezom takto rozhodol:

„Ustanovenie § 58 ods. 5, 6, 7 a § 63 ods. 6 zákona NR SR Č. 351/2011 Z. z. o elektronických komunikáciách, § 116 zákona NR SR č. 301/2005 Trestného poriadku a § 76a ods. 3 zákona č. 171/1993 Z. z. o Policajnom zbore nie je v súlade s čl. 13 ods. 4, čl. 16 ods. 1, čl. 19 ods. 2, 3, čl. 22, čl. 26 Ústavy SR, čl. 7 ods. 1, čl. 10 ods. 2, 3, čl. 13, čl. 17 ústavného zákona č. 23/1991 Zb., ktorým sa uvádza Listina základných práv a slobôd, čl. 8. čl. 10 Dohovoru o ochrane ľudských práv a základných slobôd a čl. 7, čl. 8, čl. 11, 52 ods. 1 Charty základných práv Európskej únie.“

26. Skupina poslancov rovnako navrhla, aby ústavný súd položil Súdnemu dvoru Európskej únie (ďalej aj „Súdny dvor“) podľa čl. 267 Zmluvy o fungovaní Európskej únie otázku týkajúcu sa platnosti čl. 3, čl. 5 a čl. 6 Smernice Rady č. 2006/24/ES o uchovávaní údajov vytvorených alebo spracovaných v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb alebo verejných komunikačných sietí (ďalej len „smernica 2006/24/ES“).

27. Ústavný súd návrh skupiny poslancov predbežne prerokoval a uznesením č. k. PL. ÚS 10/2014-29 z 23. apríla 2014 ho podľa § 25 ods. 3 zákona Národnej rady Slovenskej republiky č. 38/1993 Z. z. o organizácii Ústavného súdu Slovenskej republiky, o konaní pred ním a o postavení jeho sudcov v znení neskorších predpisov (ďalej len „zákon o ústavnom súde“) prijal na ďalšie konanie. Predmetným uznesením zároveň pozastavil účinnosť § 58 ods. 5 až 7 a § 63 ods. 6 zákona o elektronických komunikáciách.

II. Ďalší priebeh konania

28. Po prijatí návrhu skupiny poslancov na ďalšie konanie si ústavný súd podľa § 39 ods. 1 zákona o ústavnom súde vyžiadal k tomuto návrhu stanovisko Národnej rady Slovenskej republiky (ďalej aj „národná rada“), vlády Slovenskej republiky (ďalej aj „vláda“) ako vedľajšieho účastníka, zastúpenej Ministerstvom spravodlivosti Slovenskej republiky (ďalej len „ministerstvo spravodlivosti“), a zároveň ich vyzval, aby sa vyjadrili aj k tomu, či trvajú na ústnom pojednávaní vo veci.

II.1 Stanovisko Národnej rady Slovenskej republiky

29. Listom z 8. júla 2014 predseda národnej rady ústavnému súdu oznámil, že národná rada netrvá na ústnom pojednávaní a k predmetnej veci stanovisko zaujímať nebude.

II.2 Stanovisko vlády Slovenskej republiky

30. Stanovisko vlády ako vedľajšieho účastníka, zastúpeného ministrom spravodlivosti Slovenskej republiky, je obsiahnuté v prípise ministra spravodlivosti Slovenskej republiky č. 38669/2014/21 zo 16. júla 2014. Vláda vo svojom stanovisku navrhla, aby ústavný súd návrhu skupiny poslancov nevyhovel, a zároveň oznámila, že netrvá na ústnom pojednávaní v predmetnej veci.

31. V stanovisku vlády sa okrem iného uvádza:

«Podľa § 58 ods. 5 zákona č. 351/2011 Z. z. o elektronických komunikáciách (ďalej len „ZEK“) je každá osoba alebo sieť (ďalej len „podnik“), ktorá poskytuje elektronickú komunikačnú službu, povinná uchovávať prevádzkové údaje, lokalizačné údaje a údaje komunikujúcich strán v zákonom stanovenej lehote, pričom v ustanovení § 58 ods. 7 ZEK je presne vymedzený a špecifikovaný účel, na aký sa predmetné údaje uchovávajú. Ide o vyšetrovanie, odhaľovanie a stíhanie trestných činov súvisiacich s terorizmom, nedovoleným obchodovaním, organizovanou trestnou činnosťou, únikom a ohrozením utajovaných skutočností a s trestnými činmi spáchanými nebezpečným zoskupením.

Pokiaľ sa týka uchovávania určitých údajov, je potrebné upozorniť na skutočnosť, že všetky údaje, ktoré ZEK vymenováva, sú údaje prevádzkové (údaje vzťahujúce sa na užívateľa a na konkrétny prenos informácie, ktoré sa spracúvajú na účely prenosu správ a fakturácie), lokalizačné (údaje, ktoré označujú geografickú polohu koncového zariadenia) a údaje komunikujúcich strán (telefónne číslo, obchodné meno a sídlo právnickej osoby, osobné údaje fyzickej osoby), teda predmetom uchovávania nie je obsah správ. Tieto údaje sú zároveň telekomunikačným tajomstvom a ZEK presne definuje komu, za akých okolností a na základe akého postupu môžu byť uchovávané údaje sprístupnené. Povinnosť uchovať vymedzené údaje nemožno chápať samostatne bez zákonného mechanizmu prístupu k nim. § 58 ods. 7 ZEK preto priamo odkazuje na ustanovenie § 63 ods. 6 ZEK, v ktorom sú podmienky sprístupnenia definované. Podľa § 63 ods. 6 ZEK je podnik povinný poskytnúť inému orgánu štátu údaje, ktoré sú predmetom telekomunikačného tajomstva, a to na účely

plnenia jeho úloh podľa osobitných predpisov. ZEK presne vymedzuje, kto je iný orgán štátu, pričom ide o ozbrojený bezpečnostný zbor, ozbrojený zbor a štátny orgán, ktorý v rozsahu ustanovenom osobitnými predpismi plní úlohy na úseku ochrany ústavného zriadenia, obrany štátu, vnútorného poriadku a bezpečnosti štátu (napr. Slovenská informačná služba, Vojenské spravodajstvo atď.). ZEK priamo upravuje taktiež procesný postup sprístupnenia informácií. Údaje môžu byť poskytnuté len na základe písomnej žiadosti a so súhlasom súdu alebo na príkaz súdu. ZEK je previazaný so zákonom č. 301/2005 Z. z. Trestným poriadkom (ďalej len „trestný poriadok“) a so zákonom č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) v znení neskorších predpisov.

§ 116 Trestného poriadku upravuje osobitnú formu informačného technického prostriedku (odpočúvanie a záznam telekomunikačnej prevádzky), ktorý v konaní o úmyselnom trestnom čine umožňuje získanie údajov o uskutočnenej telekomunikačnej prevádzke, ktoré sú predmetom telekomunikačného tajomstva alebo na ktoré sa vzťahuje ochrana osobných údajov v prípade, ak sú takéto údaje potrebné na objasnenie skutočností dôležitých pre trestné konanie. Príkaz na zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke vydáva písomne predseda senátu, pred začatím trestného stíhania alebo v prípravnom konaní sudca pre prípravné konanie na návrh prokurátora, ktorý musí byť odôvodnený aj skutkovými okolnosťami.

Z pohľadu základných zásad trestného konania upravených v § 2 Trestného poriadku, konkrétne zásady upravenej v ods. 2, v zmysle ktorej „do základných práv a slobôd osôb v prípadoch dovolených zákonom možno zasahovať len v miere nevyhnutnej na dosiahnutie účelu trestného konania, pričom treba rešpektovať dôstojnosť osôb a ich súkromie“, ako i v zmysle Ústavy Slovenskej republiky (ďalej len „ústava“) možno považovať ustanovenie § 116 Trestného poriadku za súladné s ústavou, keďže predstavuje ústavne predpokladanú výnimku zásahu do garantovaných práv a slobôd, a to vymedzením ustanoveného cieľa, ktorým je objasnenie skutočností dôležitých pre trestné konanie.

Pokiaľ ide o vhodnosť inštitútu uchovávania údajov na účel vyšetrovania, odhaľovania a stíhania závažných trestných činov, s tvrdením navrhovateľa, že zbieranie

týchto údajov nemá žiaden pozitívny vplyv na odhaľovanie závažných trestných činov v Európe, sa nemožno stotožniť. Neexistuje menej závažný prostriedok, ktorý by rovnako efektívne napĺňal vymedzený cieľ. Z hodnotiacej správy Európskej komisie o smernici o uchovávaní údajov [K0M(20ii) 225 z 18. apríla 2011] vyplýva, že členské štáty považujú uchovávanie údajov na účely predchádzania a boja proti zločinnosti za prinajmenšom cenné a v niektorých prípadoch priam nevyhnutné. Uchovávanie údajov sa ukázalo ako nevyhnutné pri takých činnostiach, ako sú zabezpečovanie a rekonštrukcia dôkazov alebo stôp pri určovaní spolupáchateľstva pri trestnom čine, pričom v niektorých prípadoch uchovávané údaje poskytujú jediný spôsob usvedčenia páchateľa, a to napr. v tak závažných prípadoch ako sú prípady sexuálneho zneužívania detí alebo prechovávania detskej pornografie. Prístup k výpisom z prevádzky telefónnych hovorov je nenahraditeľný zdroj informácií pre odhaľovanie trestnej činnosti terorizmu a niektorých foriem účasti na terorizme, ktoré nie je možné získať iným spôsobom. Trestná činnosť súvisiaca s terorizmom je vysoko latentná, uzatvorená v komunitách, kde prienik zvonku je takmer nemožný. Telefonické výpisy prispievajú ku komplexnému zmonitorovaniu kontaktov a ich prepojení na zahraničné teroristické zoskupenia.

Vhodnosť uchovávania údajov na stanovené účely ďalej potvrdzuje skutočnosť, že ich využitím sa redukuje, resp. zefektívňuje potreba invazívnejších vyšetrovacích metód (napr. odpočúvanie, domová prehliadka atď.).

Čo sa týka namietaného ustanovenia § 76a zákona NRSR č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov (ďalej len „zákon o PZ"), podľa ktorého je policajný zbor pri odhaľovaní a dokumentovaní trestnej činnosti oprávnený žiadať údaje od právnických osôb a fyzických osôb , ktoré poskytujú elektronické komunikačné siete a elektronické komunikačné služby, je potrebné uviesť, že priebeh odhaľovania a dokumentovania trestnej činnosti prebieha na základe zákonom stanovených postupov, a teda na základe platných právnych predpisov. Základným procesným predpisom pre oblasť trestnej činnosti je Trestný poriadok, ktorý upravuje postup orgánov činných v trestnom konaní a súdov. Ako bolo už vyššie uvedené, Trestný poriadok vcelku konkrétne upravuje postup pri získavaní informácií o uskutočnenej telekomunikačnej prevádzke, a

teda v žiadnom prípade nemôže ísť o svojvôľu policajného zboru v procese vyšetrovania trestnej činností.

Jedinú výnimku z uvedených princípov ZEK povoľuje v prípade údajov potrebných pre pátranie po nezvestných osobách a odcudzených motorových vozidlách, kedy sa postupuje podľa § 76 ods. 4 a 5 zákona o PZ. V prípade pátraní po nezvestných osobách, je policajný zbor oprávnený žiadať predmetné informácie len s predchádzajúcim súhlasom príbuzného v priamom rade, resp. ďalších blízkych osôb tak ako to zákon o PZ stanovuje v § 76 ods. 4. Ak ide o pátranie po odcudzenom motorovom vozidle, v ktorom sa v čase odcudzenia nachádzalo telekomunikačné zariadenie, je policajný zbor oprávnený žiadať o prevádzkové a lokalizačné údaje na základe písomnej žiadosti majiteľa, prevádzkovateľa alebo držiteľa telekomunikačného zariadenia. V oboch prípadoch je teda potrebný súhlas, resp. žiadosť dotknutej osoby, resp. osoby blízkej.

Navrhovateľ vo svojom návrhu konštatuje, že „... samotný zber podlieha minimálnemu počtu pravidiel. Systém uchovávania údajov neobsahuje takmer žiadne záruky proti ich zneužívaniu a hlavná úloha je ponechaná súkromným spoločnostiam, ktoré majú prirodzene skôr záujem na minimalizácii nákladov, keďže im štát túto činnosť neuhrádza.“. Podľa § 58 ZEK je podnik pri uchovávaní údajov povinný zabezpečiť, aby:

- uchovávané údaje mali rovnakú kvalitu a podliehali rovnakému zabezpečeniu a ochrane ako údaje podnikom spracúvané alebo uchovávané pri poskytovaní sietí alebo služieb,

- údaje podliehali príslušným technickým opatreniam a organizačným opatreniam na ochranu údajov proti zničeniu, strate, zmene alebo protiprávnemu uchovaniu, spracovaniu, prístupu alebo zverejneniu,

- údaje podliehali technickým a organizačným opatreniam, ktoré zabezpečia, aby údaje mohli byť sprístupnené len oprávneným osobám konajúcim na základe poverenia podniku a orgánom činným v trestnom konaní, súdom alebo iným orgánom štátu,

- údaje boli na konci obdobia určeného na ich uchovávanie zlikvidované, okrem údajov, ktoré boli poskytnuté a zabezpečené.

Z uvedených ustanovení teda jednoznačne vyplývajú povinnosti a zásady, ktoré sú podniky povinné dodržiavať pri uchovávaní a poskytovaní údajov.

Je v najvyššom záujme podnikov, aby ochrane údajov venovali maximálnu pozornosť, a to jednak zo zákonných dôvodov (ZEK, zákon č. 122/2013 Z. z. o ochrane osobných údajov v znení neskorších predpisov), ako aj z dôvodu dôvery zákazníkov, keďže únikom osobných údajov z rôznych dôvodov utrpí dobré meno podniku, čo môže mať vo vysoko konkurenčnom prostredí, akým je telekomunikačný trh, veľmi negatívne dopady na budúcnosť podniku.

V súvislosti s úhradou nákladov zo strany štátu, existuje množstvo situácií, kedy je podnik povinný plniť si svoje zákonné povinnosti bez toho, aby takto vzniknuté náklady boli kompenzované štátom (napr. ochrana osobných údajov klientov bankami, lekármi atď.).

Argument navrhovateľa, že „... k zneužitiu uchovávaných údajov môže dôjsť aj samotným poskytovateľom, a to najmä za účelom marketingu svojich služieb...“ je v kontexte problematiky uchovávania údajov pre potreby vyšetrovania trestných činov irelevantný. Podniky majú prevádzkové údaje, lokalizačné údaje a údaje komunikujúcich strán štandardne k dispozícii, nakoľko ide o údaje, ktoré sú potrebné pre poskytovanie služieb, resp. sietí a súvisia napríklad s fakturáciou.

Vzhľadom na vyššie uvedené možno teda právnu úpravu ZEK, ako i Trestného poriadku a zákona o PZ považovať za súladné s ústavou a ostatnými medzinárodnými dokumentmi, ktorými je Slovenská republika viazaná.»

II.3 Doplnenie návrhu skupiny poslancov

32. Dňa 13. apríla 2015 bolo ústavnému súdu doručené doplnenie návrhu skupiny poslancov, v ktorom poukazuje na rozhodnutie Súdneho dvora vo veci Digital Rights Ireland C-293/12 a Kärntner Landesregierung C-594/12 z 8. apríla 2014, a podanie, ktorým oznamuje, že netrvá na ústnom prerokovaní veci a súhlasí s upustením od ústneho pojednávania.

III. Základné východiská pre rozhodovanie o návrhu skupiny poslancov

III.1 Podstata problému nastoleného návrhom skupiny poslancov, napadnutá právna úprava a súvisiace ustanovenia ústavy, listiny, dohovoru a charty

33. Skupina poslancov namieta nesúlad ustanovení § 58 ods. 5 až 7 a § 63 ods. 6 zákona o elektronických komunikáciách, § 116 Trestného poriadku a § 76a ods. 3 zákona o Policajnom zbore s čl. 13 ods. 4, čl. 16 ods. 1, čl. 19 ods. 2 a 3, čl. 22 a čl. 26 ústavy, čl. 7 ods. 1, čl. 10 ods. 2 a 3, čl. 13 a čl. 17 listiny, čl. 8 a čl. 10 dohovoru a čl. 7, čl. 8, čl. 11 a čl. 52 ods. 1 charty.

34. Skupina poslancov tvrdí, že napadnuté ustanovenia zákona o elektronických komunikáciách ustanovujúce povinnosť poskytovateľov elektronických komunikácií uchovávať prevádzkové údaje, lokalizačné údaje a údaje komunikujúcich strán odo dňa uskutočnenia komunikácie počas 6 mesiacov, ak ide o pripojenie k internetu, internetovú elektronickú poštu a telefonovanie prostredníctvom internetu, a počas 12 mesiacov, ak ide o ostatné druhy komunikácie, a to v rozsahu, v akom ich vytvára alebo spracúva pri poskytovaní služby alebo siete, vrátane údajov súvisiacich s neúspešnými pokusmi o volanie, a povinnosť podniku tieto údaje na základe písomnej žiadosti bezodkladne poskytnúť za stanovených podmienok orgánom činným v trestnom konaní, súdu a inému orgánu štátu na účely vyšetrovania, odhaľovania a stíhania trestných činov súvisiacich s terorizmom, nedovoleným obchodovaním, organizovanou trestnou činnosťou, únikom a ohrozením utajovaných skutočností a s trestnými činmi spáchanými nebezpečným zoskupením sú v rozpore s označenými ustanoveniami ústavy, listiny, dohovoru a charty.

35. Ustanovenia Trestného poriadku, ktoré navrhovatelia napádajú pre ich nesúlad s označenými ustanoveniami ústavy, listiny, dohovoru a charty, zakladajú orgánom činným v trestnom konaní oprávnenie, aby v trestnom konaní pre úmyselný trestný čin na účely objasnenia skutočností dôležitých pre trestné konanie získali od poskytovateľov elektronických komunikácií údaje o uskutočnenej telekomunikačnej prevádzke, ktoré sú

inak predmetom telekomunikačného tajomstva alebo na ktoré sa vzťahuje ochrana osobných údajov.

36. Ustanovenia zákona o Policajnom zbore, ktoré skupina poslancov napáda pre ich nesúlad s označenými ustanoveniami ústavy, listiny, dohovoru a charty, zakladajú pre Policajný zbor oprávnenie žiadať v rozsahu potrebnom na plnenie konkrétnej úlohy Policajného zboru a na čas nevyhnutný na splnenie tejto úlohy od právnických osôb a fyzických osôb, ktoré poskytujú elektronické komunikačné siete a elektronické komunikačné služby, prevádzkové údaje a údaje komunikujúcich strán spôsobom umožňujúcim diaľkový, nepretržitý a priamy prístup.

37. Podľa § 58 ods. 5, 6 a 7 zákona o elektronických komunikáciách:

„(5) Podnik je povinný na účely podľa odseku 7 uchovávať prevádzkové údaje, lokalizačné údaje a údaje komunikujúcich strán odo dňa uskutočnenia komunikácie počas

a) 6 mesiacov, ak ide o pripojenie k internetu, internetovú elektronickú poštu a telefonovanie prostredníctvom internetu, a

b) 12 mesiacov, ak ide o ostatné druhy komunikácie.

(6) Údaje podľa odseku 5 podnik uchováva v rozsahu, v akom ich vytvára alebo spracúva pri poskytovaní služby alebo siete. Podnik uchováva údaje podľa odseku 5 súvisiace s neúspešnými pokusmi o volanie, ktoré podnik vytvára alebo spracúva a ukladá, ak ide o telefónne údaje alebo zaznamenáva, ak ide o internetové údaje. Neuchovávajú sa údaje, ktoré sa týkajú nespojených volaní. Zoznam údajov, ktoré je podnik povinný uchovávať podľa tohto odseku a odseku 5, je uvedený v prílohe č. 2.

(7) Údaje uchovávané podľa odsekov 5 a 6 spolu s údajmi účastníka v rozsahu podľa § 63 ods. 1 písm. b) je podnik povinný na základe písomnej žiadosti a bezodkladne poskytnúť za podmienok ustanovených v § 63 ods. 6 orgánom činným v trestnom konaní, súdu a inému orgánu štátu na účely vyšetrovania, odhaľovania a stíhania trestných činov súvisiacich s terorizmom, nedovoleným obchodovaním, organizovanou trestnou činnosťou, únikom a ohrozením utajovaných skutočností a s trestnými činmi spáchanými nebezpečným zoskupením; údaje a informácie môže podnik uchovávať len v elektronickej podobe.“

38. Podľa § 63 ods. 6 zákona o elektronických komunikáciách:

„(6) Podnik je povinný poskytnúť inému orgánu štátu podľa § 55 ods. 6 na účely plnenia jeho úloh podľa osobitných predpisov na základe písomnej žiadosti a so súhlasom súdu alebo na príkaz súdu podľa osobitných predpisov údaje, ktoré sú predmetom telekomunikačného tajomstva podľa odseku 1 písm. b) až d); v prípade údajov potrebných pre pátranie po nezvestných osobách a odcudzených motorových vozidlách sa postupuje podľa osobitného predpisu. Podnik je povinný poskytnúť tieto údaje inému orgánu štátu podľa § 55 ods. 6 v písomnej forme alebo v elektronickej podobe v šifrovanej forme a zrozumiteľným spôsobom. Náklady na hmotné nosiče, ktoré sú potrebné na poskytnutie údajov, uhrádza orgán štátu, ktorému sa takéto údaje poskytli.“

39. V prílohe č. 2 s označením „Kategórie uchovávaných údajov“ zákona o elektronických komunikáciách sa uvádza:

„A. Údaje potrebné na zistenie a identifikáciu zdroja komunikácie:

1. ak ide o telefónne spojenie prostredníctvom pevnej siete a mobilné telefónne spojenie:

a) telefónne číslo volajúceho,

b) meno, priezvisko a adresa trvalého pobytu, alebo obchodné meno a sídlo alebo miesto podnikania účastníka alebo registrovaného užívateľa,

2. ak ide o pripojenie k internetu, internetovú elektronickú poštu a telefonovanie prostredníctvom internetu:

a) pridelené označenie užívateľa,

b) označenie užívateľa a telefónne číslo pridelené každej komunikácii, ktorá vstupuje do verejnej telefónnej siete,

c) meno, priezvisko a adresa trvalého pobytu, alebo obchodné meno a sídlo alebo miesto podnikania účastníka alebo registrovaného užívateľa a adresa internetového protokolu (IP), ktorá mu bola v čase komunikácie pridelená, označenie užívateľa alebo telefónne číslo.

B. Údaje potrebné na identifikáciu adresáta komunikácie:

1. ak ide o telefónne spojenie prostredníctvom pevnej siete a mobilné telefónne spojenie:

c) volené číslo alebo čísla (volané telefónne číslo alebo čísla) a v prípadoch, keď sú poskytnuté doplnkové služby, napríklad presmerovanie alebo odovzdanie volania, číslo alebo čísla, na ktoré je volanie smerované,

d) meno, priezvisko a adresa trvalého pobytu, alebo obchodné meno a sídlo alebo miesto podnikania účastníka alebo registrovaného užívateľa,

2. ak ide o internetovú elektronickú poštu a telefonovanie prostredníctvom internetu:

a) označenie užívateľa alebo telefónne číslo určených príjemcov telefónneho volania,

b) meno, priezvisko a adresa trvalého pobytu, alebo obchodné meno a sídlo alebo miesto podnikania účastníka alebo registrovaného užívateľa, ktorý je určeným príjemcom komunikácie.

C. Údaje potrebné na identifikáciu dátumu, času a trvania komunikácie:

1. ak ide o telefónne spojenie prostredníctvom pevnej siete a mobilné telefónne spojenie: dátum a čas začatia a ukončenia komunikácie,

2. ak ide o pripojenie k internetu, internetovú elektronickú poštu a telefonovanie prostredníctvom internetu:

e) dátum a čas prihlásenia a odhlásenia zo služby pripojenia k internetu v určitom časovom pásme spolu s dynamickou alebo statickou IP adresou, ktorú komunikácii pridelil poskytovateľ služby pripojenia k internetu, a užívateľské označenie účastníka alebo registrovaného užívateľa,

f) dátum a čas prihlásenia a odhlásenia zo služieb internetovej elektronickej pošty alebo telefonovania prostredníctvom internetu v určitom časovom pásme.

D. Údaje potrebné na identifikáciu typu komunikácie:

1. ak ide o telefónne spojenie prostredníctvom pevnej siete a mobilné telefónne spojenie: používaná telefónna služba,

2. ak ide o internetovú elektronickú poštu a telefonovanie prostredníctvom internetu: používaná internetová služba.

E. Údaje potrebné na identifikáciu koncového zariadenia užívateľov alebo ich údajného zariadenia:

1. ak ide o telefónne spojenie prostredníctvom pevnej siete: číslo volajúceho a volaného,

2. ak ide o mobilné telefónne spojenie:

g) číslo volajúceho a volaného,

h) IMSI volajúceho,

i) IMEI volajúceho,

j) IMSI volaného,

k) IMEI volaného,

l) v prípade predplatených anonymných služieb dátum a čas počiatočnej aktivácie služby a označenie bunky, z ktorej sa vykonala aktivácia služby,

3. ak ide o pripojenie k internetu, internetovú elektronickú poštu a telefonovanie prostredníctvom internetu:

a) telefónne číslo volajúceho pri prístupe prostredníctvom modemu (dial-up prístup),

b) digitálna účastnícka prípojka alebo iný koncový bod pôvodcu komunikácie.

F. Údaje potrebné na identifikáciu polohy mobilného koncového zariadenia:

1. údaje o polohe bunky pri začatí komunikácie,

2. údaje identifikujúce zemepisnú polohu buniek podľa ich označenia počas obdobia uchovávania údajov o komunikácii.“

40. Podľa § 116 Trestného poriadku:

„(1) V trestnom konaní pre úmyselný trestný čin možno vydať príkaz na zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke, ktoré sú predmetom telekomunikačného tajomstva alebo na ktoré sa vzťahuje ochrana osobných údajov, ktoré sú potrebné na objasnenie skutočností dôležitých pre trestné konanie.

(2) Príkaz na zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke vydáva písomne predseda senátu, pred začatím trestného stíhania alebo v prípravnom konaní sudca pre prípravné konanie na návrh prokurátora, ktorý musí byť odôvodnený aj skutkovými okolnosťami; príkaz sa doručí osobám uvedeným v odseku 3.

(3) Právnické osoby alebo fyzické osoby, ktoré zabezpečujú telekomunikačnú prevádzku, oznámia predsedovi senátu a v prípravnom konaní prokurátorovi alebo policajtovi údaje o uskutočnenej telekomunikačnej prevádzke.

(4) Ustanovenia odsekov 1 až 3 sa primerane vzťahujú na obsahové údaje alebo prevádzkové údaje prenášané prostredníctvom počítačového systému.“

41. Podľa § 76a ods. 3 zákona o Policajnom zbore:

„Policajný zbor je pri odhaľovaní a dokumentovaní trestnej činnosti oprávnený žiadať v rozsahu potrebnom na plnenie konkrétnej úlohy Policajného zboru a na čas nevyhnutný na splnenie tejto úlohy od právnických osôb a fyzických osôb, ktoré poskytujú elektronické komunikačné siete a elektronické komunikačné služby, prevádzkové údaje a údaje komunikujúcich strán podľa osobitného predpisu spôsobom umožňujúcim diaľkový, nepretržitý a priamy prístup. Právnické osoby a fyzické osoby, ktoré poskytujú elektronické komunikácie, sú povinné písomnej žiadosti Policajného zboru bez zbytočného odkladu vyhovieť.“

42. Napadnuté ustanovenia zákona o elektronických komunikáciách, Trestného poriadku a zákona o Policajnom zbore sú podľa názoru navrhovateľov v rozpore s čl. 16 ods. 1, čl. 19 ods. 2 a 3, čl. 22 a čl. 26 ústavy v spojení s čl. 13 ods. 4 ústavy, čl. 7 ods. 1, čl. 10 ods. 2 a 3, čl. 13 a čl. 17 listiny, čl. 8 a čl. 10 dohovoru a čl. 7, čl. 8, čl. 11 charty v spojení s čl. 52 ods. 1 charty.

43. Podľa čl. 16 ods. 1 ústavy a čl. 7 ods. 1 listiny nedotknuteľnosť osoby a jej súkromia je zaručená. Obmedzená môže byť len v prípadoch ustanovených zákonom.

44. Podľa čl. 19 ods. 2 ústavy a čl. 10 ods. 2 listiny každý má právo na ochranu pred neoprávneným zasahovaním do súkromného a rodinného života.

45. Podľa čl. 19 ods. 3 ústavy a čl. 10 ods. 3 listiny každý má právo na ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe.

46. Podľa čl. 22 ods. 1 ústavy listové tajomstvo, tajomstvo dopravovaných správ a iných písomností a ochrana osobných údajov sa zaručujú.

47. Podľa čl. 22 ods. 2 ústavy nikto nesmie porušiť listové tajomstvo ani tajomstvo iných písomností a záznamov, či už uchovávaných v súkromí, alebo zasielaných poštou, alebo iným spôsobom; výnimkou sú prípady, ktoré ustanoví zákon. Rovnako sa zaručuje tajomstvo správ podávaných telefónom, telegrafom alebo iným podobným zariadením. Obdobné je znenie čl. 13 listiny.

48. Podľa čl. 26 ods. 1 ústavy a čl. 17 ods. 1 listiny sloboda prejavu a právo na informácie sú zaručené.

49. Podľa čl. 26 ods. 2 ústavy každý má právo vyjadrovať svoje názory slovom, písmom, tlačou, obrazom alebo iným spôsobom, ako aj slobodne vyhľadávať, prijímať a rozširovať idey a informácie bez ohľadu na hranice štátu. Vydávanie tlače nepodlieha povoľovaciemu konaniu. Podnikanie v odbore rozhlasu a televízie sa môže viazať na povolenie štátu. Podmienky ustanoví zákon.

50. Podľa čl. 26 ods. 3 ústavy cenzúra sa zakazuje.

51. Podľa čl. 26 ods. 4 ústavy a čl. 17 ods. 4 listiny slobodu prejavu a právo vyhľadávať a šíriť informácie možno obmedziť zákonom, ak ide o opatrenia v demokratickej spoločnosti nevyhnutné na ochranu práv a slobôd iných, bezpečnosť štátu, verejného poriadku, ochranu verejného zdravia a mravnosti.

52. Podľa čl. 26 ods. 5 ústavy orgány verejnej moci majú povinnosť primeraným spôsobom poskytovať informácie o svojej činnosti v štátnom jazyku. Podmienky a spôsob vykonania ustanoví zákon.

53. Podľa čl. 13 ods. 4 ústavy pri obmedzovaní základných práv a slobôd sa musí dbať na ich podstatu a zmysel. Takéto obmedzenia sa môžu použiť len na ustanovený cieľ.

54. Podľa čl. 8 dohovoru každý má právo na rešpektovanie svojho súkromného a rodinného života, obydlia a korešpondencie. Štátny orgán nemôže do výkonu tohto práva zasahovať s výnimkou prípadov, keď je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom alebo zločinnosti, ochrany zdravia alebo morálky alebo na ochranu práv a slobôd iných.

55. Podľa čl. 10 dohovoru každý má právo na slobodu prejavu. Toto právo zahŕňa slobodu zastávať názory a prijímať a rozširovať informácie alebo myšlienky bez zasahovania štátnych orgánov a bez ohľadu na hranice. Tento článok nebráni štátom, aby vyžadovali udeľovanie povolení rozhlasovým, televíznym alebo filmovým spoločnostiam. Výkon týchto slobôd, pretože zahŕňa povinnosti aj zodpovednosť, môže podliehať takým formalitám, podmienkam, obmedzeniam alebo sankciám, ktoré ustanovuje zákon a ktoré sú nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, územnej celistvosti alebo verejnej bezpečnosti, na predchádzanie nepokojom alebo zločinnosti, ochranu zdravia alebo morálky, ochranu povesti alebo práv iných, zabránenia úniku dôverných informácií alebo zachovania autority a nestrannosti súdnej moci.

56. Podľa čl. 7 charty každý má právo na rešpektovanie svojho súkromného a rodinného života, obydlia a komunikácie.

57. Podľa čl. 8 charty každý má právo na ochranu osobných údajov, ktoré sa ho týkajú. Tieto údaje musia byť riadne spracované na určené účely na základe súhlasu dotknutej osoby alebo na inom oprávnenom základe ustanovenom zákonom. Každý má právo na prístup k zhromaždeným údajom, ktoré sa ho týkajú, a právo na ich opravu. Dodržiavanie týchto pravidiel podlieha kontrole nezávislého orgánu.

58. Podľa čl. 11 charty každý má právo na slobodu prejavu. Toto právo zahŕňa slobodu zastávať názory a prijímať a rozširovať informácie a myšlienky bez zasahovania orgánov verejnej moci a bez ohľadu na hranice. Rešpektuje sa sloboda a pluralita médií.

59. Podľa čl. 52 ods. 1 charty akékoľvek obmedzenie výkonu práv a slobôd uznaných v tejto charte musí byť ustanovené zákonom a rešpektovať podstatu týchto práv a slobôd. Za predpokladu dodržiavania zásady proporcionality možno tieto práva a slobody obmedziť len vtedy, ak je to nevyhnutné a skutočne to zodpovedá cieľom všeobecného záujmu, ktoré sú uznané Úniou, alebo ak je to potrebné na ochranu práv a slobôd iných.

III.2 Položenie predbežnej otázky Súdnemu dvoru Európskej únie

60. Skupina poslancov navrhla, aby ústavný súd položil Súdnemu dvoru Európskej únie podľa čl. 267 Zmluvy o fungovaní Európskej únie otázku týkajúcu sa platnosti čl. 3, čl. 5 a čl. 6 smernice 2006/24/ES. Skupina poslancov vyjadrila pochybnosť o tom, či samotný princíp retencie údajov podľa čl. 3, rozsah povinnej retencie podľa čl. 5 a doba povinnej retencie podľa čl. 6 smernice 2006/24/ES sú v súlade s čl. 7, čl. 8 a čl. 52 ods. 1 charty. Posúdenie otázky platnosti príslušných ustanovení samotnej smernice 2006/24/ES skupina poslancov navrhuje z dôvodu, že napadnuté ustanovenia zákona o elektronických

komunikáciách, Trestného poriadku a zákona o Policajnom zbore boli prijaté pre účely implementácie smernice 2006/24/ES do právneho poriadku Slovenskej republiky.

61. Identická predbežná otázka týkajúca sa platnosti smernice 2006/24/ES sa po podaní návrhu skupiny poslancov už stala predmetom konania pred Súdnym dvorom. Súdny dvor svojím rozsudkom v spojených veciach C-293/12 a C-594/12 *Digital Rights Ireland Ltd* z 8. 4. 2014 (rozsudok *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources a iní a Kärntner Landesregierung a iní*, C-293/12 a C-594/12, EU:C:2014:238) vyslovil neplatnosť smernice 2006/24/ES z dôvodu, že normotvorca Európskej únie (ďalej aj „Únia“) pri prijatí tejto smernice prekročil hranice, ktoré mu ukladá dodržiavanie zásady proporcionality so zreteľom na čl. 7, 8 a čl. 52 ods. 1 charty. Keďže predbežná otázka, s ktorou skupina poslancov navrhuje ústavnému súdu obrátiť sa na Súdny dvor, už bola Súdnym dvorom rozhodnutá, ústavný súd tomuto návrhu skupiny poslancov nevyhovel.

III.3 K namietanému nesúladu napadnutých ustanovení zákona o elektronických komunikáciách, Trestného poriadku a zákona o Policajnom zbore s ustanoveniami charty

62. Ústavný súd je podľa čl. 124 ústavy nezávislým súdnym orgánom ochrany ústavnosti. Preto i po pristúpení Slovenskej republiky k Európskej únii zostávajú referenčným rámcom prieskumu ústavného súdu normy ústavného poriadku Slovenskej republiky. Ústavný súd však nemôže neprihliadnuť na dopad práva Európskej únie na tvorbu, aplikáciu a výklad vnútroštátneho práva v oblasti právnej úpravy, ktorej vznik, pôsobenie a účel majú svoj pôvod v práve Európskej únie (porovnaj nález Ústavného súdu Českej republiky sp. zn. Pl. ÚS 24/10, bod 25). Právo Európskej únie má uvedený dopad na vnútroštátne právo v prípade, ak vnútroštátna úprava spadá do rámca pôsobnosti práva Európskej únie. Je potrebné uviesť, že aj po zrušení platnosti smernice 2006/24/ES sa

napadnutá práva úprava Slovenskej republiky prijatá pre účely jej implementácie nedostala mimo rámec pôsobnosti práva Európskej únie.

63. Podľa čl. 51 ods. 1 charty sú ustanovenia charty určené pre členské štáty výlučne vtedy, ak vykonávajú právo Únie. Vymedzenie rozsahu pôsobnosti charty pre členské štáty konkretizujú Vysvetlivky k Charte základných práv (Ú. v. EÚ C 303, 14. 12. 2007, s. 17 – 35, ďalej len „vysvetlivky“), ktoré sa majú podľa čl. 6 ods. 1 tretieho pododseku Zmluvy o Európskej únii riadne zohľadniť a na ktoré sa má podľa čl. 52 ods. 7 charty náležite pri jej výklade prihliadať (pozri napr. aj rozsudok DEB, C 279/09, EU:C:2010:811, bod 32). Podľa vysvetliviek k čl. 51 charty, ktoré poukazujú na judikatúru Súdneho dvora, *„povinnosť rešpektovať základné práva vymedzené v rámci Únie je pre členské štáty záväzná výlučne vtedy, ak konajú v rámci rozsahu pôsobnosti práva Únie“*. Ak vnútroštátna právna úprava patrí do pôsobnosti práva Únie, základné práva zaručené chartou musia byť dodržané a nemôže nastať prípad, ktorý by spadal pod právo Únie a neuplatnili by sa základné práva zaručené chartou (pozri rozsudok *Åklagaren proti Hans Åkerberg Fransson*, C-617/10, EU:C:2013:105, bod 21). Z uplatniteľnosti práva Únie vyplýva uplatniteľnosť základných práv zaručených chartou.

64. Judikatúra Súdneho dvora, na ktorú odkazujú aj vysvetlivky k čl. 51 charty, upresňuje situácie, kedy konanie členských štátov spadá do rámca pôsobnosti práva Európskej únie. Je to tak v troch situáciách, a to ak členské štáty preberajú (implementujú) právo Únie (pozri rozsudok *Hubert Wachauf proti Bundesamt für Ernährung und Forstwirtschaft*, 5/88, EU:C:1989:321), ak ich konanie spadá pod výnimku z uplatňovania únijných pravidiel prípustnú samotným právom Únie [pozri rozsudok *Elliniki Radiophonia Tiléorassi AE a Panellinia Omospondia Syllogon Prossopikou proti Dimotiki Etairia Pliroforissis a Sotirios Kouvelas a Nicolaos Avdellas a iní. („ERT“)*, C-260/89 EU:C:1991:254] a napokon ak vo všeobecnosti ich konanie spadá do rámca práva Únie [pozri rozsudok *Daniele Annibaldi proti Sindaco del Comune di Guidonia a Presidente Regione Lazio („Annibaldi“)*, C-309/96, EU:C:1997:631]. O tretiu situáciu ide vtedy, ak sa v konkrétnej a špecifickej situácii v určitej spojitosti uplatní osobitná hmotnoprávna norma

práva Európskej únie (pozri rozsudok *Karner*, C 71/02, EU:C:2004:181, body 48 až 53; rozsudok *Åklagaren proti Hans Åkerberg Fransson*, C-617/10, EU:C:2013:105).

65. Napadnutá vnútroštátna právna úprava, konkrétne ustanovenia § 58 ods. 5 až 7 a § 63 ods. 6 zákona o elektronických komunikáciách, boli prijaté pre účely implementácie smernice 2006/24/ES do právneho poriadku Slovenskej republiky. Do vyhlásenia smernice 2006/24/ES za neplatnú Súdnym dvorom tak napadnuté ustanovenia zákona o elektronických komunikáciách spadali pod prvú situáciu, kedy konanie členských štátov spadá do rozsahu pôsobnosti práva Európskej únie, konkrétne, ak členské štáty preberajú (implementujú) právo Únie.

66. Podľa čl. 3 zrušenej smernice 2006/24/ES *„Členské štáty odchylne od článkov 5, 6 a 9 smernice 2002/58/ES prijmú opatrenia, aby zabezpečili, že údaje uvedené v článku 5 tejto smernice sa uchovávajú v súlade s jej ustanoveniami v rozsahu, v akom sú vytvárané alebo spracúvané poskytovateľmi verejne dostupných elektronických komunikačných služieb alebo verejnej komunikačnej siete v ich pôsobnosti v rámci procesu poskytovania príslušných komunikačných služieb.“*. Súdnym dvorom zrušená smernica 2006/24/ES predstavovala výnimku z uplatňovania ustanovení Smernice Rady č. 2002/58/ES z 12. júla 2002 týkajúcej sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií [smernica o súkromí a elektronických komunikáciách; (ďalej len „smernica 2002/58/ES“)] zavádzajúcich povinnosť zabezpečiť primeranú úroveň ochrany základných práv a slobôd a najmä práva na súkromie a dôvernosť z hľadiska spracúvania osobných údajov v elektronickom komunikačnom sektore (pozri čl. 1 smernice 2002/58/ES). Zrušená smernica 2006/24/ES predstavovala derogáciu z ustanovení smernice 2002/58/ES. Cieľom zrušenej smernice bolo zosúladiť právnu úpravu členských štátov zavádzajúcu povinnosti poskytovateľom verejne dostupných elektronických komunikačných služieb alebo verejných komunikačných sietí v súvislosti s uchovávaním určitých údajov, ktoré oni vytvárajú alebo spracovávajú, aby zabezpečili dostupnosť týchto údajov na účely vyšetrovania, odhaľovania a stíhania závažných trestných činov (čl. 1 ods. 1 smernice 2006/24/ES), keďže niektoré členské štáty prijali podľa čl. 15 ods. 1 smernice 2002/58/ES

právne predpisy ustanovujúce poskytovateľom služieb povinnosť uchovávať údaje na predchádzanie, vyšetrovanie, odhaľovanie a stíhanie trestných činov a právne a technické odlišnosti v tejto vnútroštátnej úprave sú prekážkou vnútorného trhu elektronických komunikácií.

67. Napokon, podľa čl. 15 ods. 1 smernice 2002/58/ES *„Členské štáty môžu prijať legislatívne opatrenia na obmedzenie rozsahu práv a povinností uvedených v článku 5, článku 6, článku 8 ods. 1, 2, 3 a 4 a článku 9 tejto smernice, ak také obmedzenie predstavuje nevyhnutné, vhodné a primerané opatrenie v demokratickej spoločnosti na zabezpečenie národnej bezpečnosti (t. j. bezpečnosti štátu), obrany, verejnej bezpečnosti a na zabránenie, vyšetrovanie, odhaľovanie a stíhanie trestných činov alebo neoprávnené používanie elektronického komunikačného systému podľa článku 13 ods. 1 smernice 95/46/ES. Na tento účel členské štáty môžu medzi iným, okrem iného prijať legislatívne opatrenia umožňujúce zadržanie údajov na limitované obdobie, oprávnené z dôvodov ustanovených v tomto odseku. Všetky opatrenia uvedené v tomto odseku musia byť v súlade so všeobecnými princípmi práva spoločenstva vrátane tých, ktoré sú uvedené v článku 6 ods. 1 a 2 Zmluvy o Európskej únii.“* Smernica 2002/58/ES v citovanom ustanovení pripúšťa výnimku z uplatnenia jej ustanovení zavádzajúcich povinnosť poskytovateľov elektronických komunikácií vymazať prevádzkové údaje a údaje o polohe vytvorené používaním elektronických komunikačných služieb alebo zabezpečiť ich anonymnosť, ak už nie sú naďalej potrebné na účely prenosu komunikácie, s výnimkou údajov potrebných na účtovanie alebo pre poplatky za prepojenie, z dôvodu zabezpečenia primeranej úrovne ochrany základných práv a slobôd a najmä práva na súkromie v oblasti spracovávania osobných údajov v elektronickom komunikačnom sektore.

68. Napadnuté ustanovenia zákona o elektronických komunikáciách tak aj po vyhlásení smernice 2006/24/ES za neplatnú Súdnym dvorom ostávajú vo sfére pôsobnosti práva Európskej únie, keďže predstavujú výnimku z uplatňovania únijných pravidiel (smernice 2002/58/ES) prípustnú samotným právom Únie (čl. 15 ods. 1 smernice. 2002/58/ES). Rovnako tak aj napadnuté ustanovenia Trestného poriadku a zákona

o Policajnom zbore je potrebné z dôvodu ich povahy a cieľov, ktoré sledujú, považovať za úpravu spadajúcu do rámca pôsobnosti čl. 15 ods. 1 smernice 2002/58/ES (pozri v tomto ohľade: rozsudok *Kreshnik Ymeraga a iní proti Ministre du Travail, de l'Emploi et de l'Immigration*, C-87/12, EU:C:2013:291, bod 41; rozsudok *Cruciano Siragusa proti Regione Sicilia – Soprintendenza Beni Culturali e Ambientali di Palermo*, C-206/13, EU:C:2014:126, bod 25). V rámci ústavného prieskumu napadnutých ustanovení zákona o elektronických komunikáciách, Trestného poriadku a zákona o Policajnom zbore musí preto ústavný súd zohľadniť aj znenie relevantných ustanovení charty, konkrétne v rozsahu návrhu skupiny poslancov, predovšetkým čl. 7, čl. 8 a čl. 52 ods. 1 charty a príslušnú judikatúru Súdneho dvora Európskej únie.

69. Ústavný súd od začiatku svojej činnosti v súlade s princípom *pacta sunt servanda* konštantne judikuje, že základné práva a slobody podľa ústavy je potrebné vykladať a uplatňovať v zmysle a duchu medzinárodných zmlúv o ľudských právach a základných slobodách (PL. ÚS 5/93, PL. ÚS 15/98, PL. ÚS 17/00, PL. ÚS 24/2014). Ústavný súd tak vždy, pokiaľ to ústava svojím znením nevylučovala, prihliadal pri vymedzení obsahu základných práv a slobôd ustanovených v ústave aj na znenie týchto zmlúv a príslušnú judikatúru k nim vydanú (II. ÚS 55/98, PL. ÚS 24/2014). Charta (Ú. v. EÚ C- 326, 26. 10. 2012, s. 391 – 407) síce nebola prijatá vo forme medzinárodnej zmluvy, nadobudnutím platnosti Lisabonskej zmluvy sa však stala právne záväznou súčasťou primárneho práva Európskej únie s rovnakou právnou silou ako zmluvy, na ktorých je Únia založená (čl. 6 ods. 1 Zmluvy o Európskej únii v znení Lisabonskej zmluvy). Postavenie zmlúv, na ktorých je Únia založená (Zmluva o Európskej únii a Zmluva o fungovaní Európskej únie), v právnom poriadku Slovenskej republiky upravujú čl. 1 ods. 2 ústavy a čl. 7 ods. 5 ústavy. Článok 1 ods. 2 ústavy upravuje záväzok Slovenskej republiky uznávať a dodržiavať všeobecné pravidlá medzinárodného práva, medzinárodné zmluvy, ktorými je viazaná, ako aj jej ďalšie medzinárodné záväzky. Článok 7 ods. 5 ústavy vymenúva kategórie medzinárodných zmlúv, ktoré majú prednosť pred zákonmi. Do kategórií medzinárodných zmlúv uvedených v tomto ustanovení možno nepochybne zaradiť aj zmluvy, na ktorých je založená Únia. Charte majúcej rovnakú právnu silu ako zmluvy, na ktorých je Únia

založená, je preto potrebné v ústavnom poriadku Slovenskej republiky priznať také postavenie, aké ústava v čl. 7 ods. 5 priznáva uvedeným kategóriám medzinárodných zmlúv. Konkrétne charte je potrebné v ústavnom poriadku Slovenskej republiky priznať postavenie, aké majú podľa čl. 7 ods. 5 ústavy medzinárodné zmluvy o ľudských právach a základných slobodách.

70. Podľa čl. 125 ods. 1 písm. a) ústavy ústavný súd rozhoduje o súlade zákonov s ústavou, s ústavnými zákonmi a s medzinárodnými zmluvami, s ktorými vyslovila súhlas národná rada a ktoré boli ratifikované a vyhlásené spôsobom ustanoveným zákonom. Z citovaného textu vyplýva, že právomoc ústavného súdu podľa čl. 125 ods. 1 písm. a) ústavy sa vzťahuje aj na medzinárodné zmluvy, s ktorými vyslovila súhlas národná rada a ktoré boli ratifikované a vyhlásené spôsobom ustanoveným zákonom [to isté platí aj o právomoci podľa čl. 125 ods. 1 písm. b), c) a d) ústavy, pozn.].

71. Národná rada uznesením č. 365 z 1. júla 2003 vyslovila súhlas so Zmluvou o pristúpení Slovenskej republiky k Európskej únii (ďalej len „zmluva o pristúpení“) a súčasne rozhodla, že ide o zmluvu podľa čl. 7 ods. 5 ústavy, ktorá má prednosť pred zákonmi Slovenskej republiky. Prezident Slovenskej republiky zmluvu ratifikoval 26. augusta 2003, platnosť nadobudla 1. mája 2004 a v Zbierke zákonov Slovenskej republiky bola uverejnená pod č. 185/2004 Z. z. Súčasťou zmluvy o pristúpení bola aj zmena a doplnenie Zmluvy o založení Európskeho spoločenstva a Zmluvy o Európskej únii.

72. Uznesením č. 809 z 10. apríla 2008 národná rada vyslovila súhlas s Lisabonskou zmluvou, ktorou sa mení a dopĺňa Zmluva o Európskej únii a Zmluva o založení Európskeho spoločenstva (touto zmluvou došlo okrem iných zmien k premenovaniu Zmluvy o založení Európskeho spoločenstva na Zmluvu o fungovaní Európskej únie a k nadobudnutiu právnej záväznosti charty priznaním jej rovnakej právnej sily, ako majú zmluvy, na ktorých je Únia založená; konsolidované znenie Zmluvy o Európskej únii a Zmluvy o fungovaní Európskej únie, teda znenie so zapracovanými zmenami zavedenými Lisabonskou zmluvou bolo uverejnené v Úradnom vestníku Európskej únie C 83

z 30. marca 2010, pozn.), a zároveň rozhodla, že ide o zmluvu podľa čl. 7 ods. 5 ústavy, ktorá má prednosť pred zákonmi Slovenskej republiky. Prezident Slovenskej republiky ratifikačnú listinu podpísal 12. mája 2008 a Lisabonská zmluva nadobudla platnosť 1. decembra 2009. V Zbierke zákonov Slovenskej republiky bola uverejnená pod č. 486/2009 Z. z.

73. Na tomto základe možno do subkategórie medzinárodných zmlúv podľa čl. 7 ods. 5 ústavy zaradiť aj zmluvu o pristúpení a jej prostredníctvom Zmluvu o založení Európskeho spoločenstva a Zmluvu o Európskej únii a Lisabonskú zmluvu, ktorá premenovala Zmluvu o založení Európskeho spoločenstva na Zmluvu o fungovaní Európskej únie. Na základe čl. 6 ods. 1 Zmluvy o Európskej únii, ktorý priznáva charte rovnakú právnu silu, ako majú zmluvy, na ktorých je Únia založená, možno charte priznať v právnom poriadku Slovenskej republiky rovnaké postavenie, ako majú medzinárodné zmluvy podľa čl. 7 ods. 5 ústavy. Ide zároveň nepochybne o zmluvy, ktoré spĺňajú kritériá ustanovené v čl. 125 ods. 1 ústavy.

74. Vychádzajúc z konštantnej judikatúry ústavného súdu, ktorá v súlade s princípom *pacta sunt servanda* požaduje, aby základné práva a slobody podľa ústavy boli vykladané a uplatňované minimálne v zmysle a duchu medzinárodných zmlúv o ľudských právach a základných slobodách (PL. ÚS 5/93, PL. ÚS 15/98, PL. ÚS 17/00, PL. ÚS 24/2014) a príslušnej judikatúry k nim vydanej (II. ÚS 55/98, PL. ÚS 24/2014), základné práva a slobody podľa ústavy je potrebné v prípade, ak napadnutá vnútroštátna právna úprava spadá do rámca pôsobnosti práva Únie, vykladať a uplatňovať aj v zmysle a duchu charty a príslušnej judikatúry Súdneho dvora k nej vydanej.

75. Povinnosť členských štátov vykladať a uplatňovať príslušné ustanovenia ústavy v zmysle a duchu charty a príslušnej judikatúry Súdneho dvora k nej vydanej, v prípade, ak vnútroštátne opatrenie spadá do rámca pôsobnosti práva Únie, vyplýva aj z čl. 4 ods. 3 Zmluvy o Európskej únii, ktorý *inter alia* požaduje, aby členské štáty prijali všetky

opatrenia všeobecnej alebo osobitnej povahy, aby zabezpečili plnenie záväzkov vyplývajúcich zo zmlúv alebo z aktov inštitúcií Únie.

76. Ústavný súd však považuje za potrebné poukázať aj na svoju predchádzajúcu judikatúru (PL. ÚS 3/09), podľa ktorej v prípade, ak v konaní podľa čl. 125 ods. 1 písm. a) ústavy ústavný súd zistí a rozhodne, že napadnutý zákon, jeho časť alebo niektoré jeho ustanovenia nie sú v súlade s ústavou alebo ústavným zákonom, nie je v zásade už potrebné preskúmavať aj ich nesúlad s právom Európskej únie (aj napriek tomu, že to navrhovatelia navrhujú), pretože aj ich prípadný nesúlad by viedol len k rovnakému výsledku a rovnakým právnym účinkom, aké sa dosiahli rozhodnutím, podľa ktorého napadnutá právna úprava nie je v súlade s ústavou alebo ústavným zákonom. Takýto „samo obmedzujúci“ prístup k výkonu svojej právomoci ústavný súd odôvodňuje tým, že po vyslovení nesúladu s ústavou alebo ústavnými zákonmi zaniká predmet konania o súlade právnych predpisov vo vzťahu k namietanému nesúladu s právom Európskej únie.

III.4 Základná charakteristika práva na súkromie, všeobecne k východiskám a kritériám posudzovania zásahu do súkromia

(právo na nedotknuteľnosť osoby a jej súkromia podľa čl. 16 ods. 1 ústavy a čl. 7 ods. 1 listiny, právo na ochranu pred neoprávneným zasahovaním do súkromného a rodinného života podľa čl. 19 ods. 2 ústavy a čl. 10 ods. 2 listiny, právo na ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov podľa čl. 19 ods. 3 ústavy a čl. 10 ods. 3 listiny, právo na ochranu osobných údajov podľa čl. 22 ústavy a čl. 13 listiny, právo na rešpektovanie súkromného života a korešpondencie podľa čl. 8 dohovoru, právo na rešpektovanie súkromného života podľa čl. 7 charty a právo na ochranu osobných údajov podľa čl. 8 charty)

77. Podľa čl. 16 ods. 1 ústavy a čl. 7 ods. 1 listiny nedotknuteľnosť osoby a jej súkromia je zaručená. Obmedzená môže byť len v prípadoch ustanovených zákonom.

78. Podľa čl. 19 ods. 2 ústavy a čl. 10 ods. 2 listiny každý má právo na ochranu pred neoprávneným zasahovaním do súkromného a rodinného života.

79. Podľa čl. 19 ods. 3 ústavy a čl. 10 ods. 3 listiny každý má právo na ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe.

80. Podľa čl. 22 ods. 1 ústavy listové tajomstvo, tajomstvo dopravovaných správ a iných písomností a ochrana osobných údajov sa zaručujú. Podľa čl. 22 ods. 2 ústavy a čl. 13 listiny nikto nesmie porušiť listové tajomstvo ani tajomstvo iných písomností a záznamov, či už uchovávaných v súkromí, alebo zasielaných poštou, alebo iným spôsobom; výnimkou sú prípady, ktoré ustanoví zákon. Rovnako sa zaručuje tajomstvo správ podávaných telefónom, telegrafom alebo iným podobným zariadením.

81. Uvedené ustanovenia ústavy a listiny zakotvujú právo na ochranu súkromia. V zmysle ustálenej judikatúry ústavného súdu (I. ÚS 274/05) ochrana súkromia je zakotvená vo viacerých ustanoveniach ústavy a listiny vrátane čl. 19 ods. 3 ústavy, čl. 22 ústavy, čl. 10 ods. 3 a čl. 13 listiny. Súkromím sa chápe predovšetkým sféra života človeka, do ktorej nemožno zasahovať bez jeho súhlasu. Právom na súkromie sa zaručuje osobe možnosť rozhodovať samostatne o tých svojich záležitostiach, ktoré sa uznávajú za súkromie. Podľa judikatúry ústavného súdu právo na ochranu pred neoprávneným zasahovaním do súkromnej sféry jednotlivca zahŕňa nielen negatívnu povinnosť štátu zdržať sa mocenského zásahu, ale aj jeho pozitívny záväzok prijať účinné opatrenia na zabezpečenie jeho efektívnej ochrany (III. ÚS 331/09). Prelomovým rozhodnutím v tomto smere bolo rozhodnutie Európskeho súdu pre ľudské práva (ďalej aj „ESĽP“) vo veci *Marckx c. Belgicko* z 13. júna 1979, ktoré rozšírilo ochranu práva na súkromie aj na prípady, keď štát nevytvoril podmienky proti porušeniu tohto práva, z čoho bol odvodený tzv. pozitívny záväzok štátu na vytvorenie takých podmienok, ktoré by znemožňovali porušenie práva na súkromie (III. ÚS 133/2010).

82. S ohľadom na svoju konštantnú judikatúru ústavný súd vždy, pokiaľ to ústava svojím znením nevylučuje, prihliada pri vymedzení obsahu základných práv a slobôd ustanovených v ústave aj na znenie medzinárodných zmlúv o ľudských právach a základných slobodách a príslušnú judikatúru k nim vydanú (II. ÚS 55/98, PL. ÚS 24/2014).

83. Podľa čl. 8 ods. 1 dohovoru každý má právo na rešpektovanie svojho súkromného a rodinného života, obydlia a korešpondencie. Podľa čl. 8 ods. 2 dohovoru štátny orgán nemôže do výkonu tohto práva zasahovať okrem prípadov, keď je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom a zločinnosti, ochrany zdravia alebo morálky, alebo ochrany práv a slobôd iných.

84. Naproti zneniu ústavy a listiny ochrana práva na súkromie je v dohovore sústredená do jedného článku, článku 8. Keďže základné práva a slobody podľa ústavy je potrebné vykladať a uplatňovať v zmysle a duchu medzinárodných zmlúv o ľudských právach a základných slobodách (PL. ÚS 5/93, PL. ÚS 15/98, PL. ÚS 24/2014) a príslušnú judikatúru k nim vydanú, ústavný súd pri vymedzení obsahu a rozsahu ochrany práva na súkromie prihliada aj na príslušnú judikatúru ESĽP týkajúcu sa čl. 8 dohovoru.

85. Pri posudzovaní zásahov štátu do práva na súkromie ESĽP uplatňuje mechanizmus postupnosti skúmania niekoľkých hľadísk. V prvom rade skúma, či daný skutkový stav možno *ratione materiae* považovať za súčasť práva na súkromie. Po kladnej odpovedi na túto otázku ESĽP následne pristupuje k posúdeniu kritéria legality zásahu, jeho legitímnosti a napokon jeho proporcionality. Ak ESĽP dospeje k negatívnej odpovedi pri niektorej z týchto otázok, ďalej už v posudzovaní zásahov štátu do práva na súkromie nepokračuje.

86. Vychádzajúc z úpravy dohovoru a jeho dodatkov možno v zásade právo na súkromie rozdeliť na dve oblasti, a to právo na súkromný život a právo na rodinný život.

Podľa obsahového zamerania judikatúry ESĽP možno potom právo na súkromný život vymedziť ako a) zákaz zhromažďovania a úschovy osobných údajov, b) práva spojené s menšinovou sexuálnou orientáciou, c) ochranu obydlia a domovú slobodu, d) ochranu korešpondencie a tajomstva dopravovaných správ.

87. Európsky súd pre ľudské práva vo veci *Malone proti UK* (č. 8691/79 z 2. 8. 1984) pri výklade čl. 8 dohovoru viackrát zdôraznil, že zber a uchovávanie údajov týkajúcich sa súkromného života jednotlivca spadajú pod rozsah čl. 8 dohovoru, pretože výraz „súkromný život" nesmie byť interpretovaný reštriktívne. Právo na súkromný život tak v sebe zahŕňa i právo na ochranu pred sledovaním, striehnutím a prenasledovaním zo strany verejnej moci, a to i vo verejnom priestore či na verejne prístupných miestach. Navyše, žiadny zásadný dôvod neumožňuje vylúčiť z pojmu súkromný život profesijné, obchodné či sociálne aktivity (rozhodnutie ESĽP vo veci *Niemietz proti Nemecku,* č. 13710/88 zo 16. 12. 1992). Podľa ESĽP tento extenzívny výklad pojmu „súkromný život" je v súlade s Dohovorom Rady Európy č. 108 o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (tento dohovor a dodatky k tomuto dohovoru nadobudli pre Slovenskú republiku platnosť 1. januára 2001, publikovaný v Zbierke zákonov Slovenskej republiky vo forme Oznámenia Ministerstva zahraničných vecí Slovenskej republiky č. 49/2001 Z. z.), ktorého účelom je *„zabezpečiť pre každého jednotlivca na území každej strany dohovoru rešpektovanie jeho práv a základných slobôd, najmä práva na súkromie pri automatizovanom spracovaní osobných údajov o ňom..."* (čl. 1 Dohovoru o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov), pričom podľa čl. 2 tohto dohovoru sa osobnými údajmi rozumejú *„všetky informácie, ktoré sa vzťahujú na nejakého identifikovaného alebo identifikovateľného jednotlivca"*.

88. Európsky súd pre ľudské práva vo svojej judikatúre k právu na rešpektovanie súkromného života podľa čl. 8 dohovoru označil za zásahy do súkromia jednotlivca zásahy v podobe kontroly dát, obsahu pošty či odpočúvaní telefónnych rozhovorov (rozhodnutie ESĽP vo veci *Klass a další proti Nemecku*, č. 5029/71, zo 6. 9. 1978; rozhodnutie ESĽP vo veci *Leander proti Švédsku*, č. 9248/81, z 26. 3. 1987; rozhodnutie ESĽP vo veci *Kruslin*

proti Francúzsku, č. 11801/85, z 24. 4. 1990; rozhodnutie ESĽP vo veci *Kopp proti Švajčiarsku*, č. 23224/94, z 25. 3. 1998), zisťovanie telefónnych čísel telefonujúcich osôb (rozhodnutie ESĽP vo veci *P.G. a J.H. proti UK*, č. 44787/98, z 25. 9. 2001) zisťovanie údajov o telefónnom spojení (rozhodnutie ESĽP vo veci *Amann proti Švajčiarsku*, zo 16. 2. 2000, č. 27798/95) alebo uchovávanie údajov DNA jednotlivcov v databázach obvinených (rozhodnutie ESĽP vo veci *S. a Marper proti UK*, č. 30562/04 a 30566/04, zo 4. 12. 2008). V rozhodnutí vo veci *Rotaru proti Rumunsku* (č. 28314/95 zo 4. 5. 2000) ESĽP vyvodil z práva na súkromný život i pozitívnu povinnosť štátu zlikvidovať údaje, ktoré o osobe z jej súkromnej sféry štát zhromaždil a spracoval.

89. Obdobný prístup k ochrane súkromia zastáva aj judikatúra zahraničných ústavných súdov. Napríklad Spolkový ústavný súd Nemecka prostredníctvom práva na informačné sebaurčenie garantuje ochranu nielen obsahu predávaných informácií, ale chráni rovnako aj vonkajšie okolnosti, za ktorých sa uskutočňujú – t. j. miesto, čas, účastníkov, druh a spôsob komunikácie, pretože poznanie okolností uskutočnenej komunikácie môže v spojení s ďalšími údajmi samo osebe indikovať samotný obsah komunikácie a za pomoci skúmania týchto údajov a ich analýzy možno zhotoviť individuálne profily účastníkov danej komunikácie [napr. rozhodnutie z 27. 7. 2005, BVerfGE 113, 348 (*Vorbeugende Telekommunikationsüberwachung*) alebo z 27. 2. 2008, BVerfGE 120, 274 (*Grundrecht auf Computerschutz*)].

90. Legalita zásahu štátu do práva na súkromie znamená, že zásah je možný len na základe zákona, resp. platného právneho predpisu, pričom pri posudzovaní splnenia tejto podmienky sa vychádza z toho, či bola rešpektovaná dostupnosť (verejné publikovanie právneho predpisu) a predvídateľnosť zákona. V rámci podmienky predvídateľnosti zákona judikatúra ESĽP zdôrazňuje potrebu konkretizovania prostriedkov, ktorými štát disponuje pri zasahovaní do práv chránených čl. 8 dohovoru, teda dôraz kladie na kvalitu relevantnej právnej úpravy. V rozhodnutí *Sallinen c. Fínsko* z 27. decembra 2005 ESĽP vyslovil záver, že vnútroštátne právo musí poskytovať jednotlivcovi ochranu proti arbitrárnemu zásahu do jeho práv zaručených čl. 8 dohovoru, preto musí dostatočne jasne v pojmoch poskytovať

občanovi náležitú indikáciu podľa okolností a podmienok, za akých je verejná autorita zmocnená na zásahy do jeho práva na súkromie.

91. Podmienka legitímnosti vyžaduje, aby opatrenie umožňujúce zásah štátu do práva na súkromie zodpovedalo cieľu odôvodňujúcemu jeho legitimitu, ktorým môžu byť len záujmy výslovne špecifikované dohovorom, a síce záujem štátu (z dôvodu ochrany národnej bezpečnosti, verejnej bezpečnosti, predchádzania nepokojov a zločinnosti), záujem spoločnosti (z dôvodu ochrany zdravia alebo morálky, zabezpečenia hospodárskeho blahobytu krajiny) a záujem jednotlivcov (z dôvodu ochrany ich práv a slobôd).

92. Kritérium proporcionality zásahu znamená dodržanie rovnováhy vo vzťahu medzi právom jednotlivca na súkromie a výberom prostriedkov, ktorými štát disponuje pri plnení legitímneho cieľa. Pri ich výbere je limitovaný tým, že zásah do práva na súkromie je možný len vtedy, keď to je nevyhnutné, a vykonať ho možno len v duchu požiadaviek kladených na demokratickú spoločnosť. Európsky súd pre ľudské práva vo svojej rozhodovacej činnosti zdôraznil, že pri zásahoch do práva na súkromie v súlade s dohovorom sa štát nemôže dovolávať iba akejsi „všeobecnej nevyhnutnosti“. Termín „nevyhnutný“ nie je pritom podľa názoru ESĽP až taký flexibilný, aby sa mohol interpretovať ako „užitočný“, „primeraný“ alebo „žiaduci“, ale musí sa spájať s existenciou „naliehavej spoločenskej potreby“ vykonať daný zásah. Pre výklad pojmu „demokratická spoločnosť“ je zasa pre ESĽP dôležité jej spojenie s pluralizmom, toleranciou a duševnou slobodou.

93. Aj ústavný súd judikoval, že zásah do základného práva alebo slobody musí zodpovedať naliehavej spoločenskej potrebe a musí byť primeraný sledovanému legitímnemu cieľu a zároveň pri určovaní rozsahu obmedzenia je dôležité zohľadniť aj podstatu práva, ktoré sa má obmedziť (pozri I. ÚS 13/00). Podľa čl. 13 ods. 4 ústavy pri obmedzovaní základných práv a slobôd sa musí dbať na ich podstatu a zmysel, pričom takéto obmedzenia sa môžu použiť len na ustanovený cieľ.

94. Na posúdenie ústavnej akceptovateľnosti zásahu do základného práva alebo slobody ústavný súd obdobne ako ESĽP podrobuje napadnutú právnu úpravu testu proporcionality.

95. Test proporcionality uskutočňovaný v rámci ústavného prieskumu napadnutej právnej úpravy je klasicky založený na troch po sebe nasledujúcich krokoch. Prvým krokom je test existencie ústavou nevylúčeného a dostatočne dôležitého cieľa (test of legitimate aim/effect) a tiež test racionálnej väzby medzi napadnutou právnou úpravou a ňou sledovaným cieľom [účelom (conduciveness)], teda hľadisko vhodnosti (Geeignetheit). Druhým krokom je zisťovanie kritéria nevyhnutnosti, resp. potrebnosti či použitia najmenej drastických, resp. šetrnejších prostriedkov (Erforderlichkeit, test of necessity, test of subsidiarity, least intrusiveness) na dosiahnutie cieľa sledovaného napadnutou právnou úpravou. Napokon tretím krokom je hľadisko proporcionality v užšom zmysle slova (Angemessenheit, test of proporcionality in the strict sense, proporcionate effect; not overly onerous), ktorého obsah tvorí porovnanie miery zásahov do ústavou chránených hodnôt vyvolané uplatnením napadnutej právnej úpravy (pozri PL. ÚS 11/2013, PL. ÚS 3/09, m. m. PL. ÚS 19/09, m. m. PL. ÚS 23/06).

96. Vzhľadom na skutočnosť, že napadnuté ustanovenia zákona o elektronických komunikáciách, Trestného poriadku a zákona o Policajnom zbore spadajú do pôsobnosti práva Európskej únie, nemožno opomenúť príslušné ustanovenia charty a judikatúru Súdneho dvora.

97. Článok 7 charty zakotvuje právo na rešpektovanie súkromného života, obydlia a komunikácie. Podľa čl. 8 charty každý má právo na ochranu osobných údajov, ktoré sa ho týkajú. Podľa judikatúry Súdneho dvora čl. 7 a 8 charty uznávajú dodržiavanie práva na ochranu súkromného života v súvislosti so spracúvaním osobných údajov (rozsudok *Volker und Markus Schecke GbR a Hartmut Eifert proti Land Hessen*, C-92/09 a C-93/09, EU:C:2010:662, body 47, 52). Korene práva na ochranu osobných údajov ležia v práve na súkromie [PEERS, S. – HERVEY, T. – KENNER, J. – WARD, A. (ed.) The EU Charter of

Fundamental Rights. A Commentary. Oxford and Portland, Oregon : Hart Publishing, 2014. ISBN (Hart Publishing): 978-1-84946-308-9, s. 228].

98. Spojitosť medzi právom na súkromie podľa čl. 7 charty a právom na ochranu osobných údajov podľa čl. 8 charty spočíva v koncepte informačného sebaurčenia, ktorý implikuje nutnosť existencie kontroly jednotlivca nad informáciami dotýkajúcimi sa jeho osoby. Koncept informačného sebaurčenia spočíva v nároku jednotlivca určiť, kedy, ako a v akom rozsahu budú informácie o ňom sprístupnené ostatným. Koncept informačného sebaurčenia sa zakladá na existencii súhlasu jednotlivca so spracovaním údajov o jeho osobe. Ak by ochrana osobných údajov mala spočívať len v informačnom sebaurčení jednotlivca a právo na súkromie by spočívalo v práve na informačné sebaurčenie, tak medzi právom na súkromie podľa čl. 7 charty a právom na ochranu osobných údajov podľa čl. 8 charty by nebol zásadný rozdiel. Koncept ochrany osobných údajov uplatňovaný v rámci Európskej únie, ako aj Rady Európy však ide nad rámec konceptu informačného sebaurčenia.

99. Dohovor Rady Európy č. 108 o ochrane jednotlivcov pri automatickom spracovávaní osobných údajov požaduje súhlas dotknutej osoby pri spracovaní osobných údajov len v čl. 15 ods. 3, a to vo vzťahu k ustanoveniam upravujúcim pomoc dotknutým osobám, ktoré sú rezidentmi inej krajiny. Koncept súhlasu dotknutej osoby so spracovaním osobných údajov nehrá v Dohovore Rady Európy č. 108 kľúčovú úlohu. Obdobne je to tak aj v rámci Eúrópskej únie. Sekundárna úprava Európskej únie týkajúca sa ochrany osobných údajov (na ktorú odkazujú aj vysvetlivky k čl. 8 charty) považuje súhlas dotknutej osoby so spracovaním osobných údajov len za jeden z viacerých možných základov prípustného (legálneho) spracovania osobných údajov (pozri tiež čl. 7 Dohovoru Rady Európy č. 108). Sekundárna normotvorba Európskej únie týkajúca sa ochrany osobných údajov [Smernica Rady č. 95/46/EHS o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov (ďalej len „smernica 95/46/EHS“) a smernica 2002/58/ES] zavádza úpravu ochrany osobných údajov, ktorá ide nad rámec požiadavky súhlasu dotknutej osoby so spracovaním osobných údajov. Sekundárna únijná úprava ochrany osobných údajov

zavádza systém záruk (kontroly a vyváženosti, angl. „check and balances“), ktorý má zabezpečiť legalitu (prípustnosť) procesu spracovania osobných údajov aj bez existencie predchádzajúceho výslovného súhlasu dotknutej osoby.

100. Podľa judikatúry Súdneho dvora obmedzenia, ktorými možno legitímne obmedziť práva zaručené čl. 7 a čl. 8 charty, zodpovedajú obmedzeniam prípustným podľa čl.8 dohovoru (rozsudok *Volker und Markus Schecke GbR a Hartmut Eifert proti Land Hessen*, C-92/09 a C-93/09, EU:C:2010:662, bod 52). Súdny dvor zároveň dodáva, že dodržiavanie práva na ochranu súkromného života v súvislosti so spracovávaním osobných údajov, ktoré uznávajú čl. 7 a čl. 8 charty, možno obmedziť za podmienok vyplývajúcich z čl. 8 ods. 2 charty a čl. 52 ods. 1 charty [rozsudok *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) a Federación de Comercio Electrónico y Marketing Directo (FECEMD) proti Administración del Estado*, C-468/10 a C-469/10, EU:C:2011:777, bod 42]. Akýkoľvek zásah do výkonu práv uznaných čl. 7 a čl. 8 charty je preto potrebné považovať za prípustný, len pokiaľ spadá pod obmedzenia prípustné čl. 8 ods. 2 charty, čl. 52 ods. 1 charty a čl. 8 ods. 2 dohovoru (okrem už spomenutých rozsudkov Súdneho dvora pozri aj rozsudok *Michael Schwarz proti Stadt Bochum*, C-291/12, EU:C:2013:670, body 32– 34).

101. Súdny dvor v rozhodnutí v spojených veciach C-293/12 a C-594/12 *Digital Rights Ireland Ltd*, ktorým zrušil platnosť smernice 2006/24/ES, poukázal na skutočnosť, že prípustnosť uchovávať osobné údaje bez súhlasu dotknutých osôb je možná len v prípade, ak poskytovatelia verejne dostupných elektronických komunikačných služieb alebo verejnej komunikačnej siete majú povinnosť dodržať určité zásady ochrany a bezpečnosti údajov, podľa ktorých členské štáty dbajú na to, aby sa prijali vhodné technické a organizačné opatrenia proti náhodnému alebo nezákonnému zničeniu, ako aj proti strate či náhodnej zmene údajov.

102. Podľa Súdneho dvora (rozsudok *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources a iní a Kärntner Landesregierung a iní*, C-

293/12 a C-594/12, EU:C:2014:238, bod 54) právna úprava uchovávania údajov musí stanoviť jasné a presné pravidlá upravujúce rozsah a uplatnenie predmetného opatrenia a ukladajúce minimálne požiadavky spôsobom, aby osoby, ktorých údaje boli uchované, mali dostatočné záruky umožňujúce účinne chrániť ich osobné údaje proti rizikám zneužitia, ako aj proti akémukoľvek nezákonnému prístupu a akémukoľvek nezákonnému použitiu týchto údajov (v tejto súvislosti pozri analogicky rozsudky ESĽP z 1. 7. 2008, *Liberty a i. v. Spojené kráľovstvo*, č. 58243/00, body 62 a 63; *Rotaru v. Rumunsko*, už citovaný, body 57 až 59, ako aj *S a Marper v. Spojené kráľovstvo*, už citovaný, bod 99). Nevyhnutnosť disponovať takými zárukami je pritom podľa Súdneho dvora o to dôležitejšia, keď sú osobné údaje spracovávané automaticky a keď existuje značné riziko nezákonného prístupu k týmto údajom (v tejto súvislosti pozri analogicky rozsudky ESĽP, *S a Marper v. Spojené kráľovstvo*, už citovaný, bod 103, ako aj *M. K. v. Francúzsko*, č. 19522/09, bod 35 z 18. 4. 2013).

103. Podľa Súdneho dvora (rozsudok *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources a iní a Kärntner Landesregierung a iní*, C-293/12 a C-594/12, EU:C:2014:238, bod 65) právna úprava uchovávania osobných údajov musí stanovovať jasné a presné pravidlá upravujúce rozsah zásahu do základných práv zakotvených v čl. 7 a 8 charty. Zásah do týchto základných práv musí byť presne vymedzený ustanoveniami, ktoré majú zaručiť, že sa tento zásah obmedzí iba na to najnevyhnutnejšie. Právna úprava uchovávania osobných údajov musí stanovovať pravidlá, ktoré jasným a reštriktívnym spôsobom upravujú ochranu a bezpečnosť predmetných údajov, aby sa zaručila ich úplná integrita a dôvernosť (rozsudok *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources a iní a Kärntner Landesregierung a iní*, C-293/12 a C-594/12, EU:C:2014:238, bod 66). Právna úprava uchovávania osobných údajov musí zaručovať, že poskytovatelia verejne dostupných elektronických komunikačných služieb alebo verejných komunikačných sietí uplatnia mimoriadne vysokú úroveň ochrany a bezpečnosti osobných údajov pomocou technologických a organizačných opatrení.

IV. Analýza napadnutej právnej úpravy a závery

IV.1 K namietanému nesúladu napadnutých ustanovení zákona o elektronických komunikáciách s právom na ochranu súkromia

O existencii zásahu do práva na súkromie

104. Napadnuté ustanovenia zákona o elektronických komunikáciách ustanovujú povinnosť poskytovateľov elektronických komunikácií uchovávať prevádzkové údaje, lokalizačné údaje a údaje komunikujúcich strán v rozsahu, v akom ich vytvárajú alebo spracuvávajú pri poskytovaní služby alebo siete, vrátane údajov súvisiacich s neúspešnými pokusmi o volanie, ktoré podnik vytvára alebo spracúva a ukladá, ak ide o telefónne údaje, alebo zaznamenáva, ak ide o internetové údaje. Podľa § 57 ods. 1 zákona o elektronických komunikáciách sa prevádzkovými údajmi rozumejú údaje vzťahujúce sa na užívateľa a na konkrétny prenos informácií v sieti a vznikajúce pri tomto prenose, ktoré sa spracúvajú na účely prenosu správy v sieti alebo na účely fakturácie. Podľa § 57 ods. 2 toho istého zákona sa lokalizačnými údajmi rozumejú údaje spracúvané v sieti alebo prostredníctvom služby, ktoré označujú geografickú polohu koncového zariadenia užívateľa verejnej služby. Zoznam údajov, ktoré je poskytovateľ elektronických komunikácií povinný uchovávať, je podrobne vymedzený v prílohe č. 2 zákona o elektronických komunikáciách. Ide o údaje potrebné na zistenie a identifikáciu zdroja komunikácie, údaje potrebné na identifikáciu adresáta komunikácie, údaje potrebné na identifikáciu dátumu, času a trvania komunikácie, údaje potrebné na identifikáciu typu komunikácie, údaje potrebné na identifikáciu koncového zariadenia užívateľov alebo ich údajného zariadenia a údaje potrebné na identifikáciu polohy mobilného koncového zariadenia.

105. Konkrétne, pokiaľ ide o telefónne spojenie prostredníctvom pevnej siete a mobilné telefónne spojenie, poskytovatelia elektronickej komunikácie sú povinní uchovávať telefónne číslo volajúceho a volaného v prípadoch, keď sú poskytnuté doplnkové

služby, napríklad presmerovanie alebo odovzdanie volania, číslo alebo čísla, na ktoré je volanie smerované, meno, priezvisko a adresu trvalého pobytu, alebo obchodné meno a sídlo alebo miesto podnikania účastníka alebo registrovaného užívateľa, dátum a čas začatia a ukončenia komunikácie, používaná telefónna služba, ak ide o mobilné telefónne spojenie IMSI volajúceho a volaného, IMEI volajúceho a volaného, v prípade mobilného koncového zariadenia údaje o polohe bunky pri začatí komunikácie či údaje identifikujúce zemepisnú polohu buniek podľa ich označenia počas obdobia uchovávania údajov o komunikácii. Pokiaľ ide o pripojenie k internetu, internetovú elektronickú poštu a telefonovanie prostredníctvom internetu, poskytovatelia elektronickej komunikácie sú povinní uchovávať pridelené označenie užívateľa, označenie užívateľa a telefónne číslo pridelené každej komunikácii, ktorá vstupuje do verejnej telefónnej siete, meno, priezvisko a adresu trvalého pobytu, alebo obchodné meno a sídlo alebo miesto podnikania účastníka alebo registrovaného užívateľa a adresu internetového protokolu (IP), ktorá mu bola v čase komunikácie pridelená, označenie užívateľa alebo telefónne číslo, označenie užívateľa alebo telefónne číslo určených príjemcov telefónneho volania, meno, priezvisko a adresu trvalého pobytu, alebo obchodné meno a sídlo alebo miesto podnikania účastníka alebo registrovaného užívateľa, ktorý je určeným príjemcom komunikácie, dátum a čas prihlásenia a odhlásenia zo služby pripojenia k internetu v určitom časovom pásme spolu s dynamickou alebo statickou IP adresou, ktorú komunikácii pridelil poskytovateľ služby pripojenia k internetu, a užívateľské označenie účastníka alebo registrovaného užívateľa, dátum a čas prihlásenia a odhlásenia zo služieb internetovej elektronickej pošty alebo telefonovania prostredníctvom internetu v určitom časovom pásme, používanú internetovú službu, telefónne číslo volajúceho pri prístupe prostredníctvom modemu (dial-up prístup) a digitálnu účastnícku prípojku alebo iný koncový bod pôvodcu komunikácie. Poskytovatelia elektronických komunikácií majú povinnosť uchovávať v podstate všetky údaje týkajúce sa komunikujúcich strán s výnimkou obsahu samotnej komunikácie.

106. Aj napriek tomu, že zákonom o elektronických komunikáciách ustanovená povinnosť uchovávať prevádzkové údaje, lokalizačné údaje a údaje komunikujúcich strán sa nevzťahuje na obsahy jednotlivých komunikácií, z uvedených údajov o užívateľoch,

adresátoch, presnom dátume, čase a trvaní komunikácie, type komunikácie, údajov vzťahujúcich sa na identifikáciu koncového zariadenia či údajov potrebných na identifikáciu polohy mobilného koncového zariadenia možno v ich vzájomnej kombinácii zostaviť pomerne podrobné informácie o spoločenskej alebo politickej príslušnosti, osobných záľubách, zdravotnom stave, sexualite, sklonoch či slabostiach jednotlivých osôb. Aj z údajov, ktoré majú poskytovatelia elektronických komunikácií povinnosť uchovávať, možno vyvodiť dostatočné obsahové závery spadajúce do súkromnej sféry jednotlivca. Z uvedených údajov možno až s 90 % pravdepodobnosťou napr. zistiť, s kým, ako často, v akých hodinách sa daný jednotlivec stretáva, kto sú jeho najbližší známi, priatelia či kolegovia z práce alebo akým aktivitám a v akých hodinách sa venuje [porovnaj štúdiu Massachusetts Institute of Technology (MIT), Relationship Inference, dostupnú na http://reality.media.mit.edu/dyads.php]. Zber a uchovávanie prevádzkových údajov, lokalizačných údajov a údajov komunikujúcich strán tak predstavuje významný zásah do práva na súkromie. Z týchto dôvodov je preto nevyhnutné pod rozsah ochrany základného práva na rešpektovanie súkromného života zahrnúť nielen ochranu samotného obsahu elektronickej komunikácie, ale rovnako tak aj prevádzkové a lokalizačné údaje a údaje komunikujúcich strán na ňu sa vzťahujúce.

107. Podľa judikatúry ESĽP (pozri najmä rozsudky ESĽP zo 16. 2. 2000, *Amann* v. Švajčiarsko, *Zbierka rozsudkov a rozhodnutí* 2000-II, § 65, ako aj zo 4. 5. 2000, Rotaru v. Rumunsko, Zbierka rozsudkov a rozhodnutí 2000 V, § 43) a judikatúry Súdneho dvora (rozsudok *Volker und Markus Schecke GbR a Hartmut Eifert proti Land Hessen*, C-92/09 a C-93/09, EU:C:2010:662, bod 52) dodržiavanie práva na ochranu osobného života v súvislosti so spracúvaním osobných údajov, tak ako vyplýva z čl. 8 dohovoru, resp. čl. 7 a 8 charty, sa vzťahuje na všetky informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby. Právna úprava ukladajúca povinnosť poskytovateľom elektronických komunikácii uchovávať prevádzkové údaje, lokalizačné údaje a údaje komunikujúcich strán sa odchyľuje od systému ochrany práva na rešpektovanie súkromného života zavedeného smernicami 95/46/ES a 2002/58/ES, ktorý požaduje dôvernosť komunikácie a prevádzkových údajov, ako aj povinnosť vymazať alebo anonymizovať tieto

údaje, ak už nie sú potrebné na prenos komunikácie, s výnimkou, že sú tieto údaje potrebné na účely fakturácie, a to aj v tomto prípade iba počas doby, keď táto potreba pretrváva. Z toho vyplýva, že povinnosť uložená poskytovateľom elektronických komunikácií počas určitého obdobia uchovávať údaje týkajúce sa súkromného života osoby a jej komunikácie predstavuje ako taká zásah do práva na súkromie. Značná intenzita zásahu do práva na súkromie je navyše daná skutočnosťou, že napadnutá právna úprava zavádza plošné a preventívne uchovávanie predmetných údajov komunikujúcich strán, čo ma za následok, že sa dotýka obrovského a nepredvídateľného počtu účastníkov komunikácie. Právna úprava umožňujúca príslušným vnútroštátnym orgánom prístup k týmto údajom predstavuje dodatočný zásah do tohto základného práva [pozri v tejto súvislosti rozsudky ESĽP *Leander v. Švédsko* z 26. 3. 1987, séria A 116, § 48; *Rotaru v. Rumunsko* (GC), 28341/95, § 46, ESĽP 2000 V, ako aj *Weber a Saravia v. Nemecko* (rozh.), 54934/00, § 79, ESĽP 2006 XI]. Značná intenzita zásahu do práva na súkromie je daná rovnako skutočnosťou, že uchovávané údaje a ich neskoršie použitie bez toho, aby účastník alebo registrovaný užívateľ boli o tom informovaní, môže v povedomí dotknutých osôb vyvolať pocit, že ich súkromný život je predmetom neustáleho sledovania (pozri rozsudok *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources a iní a Kärntner Landesregierung a iní*, C-293/12 a C-594/12, EU:C:2014:238, bod 37).

108. Napadnuté ustanovenia zákona o elektronických komunikáciách preto predstavujú zásah do práva na súkromie, a je ich potrebné posúdiť z hľadiska uvádzaných ústavnoprávnych požiadaviek kladených na právnu úpravu umožňujúcu zásah do tohto základného práva. Vzhľadom na vysokú intenzitu zásahu do práva na súkromie je nutné splnenie uvedených požiadaviek posudzovať podľa čo najprísnejších kritérií.

O odôvodnení zásahu do práva na súkromie

109. Podľa čl. 13 ods. 4 ústavy sa pri obmedzovaní základných práv a slobôd musí dbať na ich podstatu a zmysel, pričom takéto obmedzenia sa môžu použiť len na ustanovený

cieľ. Právo na súkromie a právo na ochranu osobných údajov nemajú charakter absolútneho práva, t. j. zákonodarca ich môže obmedziť, avšak len za podmienky, že ide o také obmedzenia, ktoré dbajú na jeho podstatu a zmysel a sú použité len na ustanovený legitímny cieľ.

110. Podľa čl. 52 ods. 1 charty akékoľvek obmedzenie výkonu práv a slobôd uznaných v tejto charte musí byť ustanovené zákonom a rešpektovať podstatu týchto práv a slobôd, pričom na základe zásady proporcionality sú takéto obmedzenia možné len vtedy, ak sú nevyhnutné a skutočne spĺňajú ciele všeobecného záujmu uznané Úniou, alebo potrebu chrániť práva a slobody iných.

111. Podľa čl. 8 ods. 2 dohovoru štátny orgán nemôže do výkonu práva na súkromie zasahovať s výnimkou prípadov, keď je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom alebo zločinnosti, ochrany zdravia alebo morálky alebo na ochranu práv a slobôd iných.

112. Skupina poslancov tvrdí, že napadnutou právnou úpravou dochádza k neprípustnému zásahu do samotnej podstaty základného práva na rešpektovanie súkromného života a práva na ochranu osobných údajov, keďže *„podľa posledných výskumov Inštitútu Maxa Plancka totiž zbieranie týchto údajov nemá žiadny pozitívny vplyv na odhaľovanie závažných trestných činov v Európe“*.

113. V súvislosti s namietaným zásahom do samotnej podstaty základného práva na rešpektovanie súkromného života je potrebné konštatovať, že hoci uchovávanie údajov predstavuje zvlášť závažný zásah do tohto práva, nie je spôsobilé zasiahnuť do samotnej podstaty tohto práva, pretože napadnutá právna úprava neumožňuje oboznámiť sa so samotným obsahom elektronickej komunikácie (pozri rozsudok *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources a iní a Kärntner Landesregierung a iní*, C-293/12 a C-594/12, EU:C:2014:238, bod 39). Uchovávanie

prevádzkových údajov, lokalizačných údajov a údajov komunikujúcich strán tiež nemôže zasahovať do podstaty základného práva na ochranu osobných údajov ako zložky práva na súkromie, pretože zákon o elektronických komunikáciách v § 58 ods. 10 zavádza pre poskytovateľov elektronických komunikácií pri uchovávaní údajov povinnosť dodržať určité zásady ochrany a bezpečnosti údajov, podľa ktorých majú zabezpečiť, aby a) uchovávané údaje mali rovnakú kvalitu a podliehali rovnakému zabezpečeniu a ochrane ako údaje podnikom spracúvané alebo uchovávané pri poskytovaní sietí alebo služieb, b) údaje podliehali príslušným technickým opatreniam a organizačným opatreniam na ochranu údajov proti náhodnému alebo protiprávnemu zničeniu, náhodnej strate alebo zmene, neoprávnenému alebo protiprávnemu uchovaniu, spracovaniu, prístupu alebo zverejneniu, c) údaje podliehali príslušným technickým opatreniam a organizačným opatreniam, ktoré zabezpečia, aby údaje mohli byť sprístupnené len oprávneným osobám konajúcim na základe poverenia alebo splnomocnenia podniku a orgánom činným v trestnom konaní, súdu alebo iným orgánom štátu a ich povereným alebo inak oprávneným príslušníkom alebo zamestnancom, d) údaje na konci obdobia určeného na ich uchovávanie boli zlikvidované okrem údajov, ktoré boli poskytnuté a zabezpečené.

114. Pokiaľ ide o otázku, či uvedený zásah zodpovedá cieľu všeobecného záujmu, treba uviesť, že cieľom napadnutých ustanovení zákona o elektronických komunikáciách ustanovujúcich poskytovateľom elektronických komunikácií povinnosť uchovávať prevádzkové údaje, lokalizačné údaje a údaje komunikujúcich strán a povinnosť poskytnúť ich orgánom činným v trestnom konaní, súdu a inému orgánu štátu podľa § 55 ods. 6 zákona o elektronických komunikáciách je, ako to vyplýva z § 58 ods. 7 zákona o elektronických komunikáciách, zabezpečiť dostupnosť týchto údajov na účely vyšetrovania, odhaľovania a stíhania trestných činov súvisiacich s terorizmom, nedovoleným obchodovaním, organizovanou trestnou činnosťou, únikom a ohrozením utajovaných skutočností a s trestnými činmi spáchanými nebezpečným zoskupením. Cieľom napadnutých ustanovení zákona o elektronických komunikáciách je teda podporiť boj proti závažnej trestnej činnosti a v konečnom dôsledku tak chrániť verejnú bezpečnosť.

115. Predchádzanie zločinnosti a verejná bezpečnosť predstavujú podľa čl. 8 ods. 2 dohovoru legitímne ciele, v záujme dosiahnutia ktorých je prípustné zasiahnuť do výkonu práva na súkromie. Podľa judikatúry Súdneho dvora boj proti medzinárodnému terorizmu s cieľom zachovať mier a medzinárodnú bezpečnosť predstavuje cieľ všeobecného záujmu Únie (pozri v tomto zmysle rozsudky *Kadi a Al Barakaat International Foundation/Rada a Komisia*, C 402/05 P a C 415/05 P, EU:C:2008:461, bod 363, ako aj *Al Aqsa/Rada*, C 539/10 P a C 550/10 P, EU:C:2012:711, bod 130). To isté platí, pokiaľ ide o boj proti závažnej trestnej činnosti na účely zabezpečenia verejnej bezpečnosti (pozri v tomto zmysle rozsudok *Tsakouridis*, C 145/09, EU:C:2010:708, body 46 a 47). Vychádzajúc z uvedeného je potrebné konštatovať, že napadnutá právna úprava požadujúca uchovávanie údajov na účely ich prípadného sprístupnenia príslušným štátnym orgánom sleduje legitímny cieľ všeobecného záujmu.

116. Za týchto podmienok je potrebné preskúmať primeranosť (proporcionalitu) konštatovaného zásahu. Je potrebné preskúmať, či napadnuté ustanovenia zákona o elektronických komunikáciách sú jednak vhodné na dosiahnutie legitímnych cieľov a jednak nevyhnutné na ich dosiahnutie, t. j. či neprekračujú hranice toho, čo je primerané a potrebné na uskutočnenie týchto cieľov. Vzhľadom na dôležitosť ochrany osobných údajov so zreteľom na základné právo na rešpektovanie súkromného života je potrebné pristúpiť k prísnej kontrole dodržania kritérií proporcionality konštatovaného zásahu.

117. Pokiaľ ide o posúdenie otázky, či uchovávanie prevádzkových údajov, lokalizačných údajov a údajov komunikujúcich strán na účely ich prípadného sprístupnenia príslušným orgánom je vhodné na dosiahnutie sledovaného cieľa, je potrebné konštatovať, že vzhľadom na značný nárast možností elektronickej komunikácie ponúkajú údaje, ktoré sa majú uchovávať podľa § 58 ods. 5 zákona o elektronických komunikáciách a prílohy č. 2 tohto zákona konkretizujúcej kategórie uchovávaných údajov príslušným vnútroštátnym orgánom podľa § 58 ods. 7 v spojitosti s § 55 ods. 6 tohto zákona dodatočné možnosti na objasnenie závažných trestných činov taxatívne vymedzených v § 58 ods. 7 tohto zákona a v tomto ohľade predstavujú užitočný nástroj pre účely vyšetrovania, odhaľovania a stíhania

predmetných trestných činov (pozri rozsudok *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources a iní a Kärntner Landesregierung a iní*, C-293/12 a C-594/12, EU:C:2014:238, bod 49). Uchovávanie týchto údajov teda možno považovať za prostriedok, ktorý je vhodný a spôsobilý na dosiahnutie sledovaných cieľov.

118. Toto konštatovanie nemožno spochybniť skutočnosťou, na ktorú vo svojom návrhu poukazuje skupina poslancov, že existuje viacero spôsobov, ako sa vyhnúť uchovávaniu dát, napríklad zvolením iného spôsobu komunikácie, ktorý nie je štátom zatiaľ monitorovaný, napríklad použitím blogu, sociálnych sietí (napr. facebook), webov umožňujúcich zdieľanie videí (napr. youtube), rýchlych správ (IM), IRC (Internet relay chat), peer-to-peer (P2P) komunikácie, keďže tieto nepoužívajú protokoly predpokladané zákonom o elektronických komunikáciách, resp. šifrujú komunikáciu, či použitím telefónnej búdky alebo tzv. anonymných predplatených telefónnych kariet (kariet, pri kúpe ktorých nie je nevyhnutné preukazovať svoju totožnosť), alebo použitím komerčných služieb na anonymizáciu komunikácie alebo systému The Onion Rouler (TOR) či systému JAP (JonDo), v dôsledku čoho by napadnutá právna úprava nemala byť vhodná na dosiahnutie sledovaného cieľa, a to boj proti organizovanému zločinu a terorizmu, pretože práve osoby páchajúce takúto trestnú činnosť najlepšie poznajú spôsoby, ako sa uchovávaniu údajov efektívne vyhnúť. Hoci je pravda, že táto okolnosť môže obmedziť účinnosť (efektivitu) uchovávania údajov pri dosahovaní sledovaného cieľa, nemôže viesť k nespôsobilosti tohto opatrenia dosiahnuť sledovaný cieľ.

119. Pokiaľ ide o nevyhnutnosť uchovávania vybraných údajov pre dosiahnutie verejnej bezpečnosti, je potrebné konštatovať, že hoci účinnosť boja proti závažnej trestnej činnosti môže vo veľkej miere závisieť od použitia moderných vyšetrovacích technológií, ani tento cieľ všeobecného záujmu, nech je akokoľvek zásadný, nemôže sám osebe odôvodniť to, aby sa opatrenie uchovávania zavedené napadnutými ustanoveniami zákona o elektronických komunikáciách považovalo za nevyhnutné na účely uvedeného boja (pozri rozsudok *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources a iní a Kärntner Landesregierung a iní*, C-293/12 a C-594/12,

EU:C:2014:238, bod 51). Ochrana práva na súkromie vyžaduje, aby výnimky a obmedzenia v súvislosti s ochranou osobných údajov nepôsobili nad rámec toho, čo je prísne nevyhnutné (rozsudok *IPI*, C 473/12, EU:C:2013:715, bod 39).

120. V súvislosti s otázkou, či zásah, ktorý predstavuje napadnutá úprava zákona o elektronických komunikáciách, je obmedzený na to najnevyhnutnejšie, treba uviesť, že táto úprava podľa svojho § 58 ods. 5 v spojení s prílohou č. 2 zákona o elektronických komunikáciách konkretizujúcou kategórie uchovávaných údajov ukladá povinnosť uchovávať všetky prevádzkové údaje, lokalizačné údaje a údaje komunikujúcich strán týkajúce sa telefónneho spojenia prostredníctvom pevnej siete a mobilného telefónneho spojenia, pripojenia k internetu, internetovej elektronickej pošty, ako aj telefonovania prostredníctvom internetu. Vzťahuje sa tak na všetky prostriedky elektronickej komunikácie, ktorých používanie je veľmi rozšírené a ktoré majú rastúci význam pre každodenný život jednotlivca. Uvedená úprava sa pritom vzťahuje na všetkých účastníkov a registrovaných užívateľov. Uchovávanie prevádzkových údajov, lokalizačných údajov a údajov komunikujúcich strán sa všeobecným spôsobom týka všetkých osôb používajúcich elektronické komunikačné služby bez toho, aby sa tieto osoby, ktorých údaje sa uchovávajú, aspoň nepriamo nachádzali v situácii, ktorá by mohla viesť k trestnému stíhaniu. Uplatňuje sa teda aj na osoby, pri ktorých nie je dôvod domnievať sa, že by ich konanie mohlo mať aspoň nepriamu alebo vzdialenú súvislosť so závažnými trestnými činmi. Navyše, neustanovuje žiadnu výnimku, takže sa uplatňuje aj na osoby, ktorých komunikácia podľa príslušnej právnej úpravy podlieha služobnému tajomstvu alebo právom ustanovenej či uznanej povinnosti mlčanlivosti.

121. Napadnuté ustanovenia zákona o elektronických komunikáciách smerujúce k podpore boja proti závažnej trestnej činnosti nevyžadujú žiadnu súvislosť medzi údajmi, ktorých uchovávanie ustanovujú, a hrozbou pre verejnú bezpečnosť. Uchovávanie sa neobmedzuje ani na údaje z určitého časového obdobia a/alebo z určitej zemepisnej oblasti či na okruh osôb, ktoré by akýmkoľvek spôsobom bolo možné spájať so závažnými

trestnými činmi, ani na osoby, ktorých uchovávané údaje by z iných dôvodov mohli prispieť k predchádzaniu, odhaľovaniu alebo stíhaniu závažných trestných činov.

122. Vzhľadom na uvedené napadnutá právna úprava zákona o elektronických komunikáciách predstavuje závažný zásah do práva na súkromie, pričom ju nemožno považovať za úpravu nevyhnutnú pre dosiahnutie sledovaného cieľa. Cieľ sledovaný napadnutou právnou úpravou podporiť boj proti závažnej trestnej činnosti a v konečnom dôsledku verejnú bezpečnosť možno dosiahnuť aj inými prostriedkami, ktoré predstavujú menej intenzívny zásah do práva na súkromie, ako je nástroj v podobe plošného a preventívneho uchovávania predmetných údajov. Za primeranejší nástroj dosiahnutia sledovaných cieľov možno považovať napríklad tzv. *data freezing*, ktorý po splnení stanovených podmienok umožňuje sledovať a uchovávať potrebné a vybrané údaje iba u konkrétneho, vopred určeného účastníka komunikácie. Taktiež je potrebné dodať, že napadnutá právna úprava zákona o elektronických komunikáciách by predstavovala o niečo primeranejší nástroj dosiahnutia sledovaných cieľov, ak by poskytovala dostatočné záruky a prostriedky ochrany dotknutých jednotlivcov umožňujúce účinne chrániť osobné údaje proti rizikám ich úniku, zneužitia či proti akémukoľvek nezákonnému prístupu a akémukoľvek nezákonnému použitiu týchto údajov.

123. V súvislosti s pravidlami týkajúcimi sa bezpečnosti a ochrany údajov uchovávaných poskytovateľmi elektronických komunikácií treba (aj napriek skutočnosti reflektovanej ústavným súdom v bode 113) konštatovať, že napadnutá právna úprava zákona o elektronických komunikáciách neustanovuje dostatočné záruky, ako to požaduje čl. 19 ods. 3 a čl. 22 ods. 2 ústavy, čl. 8 dohovoru a čl. 8 charty, ktoré by umožňovali zabezpečenie účinnej ochrany uchovávaných údajov pred rizikom zneužitia, ako aj pred akýmkoľvek nezákonným prístupom a každým nezákonným použitím týchto údajov. Napadnutá právna úprava napríklad neustanovuje špecifické pravidlá prispôsobené veľkému množstvu údajov, ktorých uchovávanie ukladá, citlivej povahe týchto údajov, ako aj riziku nezákonného prístupu k nim, pričom tieto pravidlá by jasným a reštriktívnym spôsobom

upravovali ochranu a bezpečnosť predmetných údajov, aby sa zaručila ich úplná integrita a dôvernosť.

124. Ustanovenie § 58 ods. 10 zákona o elektronických komunikáciách nezaručuje, že poskytovatelia elektronických komunikácií uplatnia mimoriadne vysokú úroveň ochrany a bezpečnosti pomocou technologických a organizačných opatrení, pretože § 56 ods. 2 daného zákona umožňuje prevádzkovateľom elektronických komunikácií pri stanovení úrovne bezpečnosti, ktorú uplatňujú, zohľadniť ekonomické úvahy, pokiaľ ide o náklady na vykonanie bezpečnostných opatrení. Ustanovenie § 56 ods. 2 zákona o elektronických komunikáciách požaduje zo strany prevádzkovateľov elektronických komunikácií prijať opatrenia, ktoré musia zabezpečiť takú úroveň bezpečnosti služieb, ktorá je primeraná existujúcemu riziku s ohľadom na stav techniky a náklady na ich realizáciu.

125. Vzhľadom na všetky predchádzajúce konštatovania je potrebné konštatovať, že zákonodarca pri prijatí napadnutých ustanovení zákona o elektronických komunikáciách prekročil hranice, ktoré mu ukladá dodržiavanie zásady proporcionality.

126. Keďže napadnuté ustanovenia zákona o elektronických komunikáciách nie sú v súlade so základným právom na súkromie, nie je potrebné pristúpiť k ich preskúmaniu aj s ohľadom na čl. 25 ústavy a čl. 10 dohovoru, ktoré zaručujú právo na slobodu prejavu.

IV.2 K namietanému nesúladu napadnutých ustanovení Trestného poriadku a zákona o Policajnom zbore s právom na ochranu súkromia

127. Napadnuté ustanovenia Trestného poriadku zakladajú orgánom činným v trestnom konaní oprávnenie, aby na účely objasnenia skutočností dôležitých pre trestné konanie získali od poskytovateľov elektronických komunikácií údaje o uskutočnenej telekomunikačnej prevádzke, ktoré sú inak predmetom telekomunikačného tajomstva alebo na ktoré sa vzťahuje ochrana osobných údajov. Napadnuté ustanovenia zákona o Policajnom zbore zakladajú pre Policajný zbor pre účely odhaľovania a dokumentovania trestnej

činnosti oprávnenie v rozsahu potrebnom na plnenie konkrétnej úlohy Policajného zboru a na čas nevyhnutný na splnenie tejto úlohy požadovať od poskytovateľov elektronických komunikácií údaje o uskutočnenej komunikačnej prevádzke podľa zákona o elektronických komunikáciách spôsobom, ktorý umožňuje diaľkový, nepretržitý a priamy prístup.

128. Prístup orgánov verejnej moci k týmto údajom bez súhlasu užívateľov týchto služieb sa vzhľadom na možnosť odvodiť z týchto údajov informácie o mieste, čase, a účastníkoch komunikácie, ako aj o spôsobe ich komunikácie bezprostredne a citeľne dotýka ich práva na súkromie v podobe práva na informačné sebaurčenie, pretože ich v tomto rozsahu zbavuje možnosti, aby sami rozhodli, či tieto informácie sprístupnia iným osobám. Podľa judikatúry Súdneho dvora (rozsudok *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources a iní a Kärntner Landesregierung a iní*, C-293/12 a C-594/12, EU:C:2014:238, bod 35) a judikatúry ESĽP [rozsudky ESĽP vo veci *Leander v. Švédsko* z 26. marca 1987, séria A 116, bod 48; *Rotaru v. Rumunsko* [GC], č. 28341/95, bod 46, ESĽP 2000 V, ako aj *Weber a Saravia v. Nemecko* (rozh.), č. 54934/00, bod 79, ESĽP 2006 XI] prístup príslušných vnútroštátnych orgánov k údajom týkajúcim sa súkromného života osôb a ich komunikácie predstavuje zásah do základného práva na rešpektovanie súkromného života.

129. Pre prípustnosť takéhoto zásahu sa vyžaduje splnenie podmienok vyplývajúcich z ústavného poriadku. Ide predovšetkým o to, aby predmetné obmedzenie bolo stanovené na základe zákona a aby jeho právna úprava spĺňala požiadavku určitosti vyplývajúcu zo zásady právneho štátu, teda aby bola presná a jasná vo svojej formulácii a súčasne predvídateľná v zmysle, aby potencionálne dotknutým jednotlivcom poskytovala dostatočnú informáciu o podmienkach, za ktorých môže dôjsť k obmedzeniu ich základného práva (pozri rozhodnutie ESĽP z 27. decembra 2005 vo veci *Sallinen v. Fínsko*; obdobne III. ÚS 172/2010). Zároveň musí obmedzenie práva na súkromie v podobe práva na informačné sebaurčenie sledovať ústavne aprobovaný účel, ktorým je ochrana iného základného práva alebo verejného statku, pričom pri posúdení vzájomnej kolízie týchto hodnôt je potrebné dodržať imperatív minimalizácie zásahu do základných práv a slobôd, berúc pritom ohľad na

ich podstatu a zmysel. Zásah do základného práva tak musí obstáť z hľadiska proporcionality, ktorej posúdenie pozostáva podľa ustálenej judikatúry ústavného súdu z troch krokov. Prvý krok pozostáva z posúdenia spôsobilosti (alebo vhodnosti) konkrétneho opatrenia dosiahnuť sledovaný cieľ, čím sa rozumie, či posudzované opatrenie je vôbec schopné dosiahnuť sledovaný legitímny cieľ, ktorým je ochrana iného základného práva alebo verejného statku. Druhým krokom je posúdenie potrebnosti (nevyhnutnosti) z hľadiska, či pri výbere prostriedku bol použitý ten z nich, ktorý je k základnému právu najšetrnejší. V poslednom treťom kroku je predmetom posúdenia proporcionalita v užšom zmysle, teda či ujma na základnom práve nie je neprimeraná vo vzťahu k sledovanému cieľu, t. j. že opatrenie obmedzujúce základné právo alebo slobodu nesmie svojimi negatívnymi dôsledkami prevyšovať pozitíva, ktoré predstavuje verejný záujem na uplatňovaní týchto opatrení z dôvodu dosiahnutia sledovaných cieľov.

130. Z hľadiska uvedených kritérií je potrebné konštatovať, že opatrenie spočívajúce v oprávnení orgánov činných v trestnom konaní požadovať od poskytovateľov elektronických komunikácií údaje o uskutočnenej telekomunikačnej prevádzke, ktoré sú inak predmetom telekomunikačného tajomstva alebo na ktoré sa vzťahuje ochrana osobných údajov, má zákonný základ v napadnutých ustanoveniach Trestného poriadku a zákona o Policajnom zbore. Zákonný základ prípustného zásahu do práva na súkromie však musí spĺňať podmienku istého stupňa materiálnej kvality. Z doktríny ESĽP, ktorú si ústavný súd osvojil, vyplýva, že aj zásah, ktorý má svoj právny základ v zákonnej norme, môže v konkrétnom prípade znamenať zásah do práv garantovaných ústavou, resp. dohovorom. (I. ÚS 117/07). Oprávnené zásahy do práva na súkromie možno uskutočniť zákonom len v súlade so všeobecnými princípmi, za ktorých možno obmedziť ústavné právo alebo slobodu jednotlivca (PL. ÚS 43/95).

131. Účelom oprávnenia orgánov činných v trestnom konaní požadovať od poskytovateľov elektronických komunikácií zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke, ktoré sú inak predmetom telekomunikačného tajomstva alebo na ktoré sa vzťahuje ochrana osobných údajov, je najmä nutnosť zistenia či preverenia

skutočností dôležitých pre trestné konanie v trestnom konaní pre úmyselný trestný čin. Je potrebné konštatovať, že takéto opatrenie sleduje ústavne aprobovaný verejný záujem, ktorým je boj proti trestnej činnosti, čo má význam pre zabezpečenie verejnej bezpečnosti. Takýto účel odôvodňuje zásah do základného práva. Predmetný verejný záujem obstojí aj ako legitímny cieľ odôvodňujúci zásah do základného práva podľa čl. 8 ods. 2 dohovoru. Článok 8 ods. 2 dohovoru umožňuje, ak to je v demokratickej spoločnosti nevyhnutné, zasiahnuť do práva na rešpektovanie súkromného života v záujme ochrany práv a slobôd iných, národnej a verejnej bezpečnosti, hospodárskeho blahobytu štátu, predchádzania nepokojom a zločinnosti či ochrany zdravia a morálky. Účel, ktorý sledujú napadnuté ustanovenia Trestného poriadku a zákona o Policajnom zbore, obstojí aj ako účel aprobovaný právom Európskej únie. Podľa čl. 15 smernice 2002/58/ES členské štáty môžu prijať legislatívne opatrenia, ktoré obmedzujú základné práva a slobody a najmä právo na súkromie a dôvernosť z hľadiska spracúvania osobných údajov v elektronickom komunikačnom sektore, ak také obmedzenie predstavuje nevyhnutné, vhodné a primerané opatrenie v demokratickej spoločnosti na zabezpečenie národnej bezpečnosti (t. j. bezpečnosti štátu), obrany, verejnej bezpečnosti a na zabránenie, vyšetrovanie, odhaľovanie a stíhanie trestných činov alebo neoprávneného používania elektronického komunikačného systému podľa čl. 13 ods. 1 smernice 95/46/ES. Na tento účel podľa toho istého ustanovenia smernice 2002/58/ES členské štáty môžu okrem iného prijať legislatívne opatrenia umožňujúce zadržanie údajov na limitované obdobie za splnenia ďalších podmienok.

132. Rovnako je možné konštatovať, že opatrenie spočívajúce v oprávnení orgánov činných v trestnom konaní požadovať od poskytovateľov elektronických komunikácií zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke je spôsobilé dosiahnuť sledovaný cieľ. Obstojí teda aj v prvom kroku testu proporcionality. Ústavný súd preto pristúpil k posúdeniu splnenia potrebnosti, resp. nevyhnutnosti predmetného opatrenia.

133. V úvode posúdenia potrebnosti, resp. nevyhnutnosti predmetného opatrenia je potrebné uviesť, že napadnuté ustanovenia Trestného poriadku a zákona o Policajnom zbore

vymedzujú nielen to, čo je predmetom platnej právnej úpravy oprávnenia orgánov činných v trestnom konaní, a to požadovať od poskytovateľov elektronických komunikácii zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke, ale aj to, čo predmetom takejto právnej úpravy nie je. Predmetné opatrenie predstavuje negatívny zásah do práva na rešpektovanie súkromného života v podobe práva na informačné sebaurčenie užívateľov elektronických komunikácií nielen kvôli samotnému oznámeniu údajov o uskutočnenej elektronickej komunikácii orgánom činným v trestnom konaní, ale rovnako aj kvôli ďalšej dispozícii s nimi, napríklad ich sprístupnením ďalším osobám alebo zneužitím na iné účely. Je preto potrebné preskúmať, či napadnuté ustanovenia Trestného poriadku a zákona o Policajnom zbore poskytujú z hľadiska základného práva na rešpektovanie súkromného života v podobe práva na informačné sebaurčenie, resp. práva na ochranu osobných údajov, dostatočné garancie proti zneužitiu predmetných údajov počas celého trvania trestného konania. Týmito garanciami je potrebné rozumieť stanovenie podmienok, za ktorých majú mať príslušné orgány prístup k údajom o uskutočnenej elektronickej prevádzke, ako aj účinnej kontroly ich dodržiavania (nález Ústavného súdu Českej republiky sp. zn. Pl. ÚS 42/11, bod 23). K obmedzeniu osobnej integrity a súkromia osôb zo strany verejnej moci môže dôjsť iba veľmi výnimočne, ak je to akceptované z pohľadu zákonnej existencie a dodržania účinných a konkrétnych záruk proti ľubovôli (porovnaj nález Ústavného súdu Českej republiky sp. zn. Pl. ÚS 24/10, bod 36; rovnako tiež nález Ústavného súdu Českej republiky sp. zn. I. ÚS 631/05, bod 26). Nevyhnutnosť, aby prijaté opatrenia zasahujúce do práva na súkromie obsahovali takéto záruky, sa pre jednotlivcov stáva naliehavejšou práve v dnešnej dobe, kedy vďaka enormnému rozvoju a výskytu nových informačných technológií a elektronickej komunikácie (v tzv. kyberpriestore) je predovšetkým vďaka rozvoju internetu a mobilnej komunikácie každú minútu zaznamenávané, zhromažďované a fakticky sprístupňované enormné množstvo dát, údajov a informácií, ktoré zasahujú aj do súkromnej sféry každého jednotlivca, a to aj napriek tomu, že on sám do nej vedome nikoho pustiť nechcel (porovnaj nález Ústavného súdu Českej republiky sp. zn. Pl. ÚS 24/11, bod 50).

134. Zo znenia napadnutých ustanovení Trestného poriadku vyplýva, že oprávnenie orgánov činných v trestnom konaní požadovať od poskytovateľov elektronických komunikácii zistenie a oznámenie údajov o uskutočnenej elektronickej komunikácii je podmienené iba tým, že takéto opatrenie musí smerovať k objasneniu skutočností dôležitých pre trestné konanie v trestnom konaní pre úmyselný trestný čin. Zo znenia napadnutých ustanovení zákona o Policajnom zbore vyplýva, že oprávnenie Policajného zboru požadovať od poskytovateľov elektronických komunikácií zistenie a oznámenie údajov o uskutočnenej elektronickej komunikácii spôsobom umožňujúcim diaľkový, nepretržitý a priamy prístup je podmienené iba tým, že takéto opatrenie musí smerovať k odhaleniu a dokumentovaniu trestnej činnosti a môže byť uskutočnené len v rozsahu potrebnom na plnenie konkrétnej úlohy Policajného zboru a na čas nevyhnutný na splnenie tejto úlohy. Oprávnenie orgánov činných v trestnom konaní požadovať zistenie a oznámenie údajov o elektronickej komunikácii sa teda netýka len určitej kategórie úmyselných trestných činov, a to tak, ako to ustanovuje § 58 ods. 7 zákona o elektronických komunikáciách, t. j. trestných činov súvisiacich s terorizmom, nedovoleným obchodovaním, organizovanou trestnou činnosťou, únikom a ohrozením utajovaných skutočností a trestných činov spáchaných nebezpečným zoskupením, ale akýchkoľvek úmyselných trestných činov (v prípade napadnutého ustanovenia Trestného poriadku), resp. trestných činov (v prípade napadnutého ustanovenia zákona o Policajnom zbore). Podľa ústavného súdu takto vymedzený okruh trestných činov, pre účely vyšetrovania, odhaľovania a stíhania ktorých možno zasiahnuť do základného práva na informačné sebaurčenie, upravuje medze tohto základného práva veľmi široko a neurčito. Umožňuje požiadať a použiť predmetné údaje zo strany orgánov činných v trestnom konaní stále, ak je možné nájsť určitú súvislosť s prebiehajúcim konaním o úmyselnom trestnom čine, resp. trestnom čine. Miera intenzity zásahu do práva na súkromie spôsobená uchovávaním a následným sprístupnením údajov o uskutočnenej elektronickej komunikácii orgánom činným v trestnom konaní však požaduje, aby oprávnenie orgánov činných v trestnom konaní požadovať zistenie a oznámenie údajov potrebných na objasnenie skutočností dôležitých pre trestné konanie sa vzťahovalo len na najzávažnejšie trestné činy. Je síce pravda, že príkaz na zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke vydáva podľa § 116 ods. 2 Trestného poriadku

predseda senátu, pred začatím trestného stíhania alebo v prípravnom konaní sudca pre prípravné konanie na návrh prokurátora, a teda ochrana základných práv a slobôd podlieha v prípade sprístupnenia údajov o elektronickej komunikácii orgánom činným v trestnom konaní kontrole zo strany nezávislého a nestranného súdu, ktorý by mal v každom jednotlivom prípade posúdiť, či zistenie predmetných údajov nie je vzhľadom na závažnosť trestného činu, možnosť dosiahnuť účel trestného konania inak alebo z iného dôvodu neprimeraným zásahom do práva na súkromie, napríklad tým, ako na to poukázala aj skupina poslancov vo svojom návrhu, že by predmetné ustanovenie § 116 ods. 1 Trestného poriadku vykladal v spojitosti s § 58 ods. 7 zákona o elektronických komunikáciách, a teda za úmyselné trestné činy, vo vzťahu ku ktorým by bolo možné požadovať oznámenie predmetných údajov, by príslušný súd považoval len trestné činy taxatívne vymenované v § 58 ods. 7 zákona o elektronických komunikáciách. Takáto garancia umožňujúca poskytnúť ochranu pred neprimeraným zásahom do práva na súkromie s ohľadom na skutkové okolnosti konkrétneho prípadu nemôže preklenúť nedostatok spočívajúci v neurčitosti a prílišnej všeobecnosti napadnutej právnej úpravy tým, že požaduje od konajúceho súdu, aby nahradil úvahu zákonodarcu o intenzite určitého verejného záujmu na obmedzení základného práva alebo slobody v prípade jednotlivých trestných činov. Takýto postup súdov by nezodpovedal ani čl. 13 ods. 2 ústavy, ktorý požaduje upraviť medze základných práv a slobôd, resp. obmedzenie výkonu práva a slobôd, jedine zákonom. Len zákonodarca je ústavne legitimovaný na to, aby na základe svojho uváženia pri rešpektovaní princípu proporcionality priznal stanoveniu určitej povinnosti prednosť aprobovaného verejného záujmu pred základným právom. Ponechanie určenia ústavne súladného obmedzenia základných práv a slobôd iba na rozhodovaciu prax súdov by nebolo zlučiteľné ani s požiadavkou právnej istoty, lebo prípadný zásah do práva na súkromie nie je z dôvodu neurčitosti súčasnej právnej úpravy pre jednotlivca predvídateľný v takej miere, ktorá by zodpovedala závažnosti prípadných negatívnych dôsledkov pre právo na súkromie. Ak zákonodarca ustanovil ako podmienku pre zistenie údajov o uskutočnenej komunikačnej prevádzke, že musí viesť k objasneniu skutočností dôležitých pre trestné konanie pre úmyselný trestný čin (resp. trestný čin), vytvoril tým základ pre obmedzenie práva na súkromie v podobe práva na informačné sebaurčenie v takej miere, ktorá opomína

požiadavku nevyhnutnosti takéhoto zásahu s ohľadom na ním sledovaný cieľ (porovnaj nález sp. zn. Pl. ÚS. 42/11, body 24, 25; nález sp. zn. II. ÚS 789/06, bod 16). Oprávnenie orgánov činných v trestnom konaní požadovať zistenie a oznámenie údajov o uskutočnenej komunikačnej prevádzke nemôže byť vzhľadom na intenzitu, ktorou zasahuje do tohto základného práva, považované za obvyklý alebo rutinný prostriedok prevencie a odhaľovania trestnej činnosti. K použitiu tohto prostriedku boja proti trestnej činnosti môže dôjsť jedine vtedy, ak na dosiahnutie tohto cieľa neexistuje iný a vo vzťahu k základnému právu šetrnejší prostriedok.

135. O riziku užívania oprávnenia orgánov činných v trestnom konaní požadovať zistenie a oznámenie údajov o uskutočnenej komunikačnej prevádzke od prevádzkovateľov elektronických komunikácií ako bežného alebo rutinného prostriedku na vyšetrovanie aj menej závažnej trestnej činnosti, ako je trestná činnosť vymedzená v § 58 ods. 7 zákona o elektronických komunikáciách, svedčia aj relevantné štatistické údaje. Podľa ročnej štatistiky žiadostí o sprístupnenie uchovávaných údajov, tak ako to uvádza skupina poslancov v podanom návrhu, predstavoval počet vyžiadaní si údajov o uskutočnenej telekomunikačnej prevádzke v roku 2009 číslo 5214 a v roku 2010 číslo 7417 (porovnaj so správou Komisie Rade a Európskemu parlamentu z 18. apríla 2011 s názvom „Hodnotiaca správa o smernici o uchovávaní údajov“, prístupnej na eur-lex.europa.eu, CELEX: 52011DC0225, predmetné oficiálne údaje si Komisia vyžiadala od Slovenskej republiky).

136. V záujme rešpektovania požiadavky potrebnosti, resp. nevyhnutnosti, napadnutá právna úprava by mala obsahovať aj úpravu nakladania s týmito údajmi zo strany orgánov činných v trestnom konaní. Jej súčasťou by mali byť jasné a detailné pravidlá obsahujúce minimálne požiadavky na zabezpečenie uchovávaných údajov, ktoré by zaručovali, že nedôjde k využitiu uchovávaných údajov na iné ako zákonom ustanovené legitímne ciele. Ide predovšetkým o zamedzenie prístupu tretích osôb a stanovenie procedúry vedúcej k ochrane celistvosti a dôvernosti uchovávaných údajov, ako aj ich zničenia (nález sp. zn. Pl. ÚS 24/10, bod 50). Účinná ochrana pred neprípustným zásahom do práva na

súkromie dotknutých osôb by mala byť zaručená prostredníctvom povinnosti dodatočne informovať osobu užívateľa služieb elektronickej komunikácie o tom, že prevádzkové a lokalizačné údaje a údaje komunikujúcich strán, ktoré sa jej týkajú, boli oznámené orgánom činným v trestnom konaní. Zároveň by dotknuté osoby mali mať k dispozícii právny prostriedok, na základe ktorého by sa bolo možné domáhať súdneho prieskumu postupu orgánov činných v trestnom konaní pri získavaní a nakladaní s predmetnými údajmi. Výnimku z tejto povinnosti by pritom bolo možné pripustiť len zo zákonom ustanovených dôvodov, u ktorých by prevážil záujem na zachovaní utajenia tejto informácie. Aj v týchto prípadoch však musí zákonodarca garantovať, že posúdenie príslušných orgánov, či sú dané dôvody na utajenie tejto informácie, nebolo svojvoľné, ale podliehalo povinne súdnej kontrole (porovnaj nález sp. zn. Pl. ÚS 42/11, bod 27; rozhodnutie Spolkového ústavného súdu Nemecka sp. zn. 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, body 281 až 282). Napokon je potrebné uviesť, že nie je daný žiaden dôvod, pre ktorý by sa rozsah zákonom ustanovených garancií vo vzťahu k nariadeniu oznámiť údaje o uskutočnenej telekomunikačnej prevádzke mal z hľadiska svojho obsahu odlišovať, pokiaľ takéto odlíšenie nevyplýva z povahy veci, od garancií ustanovených vo vzťahu k nariadeniu odpočúvania a záznamu telekomunikačnej prevádzky, pretože v oboch prípadoch je intenzita zásahu do práva na súkromie porovnateľná. Na rozdiel od zákonnej úpravy nariadenia odpočúvania a záznamu telekomunikačnej prevádzky podľa § 115 Trestného poriadku, ktorá obsahuje garancie ochrany pred neprípustným zásahom do práva na súkromie, zákonnej úprave nariadenia zistenia a oznámenia údajov o uskutočnenej telekomunikačnej prevádzke podľa napadnutých ustanovení Trestného poriadku a zákona o Policajnom zbore uvedené garancie chýbajú, resp. neobsahuje garancie porovnateľné s tými, ktoré sú obsiahnuté v § 115 Trestného poriadku.

137. Zákonodarca by mal napokon rovnako zvážiť aj účelnosť ustanovenia podrobnejších pravidiel pre obsah príkazu na zistenie a oznámenie údajov o uskutočnenej komunikačnej prevádzke, prípadne ustanoviť určité formálne náležitosti samotnej žiadosti zo strany orgánov činných v trestnom konaní o takéto opatrenie. Zmyslom vymedzenia nevyhnutných obsahových náležitostí priamo na úrovni zákona je zabezpečiť, aby súd pri

svojom rozhodovaní disponoval všetkými potrebnými informáciami, ktoré sú pre orgány činné v trestnom konaní bez väčších ťažkostí dostupné, napr. informáciami o užívateľovi alebo majiteľovi užívateľskej adresy či zariadenia, pokiaľ je takéto údaje možné získať od príslušného poskytovateľa komunikačných služieb bez toho, aby tým došlo k ohrozeniu účelu trestného konania. V tejto súvislosti ústavný súd zdôrazňuje požiadavku dôslednosti a efektivity súdnej kontroly, a to s ohľadom na povahu daného konania, ktoré nepredpokladá účasť protistrany pred rozhodnutím súdu. Úloha súdu tak spočíva i vo „vyvažovaní“ procesnej situácie, pričom je neprípustné, aby sa súd dostal do pozície „pomocníka“ verejnej žaloby, pretože musí byť vždy nestranný (nález sp. zn. Pl. ÚS 789/06, bod 17).

138. Z uvedených skutočností je potrebné dospieť k záveru, že napadnuté ustanovenia neobstoja v druhom kroku testu proporcionality, lebo nepodmieňujú zisťovanie údajov o uskutočnenej komunikačnej prevádzke zo strany orgánov činných v trestnom konaní požiadavkou nevyhnutnosti a pre ich aplikáciu neustanovujú účinné prostriedky kontroly, ktoré by umožňovali účinnú ochranu základného práva na informačné sebaurčenie dotknutých osôb v priebehu celého obdobia, počas ktorého tieto orgány disponujú predmetnými údajmi. Pre úplnosť posúdenia ústavnosti napadnutých ustanovení je potrebné uviesť, že by neprešli ani cez tretí krok testu proporcionality, ktorého podstatou je posúdenie proporcionality v užšom zmysle. Napadnuté ustanovenia totiž neprikladajú žiaden význam povahe a závažnosti trestného činu, pre ktorý je trestné konanie vedené, a to i napriek tomu, že tieto skutočnosti sú už vo všeobecnej rovine významné pre výsledok pomeriavania v kolízii stojaceho základného práva na informačné sebaurčenie a verejného záujmu na predchádzaní a postihovaní trestných činov. Je úlohou zákonodarcu, aby presne určil, v prípade ktorých trestných činov tento verejný záujem prevažuje, pričom vo svojom rozhodnutí musí zohľadniť ich závažnosť. Z rovnakých zásad vychádza aj obmedzenie možnosti vydať príkaz na odpočúvanie a záznam telekomunikačnej prevádzky podľa § 115 Trestného poriadku iba pre trestné konanie o zločine, korupcii, trestných činoch extrémizmu, trestnom čine zneužívania právomoci verejného činiteľa, trestnom čine

legalizácie príjmu z trestnej činnosti alebo pre iný úmyselný trestný čin, o ktorom na konanie zaväzuje medzinárodná zmluva.

139. Vzhľadom na záver, že napadnuté ustanovenia Trestného poriadku a zákona o Policajnom zbore nie sú v súlade so základným právom na súkromie, nie je potrebné preskúmať súlad napadnutých ustanovení príslušných zákonov so zreteľom na čl. 25 ústavy a čl. 10 dohovoru, ktoré zaručujú právo na slobodu prejavu.

V.

140. Podľa čl. 125 ods. 3 ústavy ak ústavný súd svojím rozhodnutím vysloví, že medzi právnymi predpismi uvedenými v odseku 1 je nesúlad, strácajú príslušné predpisy, ich časti, prípadne niektoré ich ustanovenia účinnosť. Orgány, ktoré tieto právne predpisy vydali, sú povinné do šiestich mesiacov od vyhlásenia rozhodnutia ústavného súdu uviesť ich do súladu s ústavou, s ústavnými zákonmi a s medzinárodnými zmluvami vyhlásenými spôsobom ustanoveným zákonom. Ak tak neurobia, také predpisy, ich časti alebo ustanovenia strácajú platnosť po šiestich mesiacoch od vyhlásenia rozhodnutia.

141. Podľa čl. 125 ods. 6 ústavy rozhodnutie ústavného súdu vydané podľa odsekov 1, 2 a 5 sa vyhlasuje spôsobom ustanoveným na vyhlasovanie zákonov. Právoplatné rozhodnutie ústavného súdu je všeobecne záväzné. Dňom uverejnenia v Zbierke zákonov Slovenskej republiky zároveň zaniká platnosť uznesenia ústavného súdu č. k. PL. ÚS 10/2014-29 z 23. apríla 2014 v časti týkajúcej sa pozastavenia účinnosti § 58 ods. 5 až ods. 7 a § 63 ods. 6 zákona o elektronických komunikáciách uverejneného v Zbierke zákonov Slovenskej republiky pod č. 128/2014 Z. z. Vzhľadom na účinky ustanovenia čl. 125 ods. 3 ústavy (pozri predchádzajúci bod odôvodnenia tohto nálezu) sa však účinnosť ustanovení § 58 ods. 5 až ods. 7 a § 63 ods. 6 zákona o elektronických komunikáciách neobnovuje.

142. Vychádzajúc z uvedených ustanovení ústavy bude úlohou národnej rady do šiestich mesiacov od vyhlásenia tohto nálezu v Zbierke zákonov Slovenskej republiky uviesť § 58 ods. 5, 6 a 7 a § 63 ods. 6 zákona o elektronických komunikáciách, § 116 Trestného poriadku a § 76a ods. 3 zákona o Policajnom zbore do súladu s čl. 16 ods. 1, čl. 19 ods. 2 a 3 a čl. 22 ústavy v spojení s čl. 13 ods. 4 ústavy a čl. 8 dohovoru.

143. Vzhľadom na skutočnosť, že ústavný súd dospel k záveru, že napadnuté ustanovenia zákona o elektronických komunikáciách, Trestného poriadku a zákona o Policajnom zbore nie sú v súlade so základným právom na súkromie, nebolo potrebné preskúmať súlad napadnutých ustanovení príslušných zákonov s čl. 26 ústavy, čl. 10 dohovoru a čl. 11 charty, ktoré zaručujú právo na slobodu prejavu, a preto tejto časti návrhu skupiny poslancov nevyhovel.

144. Ústavný súd vychádzajúc z čl. 125 ods. 1 ústavy a svojej doterajšej judikatúry (PL. ÚS 3/09) nevyhovel návrhu poslancov ani v časti namietajúcej nesúlad napadnutých ustanovení príslušných zákonov s čl. 7, čl. 8, čl. 11 a čl. 52 ods. 1 charty, pretože vyslovením ich nesúladu s ustanoveniami ústavy, listiny a dohovoru uvedenými vo výroku tohto nálezu sa z hľadiska právnych dôsledkov vyplývajúcich z čl. 125 ods. 3 ústavy (strata účinnosti napadnutej právnej úpravy a po márnom uplynutí šiestich mesiacov aj prípadná strata ich platnosti) naplnil účel sledovaný návrhom skupiny poslancov, čím sa zároveň odstraňuje aj ich možný nesúlad s označenými ustanoveniami charty.

P o u č e n i e : Proti tomuto rozhodnutiu nemožno podať opravný prostriedok.

V Košiciach 29. apríla 2015