European Information Society Institute, o. z.
Dobrianskeho 1580, 093 01 Vranov nad Topľou, Slovakia
IČO: 42 227 950, www.eisionline.org, eisi@eisionline.org

Generálna prokuratúra Slovenskej republiky
Štúrova 2
812 85 Bratislava

Vo Vranove nad Topľou, dňa 08.02.2012

P O D N E T
NA PRESKÚMANIE ÚSTAVNOSTI PLOŠNÉHO ZBERU DÁT O OBČANOCH

- **Úvod**
- **Príloha č. 1: Vlastné posúdenie ústavnosti**
- **Príloha č. 2: Dôkazy o zneužívaní týchto údajov**

Dovoľujeme si Vás týmto upozorniť na nesúlad § 58 ods. 5, 6, 7 zákona NR SR č. 351/2011 Z.z. o elektronických komunikáciách v znení neskorších predpisov (ďalej aj *„zákon o elektronických komunikáciách* " alebo *„ZoEP"*) a § 116 Trestného poriadku s

- čl. 13 ods. 4, čl. 16 ods. 1, čl. 19 ods. 2, 3, čl. 22 Ústavy SR[1],
- čl. 7 ods. 1, čl. 10 ods. 2, 3, čl. 13 ústavného zákona č. 23/1991 Zb., ktorým sa uvádza Listina základných práv a slobôd (ďalej aj „Listina"),
- čl. 8 Dohovoru o ochrane ľudských práv a základných slobôd (ďalej aj „Dohovor")[2] a
- čl. 7, čl. 8 Charty základných práv Európskej únie (ďalej aj „*Charta*")[3].

Zákon o elektronických komunikáciách v § 58 ods. 5, 6 ZoEP **ukladá poskytovateľom elektronických komunikácií[4] 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. Predmetom uchovávania je **niekoľko desiatok údajov**, ktoré príloha č. 2 zákona o elektronických komunikáciách pre ich nepreberné množstvo ešte ďalej rozdeľuje do nasledovných kategórií:

- Identifikácia zdroja komunikácie,
- Identifikácia adresáta komunikácie,
- Identifikácia dátumu, času a trvania komunikácie,
- Identifikácia typu komunikácie,
- Identifikácia použitého komunikačného zariadenia,
- Identifikácia polohy komunikujúceho.

V rovnakom rozsahu sa uchovávajú aj **údaje súvisiace s neúspešnými pokusmi o volanie**.

Zavedenie povinnosti uchovávať údaje podľa vyššie uvedených ustanovení predstavuje **citeľný zásah do súkromného života**, **keďže ide o plošné 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 tajomstvá.

Potvrdzuje to aj **výskum vykonaný centrom pri Massachussets Institute of Technology**, ktorý ukázal, že až s 90% presnosťou je možné na základe vyššie uvedených údajov určiť okruh spolupracovníkov, priateľov a známych. Dokonca je podľa takéhoto profilu možné **predpovedať aj správanie sa jednotlivca** (napr. kedy sa bude nachádzať doma, v práci alebo na inom mieste)[5]. O každom občanovi štát zbiera obrovské množstvo príliš citlivých informácií, ktoré denne iba čakajú na svoje zneužitie. Aby sme však neostali len pri konštatovaniach, na konci tohto podania (viď Príloha č. 2) pripájame aj **dôkazy tohto zneužitia zo strany štátnych orgánov**.

[1] Zákon č. 460/1992 Ústava SR.

[2] Oznámenie Federálneho ministerstva zahraničných vecí č. 209/1992 Zb. Dohovor o ochrane ľudských práv a základných slobôd.

[3] Charta základných práv Európskej únie (2007/C 303/01) [online]. Dostupné na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12007P/TXT:SK:HTML.

[4] Podnikom na účely tohto zákona je každá osoba, ktorá je oprávnená poskytovať sieť, službu alebo sieť a službu v oblasti elektronických komunikácií bez ohľadu na právnu formu a spôsob financovania, napr. mobilní operátori, poskytovatelia internetového pripojenia.

[5] Viac na: http://reality.media.mit.edu/dyads.php.

Sme presvedčení, že uchovávanie informácií v takom širokom rozsahu je v rozpore s ústavným poriadkom. Nadôvažok, dnešná úprava je úplne ústretová voči všetkým druhom zneužitia týchto údajov a aj proces komunikácie týchto údajov je upravený veľmi benevolentne. Pre porovnanie. **Zásah do súkromia, ktorý vzniká pri odpočúvaní je menej intenzívny** ako pri uchovávaní všetkých hore uvedených údajov (porovnaj bod 27, Pl. ÚS 42/11, ÚS ČR). V prvom rade, odpočúvanie sa týka iba úzkeho počtu osôb, zatiaľ čo plošný monitoring všetkých občanov. Ďalej, odpočúvanie je inštitút smerujúci do budúcna (odhaľuje komunikáciu, ktorá sa ešte len uskutoční), plošný monitoring je inštitútom, ktorý smeruje do minulosti (odhaľuje komunikáciu, ktorá vznikla pred tým ako bolo napr. začaté trestné stíhanie). Inštitút plošného monitoringu je teda inštitút preventívny. Za tretie, informačná hodnota údajov získaných na základe plošného monitoringu je oveľa väčšia, keďže obsah hovoru môžno zmanipulovať ľahšie, ako osobné návyky človeka. Napokon, dáta získané na základe plošného monitoringu občanov možno automaticky spracúvať, vyhodnocovať a spájať, čo nie je dobré možné pri odpočúvaní.

Napriek týmto štyrom argumetom, je **dnešná úprava získavania, uchovávania a sprístupňovania týchto dát úplne arbitrárna a oveľa benevolentnejšia ako inštitút odpočúvania**. Samotný zber podlieha minimálnemu počtu pravidiel. Systém uchovávania údajov neobsahuje takmer žiadne záruky proti ich zneužívaniu a hlavná úloha je prenechaná súkromným spoločnostiam, ktoré majú prirodzene skôr záujem na minimalizácií nákladov, keďže im štát túto činnosť neuhrádza. Sprístupňovanie týchto údajov sa potom riadi neprecíznou právnou úpravou, ktorá spôsobuje, že tieto informácie sú orgánmi verejnej moci protiústavne používané aj pri odhaľovaní priestupkov a menej závažných trestných činov.

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.

Generálnej prokuratúre ako jednému z najdôležitejších orgánov ochrany ústavnosti preto dávame do pozornosti fakt, že ustanovenia § 58 ods. 5, 6, 7 zákona o elektronických komunikáciách sú 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). Je porušením tohto ustanovenia, ak právo na nedotknuteľnosť súkromia, súkromný život, ochranu pred neoprávneným zhromažďovaním údajov o svojej osobe a tajomstva dopravovaných správ, štát obmedzí spôsobom, ktorý jednak postráda dosiahnuteľný cieľ, ale najmä ohrozuje ich samotnú podstatu. Podľa posledných **výskumov Inštitútu Maxa Plancka** totiž zbieranie týchto údajov **nemá žiadny pozitívny vplyv na odhaľovanie závažných trestných činov** v Európe[6].

K podobným záverom v iných členských štátoch Európskej únie dospel aj Ústavný súd v Rumunsku[7], Nemecku[8], Česku (Pl. ÚS 24/10, Pl. ÚS 42/11) a taktiež Najvyšší súd v Bulharsku[9] a na Cypre[10]. Ústavnosť tohto druhu právnej úpravy sa v súčasnej dobe preskúmava aj v Maďarsku a Poľsku.

[6] Kriminologická štúdia *Stutzlücken durch Wegfall der Vorratsdatenspeicherung* – http://vds.brauchts.net/MPI_VDS_Studie.pdf.
[7] Nález Rumunského ústavného súdu č.1258 zo dňa 8. októbra.2009.
[8] Rozsudok Spolkového ústavného súdu zo dňa 2. 3. 2010 sp. zn. 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08.
[9] Rozsudok Najvyššieho správneho súdu č. 13627 zo dňa 11. december 2008.
[10] Viac na: http://www.edri.org/edrigram/number9.3/data-retention-un-lawful-cyprus.

Máme za to, že plošné a preventívne uchovávanie dát bez existencie akéhokoľvek predchádzajúceho podozrenia z ohrozenia, či porušenia zákonom chránených záujmov, vedie k záveru, že vlastne **každá osoba je a priori považovaná za podozrivú**. Takýto záver je však v rozpore so základnou zásadou demokratického právneho štátu, a to zásadou prezumpcie neviny, ktorá vychádza z klasického chápania „praesumptio boni viri“, podľa ktorého sa občan zásadne považuje za dobrého a spravodlivého až do okamihu, kým sa preukáže opak. **Nie je možné akceptovať, aby prevencia boja s akýmkoľvek druhom kriminality narástla až do takej miery, že ohrozí samotné demokratické zriadenie a pohltí súkromie všetkých občanov.**

Náš návrh

Žiadame Vás preto, aby ste sa postavili na stranu ochrany ľudských práv a slobôd obyvateľov Slovenskej republiky a bez odkladu podali Ústavnému súdu SR **návrh na začatie konania o súlade** § 58 ods. 5, 6, 7 zákona NR SR č. 351/2011 Z.z. o elektronických komunikáciách v znení neskorších predpisov a § 116 Trestného poriadku s čl. 13 ods. 4, čl. 16 ods. 1, čl. 19 ods. 2, 3, čl. 22 Ústavy SR.

S úctou,
Martin Husovec a Ľubomír Lukič,
za European Information Society Institute, o.z.

Príloha č. 1
Vlastné posúdenie protiústavnosti

(1) Ústava SR v čl. 22 ods. 2 a Listina v čl. 13 ustanovujú, že 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. Z toho jednoznačne vyplýva, že ide predovšetkým o ochranu vlastného obsahu.

(2) Avšak Ústavný súd ČR vo svojom náleze sp. zn. II. ÚS 502/2000 judikoval, že v zmysle čl. 13 Listiny[11] je súkromie každého človeka hodné ochrany nielen vo vzťahu k vlastnému obsahu správ podávaných telefónom, ale i vo vzťahu k volaným číslam, dátam a čase hovoru, dobe jeho trvania, v prípade mobilných telefónov aj k základným staniciam zaisťujúcim hovor. Tieto údaje sú neoddeliteľnou súčasťou komunikácie uskutočňovanej prostredníctvom telefónu. Toto logicky vyplýva z povahy komunikácie aj na elektronickú poštu a na pripojenie k internetu.

(3) Ako zásah do súkromného života je podľa judikatúry ESĽP[12] potrebné chápať ako kontrolu obsahu pošty a telefónnych hovorov,[13] tak aj zisťovanie telefónnych čísel telefonujúcich osôb,[14] či uchovávanie informácií, že daná osoba telefonovala s určitou osobou[15]. Nie je pri tom rozhodujúce, či uchovávané údaje boli nejakým spôsobom použité alebo zverejnené.[16]

(4) 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[17].

(5) Uchovávanie údajov po dobu 6, resp. 12, mesiacov znamená latentné nebezpečie 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.

(6) 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. Dokonca je podľa takéhoto profilu možné predpovedať aj správanie sa jednotlivca.[18]

(7) Preventívne plošné uchovávanie telekomunikačných údajov predstavuje vážny zásah, resp. obmedzenie základných práv.[19] 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

[11] Teda aj v zmysle čl. 22 Ústavy SR.

[12] Európsky súd pre ľudské práva (European Court of Human Rights). Jediný skutočný súdny orgán založený Európskym dohovorom o ľudských právach. Má 46 sudcov a ako posledná inštancia zaručuje, že zmluvné štáty dodržiavajú svoje povinnosti vyplývajúce z dohovoru. Viac na: http://www.echr.coe.int/echr/Homepage_EN.

[13] Rozsudok ESĽP vo veci Klaas proti Nemecku zo dňa 22.9.1993, sťažnosť č. 15473/89.

[14] Rozsudok ESĽP vo veci P.G. a J.H. proti Spojenému kráľovstvu zo dňa 25.9.2001, sťažnosť č. 44787/98 a Rozsudok ESĽP vo veci Malone proti Spojenému Kráľovstvi zo dňa 2.8.1984, sťažnosť č. 8691/79.

[15] Rozsudok ESĽP vo veci Amann proti Švajčiarsku zo dňa 16.2.2000, sťažnosť č. 327798/95.

[16] Rozsudok ESĽP vo veci Copland proti Spojenému kráľovstvu zo dňa 3.4.2007, sťažnosť č. 62617/00 a a Rozsudok ESĽP vo veci Rotaru proti Rumunsku zo dňa 4.5.2000, sťažnosť č. 28341/95.

[17] WINDTHORST, K. *Verfassungsrecht I. Grundlagen*, 1.vydanie. Mníchov, 1994. 295 s. ISBN 9783406385360.

[18] Viac na: http://reality.media.mit.edu/dyads.php.

[19] Rovnako ako odpočúvanie telefónnych rozhovorov verejnou mocou a iné tajné sledovanie.

zodpovedajúcich právnych predpisov a účinnej kontroly ich dodržiavania. Skryté sledovanie orgánmi verejnej moci je preto s ohľadom na vyššie uvedené základné právo na ochranu súkromia možné vždy iba v legitímnom záujme a na základe zákona.[20]

(8) 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 (Nález Ústavného súdu SR, sp. zn. I. ÚS 117/07).

1. Posúdenie zberu a uchovávania údajov

(9) V prípade stretu práv či slobôd s verejným záujmom alebo inými základnými právami a slobodami, je potrebné posudzovať účel, resp. cieľ takéhoto zásahu vo vzťahu k použitým prostriedkom, pričom mierou takéhoto posúdenia je práve zásada proporcionality (primeranosti v širšom zmysle.), tiež môže byť nazývaná aj ako zákaz nadmerných zásahov do práv a slobôd (Nález Ústavného súdu ČR, sp. zn. Pl. ÚS 8/06). Zásada proporcionality teda predstavuje najvýznamnejší korektív a obmedzenie štátnych zásahov do práva na súkromie.

(10) 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 (Nález Ústavného súdu SR, sp. zn. I. ÚS 117/07). Taktiež je nevyhnutné, aby štátny orgán vykonával diskrečnú právomoc v dobrej viere, starostlivo a rozumným spôsobom a aby mal na to príslušne postačujúce dôvody.

(11) Vo veci Klaas proti Nemecku ESĽP uviedol, že demokratické spoločnosti sú v súčasnosti ohrozované veľmi sofistikovanými formami špionáže a terorizmom, a preto štát musí mať možnosť sledovať podvratné živly, ktoré by mohli operovať na jeho území.[21] Pripustil preto, že existencia zákonných opatrení oprávňujúcich štátne orgány k uskutočňovaniu tajného sledovania korešpondencie, poštových zásielok a telekomunikácií je nevyhnutná v demokratickej spoločnosti k ochrane národnej bezpečnosti a ochrane poriadku či prevencii zločinnosti. Súd pripomenul, že i keď dohovor ponecháva zmluvným štátom istú voľnosť, pokiaľ ide o voľbu podmienok systému sledovania **neznamená to, že by bola neobmedzená vo vzťahu k podrobeniu osôb, ktoré podliehajú ich jurisdikcií, tajným sledovacím opatreniam.** Štáty tak nemôžu prijať akékoľvek opatrenie, ktoré by považovali za vhodné, s odôvodnením, že tak robia v rámci boja proti špionáži a terorizmu. Súd sa musí navyše presvedčiť, že existovali tomu odpovedajúce a dostatočné záruky proti zneužitiu takýchto opatrení.[22]

(12) Ústavný súd ČR judikoval, že zásada proporcionality sa vzťahuje aj na zásahy štátu do práva na súkromie upraveného v čl. 13 Listiny. Keď ústavný poriadok pripustí prielom tejto ochrany (práva na ochranu súkromia), deje sa tak výlučne a v záujme ochrany demokratickej spoločnosti, prípadne v záujme iných ústavne zaručených základných práv a slobôd; tu patrí predovšetkým nevyhnutnosť daná všeobecným záujmom na ochrane spoločnosti pred trestnými činmi a na tom, aby takéto trestné činy boli zistené a potrestané. Prípustný je teda iba zásah do základného práva alebo slobody človeka zo strany štátnej moci pokiaľ ide o zásah nevyhnutný vo vyššie uvedenom zmysle. K tomu, aby neboli prekročené medze nevyhnutnosti, musí existovať systém adekvátnych a dostatočných záruk, skladajúci sa z odpovedajúcich právnych predpisov a účinnej kontroly ich dodržiavania (Nález Ústavného súdu ČR, sp. zn. II. ÚS 502/2000).

(13) 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.

[20] HERCZEG,J. Ústavněprávní limity monitoringu telekomunikačního provozu: konflikt mezi bezpečností a svobodou. In *Bulletin Advokácie*. 2010, č. 5, s. 22-31.

[21] Rozsudok ESĽP vo veci Klaas proti Nemecku zo dňa 22.9.1993, sťažnosť č. 15473/89.

[22] HERCZEG,J. Ústavněprávní limity monitoringu telekomunikačního provozu: konflikt mezi bezpečností a svobodou. In *Bulletin Advokácie*. 2010, č. 5, s. 22-31.

(14) Vzhľadom na vyššie uvedené, ustanovenie ukladajúce povinnosť uchovávať údaje je nevyhnutné podrobiť „testu proporcionality“, ktorý patrí k štandardným právnym nástrojom ako európskych ústavných súdov, tak aj súdov medzinárodných pri posudzovaní konfliktu ustanovenia právneho poriadku, sledujúceho ochranu ústavne zaručeného práva alebo verejného záujmu, s iným základným právom či slobodou (PL ÚS 23/06, PL. ÚS 3/09, PL. ÚS 3/00, PL. ÚS 67/07).[23] Táto zásada zahŕňa tri kritéria posudzovania prípustnosti zásahu z hľadiska:

•**test legitímneho cieľa** – je nutné určiť, či daným opatrením je vôbec možné dosiahnuť legitímny cieľ (účel),

•**test potrebnosti** – skúma sa, či je takéto opatrenie nevyhnutné k tomu, aby bol dosiahnutý cieľ, resp. či by rovnaký výsledok nemohol byť dosiahnutý aj menej obmedzujúcim spôsobom,

•**test proporcionality stricto sensu** (v užšom slova zmysle) – zisťuje sa, či ujma na základnom práve nie je neprimeraná v porovnaní so zamýšľaným cieľom, t.j. že opatrenia obmedzujúce základné ľudské práva svojimi negatívnymi dôsledkami neprevyšujú pozitíva, ktoré predstavuje verejný záujem na týchto opatreniach.

1.1 Test legitímneho cieľa

(15) Uchovávaním údajov nie je možné dosiahnuť legitímny cieľ, resp. ho možno dosiahnuť len v menej významných prípadoch, pričom sa nedá očakávať ani dlhodobý a pozitívny vplyv na zníženie kriminality a zvýšenie bezpečnosti. Existuje totiž viacero spôsobov, **ako sa vyhnúť uchovávaniu dát**. Stačí si zvoliť iný spôsob komunikácie, ktorý nie je zatiaľ štátom monitorovaný.

(16) 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)[24], IRC (Internet relay chat)[25], peer-to-peer (P2P)[26] komunikácie, nakoľko tieto nepoužívajú protokoly predpokladané ZoEK, resp. šifrujú komunikáciu.

(17) Efektivita ZoEK, resp. smernice je navyše limitovaná územím nášho štátu, resp. členských štátov. Poskytovatelia služieb a sietí tretích krajín nemajú povinnosť uchovávať údaje, a teda, ak bude niekto komunikovať prostredníctvom týchto poskytovateľov, jeho údaje sa nebudú uchovávať.

(18) Ďalším spôsobom je šifrovanie emailu alebo využívanie jedného emailového konta viacerými užívateľmi ako schránku na odkazy. Existujú aj služby, ktoré fungujú na rovnakom princípe, avšak v ich prípade nejde ani o emailové kontá, napr. Dropbox,[27] Writeboard[28].

(19) Ďalším príkladom ako sa vyhnúť uchovávaniu dôležitých údajov o komunikácií, je použitie telefónnej búdky alebo tzv. anonymných predplatených telefónnych kariet. Ide o také karty, pri kúpe ktorých nie je nevyhnutné preukazovať svoju totožnosť.

(20) Vyhnúť sa uchovávaniu možno aj oveľa sofistikovanejším spôsobom a to použitím komerčných služieb na anonymizáciu komunikácie alebo systému The Onion Router (TOR)[29] či systému JAP (JonDo)[30]. Komerčné služby na anonymizáciu komunikácie sú založené prevažne na systéme proxy serverov[31].

---

[23] HERCZEG,J. Ústavněprávní limity monitoringu telekomunikačního provozu: konflikt mezi bezpečností a svobodou. In *Bulletin Advokácie*. 2010, č. 5, s. 22-31.

[24] https://secure.wikimedia.org/wikipedia/en/wiki/Instant_messaging.

[25] https://secure.wikimedia.org/wikipedia/sk/wiki/Internet_Relay_Chat.

[26] https://secure.wikimedia.org/wikipedia/en/wiki/Peer-to-peer.

[27] Pozri https://www.dropbox.com/.

[28] Pozri http://writeboard.com/.

[29] Pozri https://www.torproject.org/.

[30] Systém fungujúci na podobnom princípe ako TOR. Je vyvíjaný za spolupráce nasledujúcich inštitúcii: Technische Universität Dresden, the Universität Regensburg and Privacy Commissioner of Schleswig-Holstein. Viac na: http://anon.inf.tu-dresden.de/index_en.html.

[31] https://secure.wikimedia.org/wikipedia/sk/wiki/Server_proxy.

(21) 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 uchovávanie 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. Ustanovenia ukladajúce povinnosť uchovávať údaje tak v konečnom dôsledku nevedú k účinnejšiemu boju proti organizovanému zločinu a terorizmu, ale iba k využívaniu iných foriem komunikácie medzi osobami, proti ktorých trestnej činnosti sú tieto ustanovenia namierené. Ospravedlňujúci dôvod, pre ktorý bolo prijaté takéto závažné obmedzenie hneď niekoľkých základných práv a slobôd, preto postráda účinnosť hodnú takéhoto obmedzenia.

1.2 Test potrebnosti

(22) V prípade potrebnosti je nutné si položiť hneď niekoľko otázok. V prvom rade, či je uchovávanie prevádzkových a lokalizačných údajov ako takých, vôbec potrebné pre ochranu verejného záujmu v demokratickej spoločnosti. Ďalej, ak áno, je rozsah dnes uchovávaných údajov, či doba, po ktorú sa údaje uchovávajú, potrebná podľa kriminologických výskumov na boj s týmto druhom kriminality. A napokon, či existujú menej invazívne, ale ekvivaletne efektívne, spôsoby boja proti závažnej kriminalite.

(23) Súčasné štúdie, predovšetkým však kriminologická štúdia Inštitútu Maxa Plancka *´Stutzlücken durch Wegfall der Vorratsdatenspeicherung?´*[32] poukazuje na to, že zbieranie prevádzkových a lokalizačných údajov, pravdepodobne z dôvodov načrtnutých vyššie, **vôbec nevedie k lepšiemu odhaľovaniu závažnej trestnej činnosti**.

1.3 Test proporcionality stricto sensu

(24) Pri posudzovaní primeranosti, resp. neprimeranosti vplyvu týchto opatrení na dotknuté osoby je nutné zohľadňovať najmä dva faktory, a to **rozsah a závažnosť zásahu** do práva na súkromie, a **existenciu adekvátnych a dostatočných záruk** proti zneužitiu uchovávaných údajov.

1.3.1 Rozsah a závažnosť zásahu do práva na súkromie dotknutých osôb

(25) 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.

(26) 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.

(27) 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 užitočností 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

[32] Kriminologická štúdia *Stutzlücken durch Wegfall der Vorratsdatenspeicherung* – http://vds.brauchts.net/MPI_VDS_Studie.pdf.

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.

(28) 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.

(29) 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.

(30) Pri pospájaní jednotlivých uchovávaných údajov a pri spojení týchto údajov s ďalšími informáciami môžeme odhaliť podstatnú časť súkromia dotknutej osoby. Umožní 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 telefónnu 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.[33]

(31) 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.

(32) To, že uchovávanie údajov vnímajú aj ľudia ako výrazný zásah do práva na súkromný život dokazujú aj zahraničné prieskumy[34].

1.3.2 Adekvátne a dostatočné záruky proti zneužitiu uchovávaných údajov

(33) 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.[35]

---

[33] Porov. FEILER, L. The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection, In *European Journal of Law and Technology*. 2010, č.3.

[34] Prieskum, ktorého sa zúčastnilo 1000 Nemcov v roku 2008, ukázal, že kvôli uchovávaniu údajov o komunikácií by jeden z dvoch Nemcov nepoužil telefón alebo email pri kontaktovaní manželského poradcu, psychoterapeuta alebo poradcu na odvykanie od drog, ak by potreboval ich pomoc. Jeden z trinástich Nemcov už aspoň raz nepoužil telefón alebo email kvôli uchovávaniu údajov. (Meinungen der Bundesbürger zur Vorratsdatenspeicherung [online]. Dostupné na: http://www.eco.de/dokumente/20080602_Forsa_VDS_Umfrage.pdf.

1.Prieskum, ktorého sa zúčastnilo 1489 nemeckých novinárov v roku 2008, ukázal, že jeden zo štrnástich novinárov už aspoň raz kvôli vedomiu, že údaje o komunikácií sa uchovávajú, pocítil negatívny účinok pri kontaktovaní svojich zdrojov na informácie. (Freie Journalisten in Deutschland [online]. Dostupné na: http://www.webcitation.org/5sLdXIt55.

2.V roku 2008 prieskum Eurobarometer ukázal, že 69-81 % občanov EÚ odmieta myšlienku monitorovania používania internetu alebo hovorov osôb, ktoré nie sú podozrivé zo spáchania tresného činu, a to aj napriek tomu, že takéto monitorovanie by pomohlo v boji proti medzinárodnému terorizmu. (Data Protection in the European Union – Citizens' Perceptions [online]. Dostupné na: http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

[35] Rozsudok Spolkového ústavného súdu zo dňa 2. 3. 2010, sp. zn. 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08.

(34) Zákonodarca síce stanovil bezpečnostné opatrenia jednak v § 56 ods. 2 ZoEK, a taktiež aj v § 58 ods. 10 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. Navyše, k zneužitiu uchovávaných údajov môže dôjsť aj samotným poskytovateľom a to najmä za účelom marketingu svojich služieb.

(35) 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[36]. 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.

(36) Záruky proti zneužitiu uchovávaných údajov treba 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.

(37) 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 v úvahu ročnú štatistiku o uchovávaných údajoch (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.

Tab. 1

Rok	Počet prípadov, v ktorých sa požadované údaje poskytli oprávneným orgánom štátu	Počet prípadov, kedy nebolo možné žiadosti o údaje vyhovieť
2008	319	65
2009	5214	157
2010	7417	7126

Štatistika bola EISI poskytnutá Ministerstvom dopravy, výstavby a regionálneho rozvoja Slovenskej republiky na základe žiadosti o sprístupnenie informácií v zmysle zákona č. 211/2000 Z.z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

(38) 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.

[36] *Alarmující výzkum: Více než polovině britských firem již unikla data [online], [25.01.2011]*. Dostupné na: http://securityworld.cz/securityworld/alarmujici-vyzkum-vice-nez-polovine-britskych-firem-jiz-unikla-data-251.

(39) Je teda zrejmé, že právna úprava je úplne benevoletná, neproporcionálna a neposkytuje žiadne záruky proti zneužitiu týchto citlivých údajov. Naopak, vytvára len priestor pre čoraz väčšiu minimalizáciu súkromia občanov. Právna úprava je teda protiústavná hneď na niekoľkých úrovniach prieskumu ústavnosti tak, ako bol načrtnutý vyššie.

2. Posúdenie sprístupňovania údajov podľa § 116 TP

(40) Uchovávané údaje je podnik povinný v súlade s § 58 ods. 7 ZoEP poskytnúť na základe **písomnej žiadosti a so súhlasom súdu alebo na príkaz súdu** podľa osobitných predpisov[37] 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.**

(41) **Predseda senátu** a pred začatím trestného stíhania alebo v prípravnom konaní **sudca pre prípravné konanie** na odôvodnený návrh prokurátora môže podľa § 116 Trestného poriadku vydať pre **úmyselný trestný čin 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.

(42) Ako sme už vyššie uviedli, 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.

(43) 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 § 116 TP (viď Tab. 1).

(44) 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.

(45) Všetky tieto garancie jednoznačne v právnej úprave absentujú, a preto je ustanovenie § 116 TP vystavené až priveľkej diskrécii zo strany súdov. Hoci by Ústavný súd nemal intervenovať tam, kde právna úprava pripúšťa ústavnoprávny výklad, jeho **autoritatívny zásah je nevyhnutný, ak prax všeobecných súdov všeobecne vybočuje z hraníc ústavnosti**.

[37] § 116 Trestného poriadku.

Príloha č. 2: Dôkazy o zneužívaní týchto údajov

KRAJSKÉ RIADITEĽSTVO POLICAJNÉHO ZBORU

ÚRAD JUSTIČNEJ A KRIMINÁLNEJ POLÍCIE

Kuzmányho 8, 040 01 Košice

[redacted]

Váš list číslo/zo dňa	Naše číslo	Vybavuje/linka	Košice
	[redacted]		

Vec
Žiadosť o poskytnutie informácií
- zaslanie

V súvislosti s preverovaním podozrenia zo spáchania trestného činu Vás v zmysle § 76a ods.3, Zákona č. 171/1993 Z.z. žiadam o poskytnutie informácií k osobe, ktorá vystupuje pod nickom „[redacted]“ - „**IP:** [redacted]“ na lokálnom dc++ hube, ktorý prevádzkujete. Taktiež Vás žiadam o termín zriadenia horeuvedeného nicku na uvedenom dc++ hube.

Zároveň Vás žiadam ak je to možné **o zálohovanie** následovných súborov z ponuky „[redacted]“ ide o tieto:

- zo súboru **Hudba** - pod súbor **Rock - celý**
  - pod súbor **N.S.B.M - celý**
  - pod súbor **Nacional Socialist - celý**

V prípade začatia trestného stíhania budú tieto informácie oficiálne vyžiadané vyšetrovateľom PZ na základe udelenia súhlasu prokurátora.

[redacted]

Telefón	Fax	E-mail	Internet	IČO
89 / 230 31	89 / 260 09	[redacted]		

OKRESNÉ RIADITEĽSTVO POLICAJNÉHO ZBORU V KOŠICIACH – OKOLIE
ODBOR PORIADKOVEJ POLÍCIE
OBVODNÉ ODDELENIE POLICAJNÉHO ZBORU JASOV
JASOV 358, 044 23 JASOV

[redacted]

Váš list číslo/zo dňa	Naše číslo	Vybavuje/linka	Jasov
	[redacted]		

Vec
neznámy páchateľ - žiadosť

Tunajšia súčasť Obvodného oddelenia PZ Jasov, okres Košice – okolie, vykonáva objasňovanie priestupku proti občianskemu spolunažívaniu podľa § 49 ods. 1 písm. d) zák. č. 372/1990 Zb. o priestupkoch, ktorého sa dopustil neznámy páchateľ a to tým spôsobom, že dňa 18.05 2010 v čase od 13.36 hod do 12.56 dňa 28.05 2010 neoprávnene vystupoval pod nickom Gejza Brostl na stránke obce Jasov, okr. Košice – okolie a týmto svojím konaním poškodil reputáciu Gejzu Brostla.

Za účelom riadneho zadokumentovania tohto priestupku žiadam Vašu spoločnosť v zmysle § 60 ods. 1 písm. e) zák. č. 372/1990 Zb. o priestupkoch o poskytnutie nasledovných údajov:

- či je u Vás registrovaná adresa počítača **IP** [redacted], ak áno žiadam Vás o poskytnutie údajov majiteľa tohto počítača
- uveďte iné skutočnosti dôležité pre objasnenie priestupku

Správu v dvoch vyhotoveniach zašlite k hore uvedenému číslu na tunajšie oddelenie Obvodné oddelenie PZ Jasov, PSČ 044 23, okres Košice – okolie, podľa možnosti obratom.

Obvodné oddelenie PZ Jasov 02

[redacted]

Telefón	Fax	E-mail	Internet	IČO
89/33904	055/4668695	oojasov@minv.sk		