Digitálna verejná správa a ľudské práva

Matej Gera

Martin Husovec

Štefan Szilva

Petra Zabuďková

EISI European Information Society Institute

Mgr. Matej Gera, LL.M.

Mgr. Martin Husovec

Štefan Szilva

Mgr. Petra Zabuďková, LL.M.

Digitálna verejná správa a ľudské práva

Prvé vydanie. Vydalo European Information Society Institute, o. z. v roku 2015, http://eisionline.org.

Recenzoval: JUDr. Jakub Harašta

Jazyková korektúra: Bc. Adriána Keszeliová

ISBN 978-80-971307-3-2 (tlač)

ISBN 978-80-971307-4-9 (pdf)

MINISTERSTVO ZAHRANIČNÝCH VECÍ
A EURÓPSKYCH ZÁLEŽITOSTÍ
SLOVENSKEJ REPUBLIKY

Realizované s finančnou podporou Ministerstva zahraničných vecí a európskych záležitostí SR v rámci dotačného programu Podpora a ochrana ľudských práv a slobôd LP/2015. Za obsah tohto dokumentu je výlučne zodpovedný European Information Society Institute, o. z.

Obsah

1. Úvod

Žijeme v období, v ktorom mnoho súčastí nášho života prešlo do digitálnej sféry. Činnosti ako vzdelávanie, práca, nakupovanie či dokonca zdravie sú v mnohých ohľadoch dnes prenesené do sveta jednotiek a núl. Je preto samozrejmé, že sa do množiny digitálnych aktivít dostáva aj interakcia so štátom. Elektronická verejná správa prináša nespočetné množstvo výhod – ušetrený čas, peniaze i energiu. Miesto chodenia po úradoch sa občania dožadujú čoraz širšieho okruhu služieb, ktoré vybavia z pohodlia domova. Digitalizácia verejnej správy je nevyhnutná pre moderné a úspešné Slovensko. Ak chce byť Slovensko ideálnym miestom na život a lukratívnym podnikateľským prostredím, obmedzovaniu papierovania a zvyšovaniu počtu „klikov“ sa nevyhne ani slovenská verejná správa.

Ako ukázalo nedávne obdobie, skutočnosť o stave informatizácie slovenskej verejnej správy je omnoho trpkejšia, než si je sama verejná správa ochotná priznať. Kým vláda hlása s veľkou pompou úspešnú finalizáciu jednej z etáp informatizácie[1], skúsenosti občanov a názory odborníkov z IT sektora hovoria o polofunkčných službách a premrhanej miliarde eur.[2] Elektronické služby štátu zostávajú zložité, neprehľadné, duplicitné, neinkluzívne, neautomatické a predovšetkým predražené.

Neteší nás preto, že v čase, keď sa na nepodarenú informatizáciu valí stále väčšia vlna kritiky, musíme sa pridať na stranu skeptikov. Len málokedy sa totiž pri digitalizácii verejnej správy hľadí na možné negatívne dopady, ktoré digitalizácia môže mať na ľudské práva. Občania môžu byť ako dôsledok nesprávnych technologických postupov postavení mimo novej digitálnej spoločnosti, znevýhodnení vo výkone svojich základných ľudských práv či dokonca priamo diskriminovaní zo strany verejnej moci. Nesprávna digitalizácia môže ohroziť samotné ľudské práva.

Je načase preskúmať, ako by sa verejná moc mala pri digitalizácii svojej

1 „Slovensko je na elektronickú komunikáciu občanov s verejnou správou pripravené a teraz je rad na ľuďoch, aby začali tieto služby využívať.“ - dostupné http://www.teraz.sk/slovensko/projekty-informatizacie-spolocnosti-s/142652-clanok.html

2 Pozri najmä iniciatívu „To sa nedá“ (https://www.facebook.com/tosanedask/, http://slovensko.digital, http://slovensko.wtf).

činnosti správať - tak, aby rešpektovala tieto hodnoty. V rámci projektu „Digitálna verejná správa a ľudské práva“ predkladá European Information Society Institute (EISi) túto publikáciu, ktorá má slúžiť ako varovný prst pre štát a verejnú správu. Zároveň by mala byť aj vstupnou bránou do problematiky ľudských práv v kontexte e-Governmentu a aj pre každého, koho problematika zaujíma a kto sa s ňou stretáva na dennej báze – právnici, úradníci, novinári, aktivisti či celkom „bežní občania“.

Publikácia sa skladá z dvoch častí. Prvá časť mapuje štvoricu reálnych problémov, ktoré svojou závažnosťou upútali pozornosť verejnosti. Účelom prvej polovice knihy je ozrejmiť faktické okolnosti problémov, dôvody ich vzniku, ich technické pozadie a načrtnutie právneho problému, ktorý pre ľudské práva predstavujú. Následne, čerpajúc z poznatkov získaných v prvej časti, v druhej sú rozoberané problémy analyzované podrobnejšie a s optikou zameranou na základné práva občanov a ľudí žijúcich na Slovensku. Rozdelená je na dva podsegmenty – prvý sa venuje elektronickej komunikácii so štátom a druhý sa zaoberá zberom osobných údajov.

Publikácia si kladie za cieľ zvýšiť povedomie čitateľov a upriamiť pozornosť na porušovanie základných práv štátom a verejnou správou ako na reálnu hrozbu. Knižka má poskytnúť prvotnú právnu analýzu ľudskoprávnych nedostatkov, ktoré v minulosti pretrvávali, v súčasnosti trvajú alebo ešte len budú implementované do života ľudí. Zároveň má čitateľovi poskytnúť referenčný rámec, aby si viac uvedomoval kam siahajú hranice toho, čo štát – s ohľadom na základné práva – v oblasti informatizácie verejnej správy smie a kde sa, naopak, dopúšťa nedovoleného obmedzovania ľudských práv.

Za autorský kolektív Vám želá príjemné čítanie,

Matej Gera

2. Prípadové štúdie

Prvá časť publikácie ukazuje a vysvetľuje problémy spojené s digitalizáciou verejnej správy na reálnych prípadoch a pochybeniach, ktorých sa zákonodarca či orgány verejnej správy na Slovensku dopustili. Vysvetlí faktické a technologické pozadie prípadov a históriu jednotlivých káuz, ktoré sa na Slovensku buď udiali a boli napravené, pretrvávajú dlhšie obdobie, alebo ktoré s veľkou pravdepodobnosťou nastanú v blízkej budúcnosti. Zároveň bude načrtnutý rozpor so základnými právami porušenými verejnou správou buď legislatívou, alebo aktivitou. Podrobná právna analýza prípadov bude nasledovať v druhej časti publikácie.

Stať venujúca sa prípadovým štúdiám poskytne náhľad na štyri prípady, ktoré zarezonovali medzi verejnosťou. Ide o:

- Elektronické výkazy k DPH – povinnosť podávať elektronické výkazy k dani z pridanej hodnoty.
- Register zverejňovania ponúk prevodu vlastníctva poľnohospodárskeho pozemku – povinnosť oznámiť zámer predať niektoré druhy pozemkov alebo záujem o kúpu pozemku elektronicky.
- Mobilná aplikácia „Superkolky“ – zber osobných údajov používateľov aplikácie Finančnej správy SR.
- Jednotný informačný systém v cestnej doprave a sledovanie žiakov autoškoly – zber a uchovávanie osobných údajov o žiakoch autoškôl a vyučujúcich.

2.1. Elektronické výkazy k DPH

Platitelia dane z pridanej hodnoty, ktorí dodávajú tovary a služby medzi rôznymi členskými štátmi EÚ sú povinní podávať mesačný alebo štvrťročný výkaz. Až do konca roka 2009 platila v SR povinnosť podávať Súhrnný výkaz k DPH v listinnej forme a daňové subjekty mali dobrovoľnú možnosť rozhodnúť sa podávať tento výkaz elektronicky. Od roku 2010 bola novelou zákona o DPH zavedená povinná elektronická forma výkazov. Technické riešenie vyžadovalo použitie portálu „eTax“,

aplikácie „Externý klient DR SR“ a aplikácie „eDane“ – tieto však boli funkčné len v prípade použitia komerčného softvéru od konkrétnej spoločnosti.

2.1.1. Vznik a história problému

Vstupom SR do Európskej únie nadobudol 1. mája 2004 účinnosť aj nový zákon o dani z pridanej hodnoty (ďalej len „ZDPH“)[3]. Zákon predpisoval povinnosť podávať súhrnné výkazy k dani z pridanej hodnoty, pričom povinná osoba mala dve možnosti – podať súhrnný výkaz v papierovej forme alebo dobrovoľne elektronicky so zaručeným elektronickým podpisom.[4] Možnosť elektronického podávania výkazov bola v roku 2005 rozšírená o možnosť podávania aj bez zaručeného elektronického podpisu, ktorý bol málo rozšírený. Subjekty povinné odovzdávať výkazy tak mali dve možnosti pri dobrovoľnom elektronickom podávaní – buď musel výkaz obsahovať zaručený elektronický podpis, alebo mohol platiteľ uzavrieť s daňovou správou osobitnú dohodu o elektronickom doručovaní, v prípade ktorého sa nemusí použiť zaručený elektronický podpis. K definovaniu tohto nového spôsobu elektronického podávania výkazov došlo novelizáciou § 80 zákona.

V roku 2010 sa možnosť podávať výkaz elektronicky zmenila na povinnosť. Úprava v ZDPH po novelizácii (a v súčasnom znení) ustanovuje, že „[Dotknuté osoby] sú povinné podať súhrnný výkaz elektronickými prostriedkami […]. Súhrnný výkaz musí byť podpísaný zaručeným elektronickým podpisom. Súhrnný výkaz podaný elektronickými prostriedkami nemusí byť podpísaný zaručeným elektronickým podpisom ak osoba, ktorá podáva súhrnný výkaz, má s daňovým úradom uzavretú písomnú dohodu […]“.[5]

Proti tejto zmene bolo v pripomienkovom konaní vznesených niekoľko rozumných pripomienok, napr. zo strany Ministerstva dopravy, pôšt a telekomunikácií SR, ktoré konštatovalo, že nie každá zdaniteľná osoba je pripojená na internet, príp. že

3 Zákona č. 222/2004 Z.z., o dani z pridanej hodnoty, v znení neskorších predpisov.

4 §80 zákona č. 222/2004 Z.z. od 1.5.2004 do 31.12.2004 znel: „(8) Platiteľ môže podať súhrnný výkaz aj elektronicky. Elektronicky podaný súhrnný výkaz musí obsahovať zaručený elektronický podpis podľa osobitného predpisu.“ (Osobitným predpisom je Zákon č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov.)

5 § 80, ods. 9 (v znení od 1.1.2010).

nie vždy sa môže osoba úspešne pripojiť na internet.[6] Slovenská komora daňových poradcov upozorňovala na potenciálny problém pre zahraničných platiteľov.[7]

Dôvodová správa k tejto legislatívnej zmene nesprávne tvrdila, že elektronická povinnosť sa vyžaduje na základe zapracovávaných právnych predpisov EÚ.[8] Ako však upozornili niektorí pripomienkovatelia zákona, smernica EÚ poukazovala iba na možnosť vyžadovania elektronického podávania výkazov, nie však na povinnosť. Tento záver je evidentný zo znenia implementovanej smernice, ktorá hovorí o tom, že „Členské štáty *povoľujú a môžu požadovať*, aby sa v súlade s podmienkami, ktoré stanovia, súhrnný výkaz uvedený v odseku 1 podával v podobe súboru zaslaného elektronicky“.[9] Nič by teda nebránilo eventuálnemu používaniu ďalších, papierových foriem a podávanie výkazov by mohlo byť umožnené napr. prostredníctvom pošty.[10] Napriek výhradám zostal § 80 ZDPH vo vyššie uvedenom znení dodnes a zákonodarca i naďalej vyžaduje elektronické podávanie súhrnných výkazov. Za nepodanie výkazu sa daňovému subjektu ukladá finančná sankcia.

Na využitie možnosti elektronického doručovania výkazov bez zaručeného elektronického podpisu je povinnou podmienkou podpísanie „Dohody o spôsobe doručovania písomností doručovaných elektronickými prostriedkami, ktoré nebudú podpísané zaručeným elektronickým podpisom uzatvorená podľa § 20 ods. 8 zákona č.

6 Citát pripomienky: "Navrhujeme dve alternatívy týkajúce sa zmeny povinnosti podať súhrnný výkaz elektronickými prostriedkami. Možnosť podať súhrnný výkaz elektronicky, ale aj poštou (nie každá zdaniteľná osoba je pripojená na internet a nie vždy je pripojenie úspešné) je v súlade so smernicou Rady 2008/117/ES v čl. 263 ods. 2 (členské štáty povoľujú a môžu požadovať, aby sa v súlade s podmienkami, ktoré stanovia, súhrnný výkaz uvedený v odseku 1 podával v podobe súboru zaslaného elektronicky)." Zdroj – *Vyhodnotenie medzirezortného pripomienkového konania* [online]. Úrad vlády SR [cit. 30.11.2015].

7 Ibid., citát pripomienky Slovenskej komory daňových poradcov: "V tejto súvislosti navrhujeme zakotviť do zákona možnosť podávať súhrnný výkaz aj inými ako elektronickými prostriedkami, kedy je použitý zaručený elektronický podpis, resp. prostredníctvom uzavretia písomnej dohody s daňovým úradom v prípade podávania súhrnných výkazov bez zaručeného elektronického podpisu aspoň počas určitého prechodného obdobia. Smernica takúto možnosť nevylučuje, a pri zahraničných platiteľoch dane zastúpených v SR prostredníctvom splnomocnenia je elektronické podávanie výkazov a priznaní problematické a oveľa menej využívané.“

8 „K bodu 31 (§ 80)“ ... „Na základe článku 263 ods. 2 smernice Rady 2006/112/ES (novelizovaný smernicou Rady 2008/117/ES) sa vyžaduje, aby sa súhrnný výkaz podával elektronicky.“ Pozri dôvodovú správu - *B. Osobitná časť* [online]. Úrad vlády SR [cit. 30.11.2015].

9 Čl. 263 ods. 2, Smernica Rady 2008/117/ES, zo 16. decembra 2008, ktorou sa mení a dopĺňa smernica 2006/112/ES o spoločnom systéme dane z pridanej hodnoty s cieľom bojovať proti daňovým podvodom spojeným s transakciami v rámci Spoločenstva.

10 Pozri pozn. č. 4.

511/1992 Zb. v znení neskorších predpisov“[11] s príslušným daňovým úradom. Dohoda je však jednostranne vytvorená Finančným riaditeľstvom SR (pôvodne Daňovým riaditeľstvom) a jej neakceptovanie znamená stratu možnosti podávania výkazov bez zaručeného elektronického podpisu. Možnosť podávania výkazov bez zaručeného elektronického podpisu vyplýva od 1. januára 2005 z §80 ods. 9 ZDPH a tiež z §20 ods. 8 zákona č. 511/1992 Zb. o správe daní, nahradeného §13 ods. 5 zákona č. 563/2009 Z.z.. V zmysle týchto predpisov dohoda „obsahuje najmä náležitosti elektronického doručovania, spôsob overovania podania urobeného elektronickými prostriedkami a spôsob preukazovania doručenia“.

Dohoda, ktorú však Daňové riaditeľstvo predpísalo, obsahovala od roku 2005 do konca roku 2011 aj požiadavky na používanie konkrétneho internetového prehliadača a tým aj konkrétneho komerčného operačného systému. Dohoda tiež obsahuje ustanovenia a požiadavky nad rámec tých, ktoré predpisuje ZDPH. Článok 4 dohody označený ako „Práva a povinnosti daňového subjektu“ v bode 4.8 napríklad ustanovuje možnosť náhradného doručovania písomností v prípade prekážok pri elektronickom doručovaní, pričom ZDPH sa o takej možnosti nezmieňuje:

> „4.8 Ak z dôvodu prekážok, ktoré nie sú na strane správcu dane, nemôže daňový subjekt doručiť správcovi dane písomnosti elektronickou formou, ktoré nebudú podpísané zaručeným elektronickým podpisom, v lehote ustanovenej osobitným zákonom, je povinný doručiť písomnosti v zákonom stanovenej lehote miestne príslušnému správcovi dane na predpísaných tlačivách iným vhodným spôsobom. Oneskorené doručenie písomností elektronickou formou má rovnaké právne následky ako oneskorené doručenie iným spôsobom.“

Bod 4.6 dohody predpisuje povinnosť samostatne v listinnej forme doručovať daňovému úradu súhrnné informácie z elektronicky podaného výkazu, pričom ich nezaslanie má podľa bodu 4.7 dohody za následok, že sa elektronicky doručený výkaz bude považovať za nedoručený:

11 Dohoda o spôsobe doručovania písomností doručovaných elektronickými prostriedkami, ktoré nebudú podpísané zaručeným elektronickým podpisom uzatvorená podľa § 20 ods. 8 zákona č. 511/1992 Zb. v znení neskorších predpisov [online]. Portál daňovej správy SR (archivovaná stránka) [cit. 30.11.2015].

„4.6 Daňový subjekt je povinný preukázať podanie písomnosti doručovanej elektronickými prostriedkami, ktoré nebudú podpísané zaručeným elektronickým podpisom tak, že do piatich pracovných dní odo dňa jej podania doručí správcovi dane prvú stranu doručenej písomnosti a písomné Vyhlásenie o podaní písomnosti elektronickou formou podľa vzoru, ktorý bude zverejnený na internetovej stránke Daňového riaditeľstva SR (www.drsr.sk).“

„4.7 Ak v lehote piatich pracovných dní odo dňa podania písomnosti na elektronickú podateľňu ... daňový subjekt nedoručí miestne príslušnému správcovi dane prvú stranu doručenej písomnosti a písomné Vyhlásenie o podaní písomnosti elektronickou formou, hľadí sa na písomnosť akoby nebola podaná. Zmeškanie lehoty nie je možné odpustiť.“

2.1.2. Technické pozadie problému

Podávanie výkazov elektronicky fungovalo na podklade niekoľkých softvérových riešení, ktoré sa vystriedali v období od roku 2004 do súčasnosti. Až do roku 2012 všetky tieto riešenia vyžadovali používanie konkrétneho komerčného operačného systému, a to pre obe možnosti elektronického podávania výkazov: so zaručeným elektronickým podpisom a aj bez zaručeného elektronického podpisu na základe dohody o elektronickom doručovaní.

2.1.2.1. Podávanie so zaručeným elektronickým podpisom

Pri podávaní elektronických výkazov so zaručeným elektronickým podpisom je až do súčasnosti zo strany Finančnej správy SR vyžadované používanie aplikácie D.Signer, ktorá bola certifikovaná Národným bezpečnostným úradom. Pre vytváranie zaručeného elektronického podpisu totiž bolo možné do roku 2014 v zmysle §3 ods. 2 písm. g) vyhlášky Národného bezpečnostného úradu č. 134/2009 Z.z. používať výlučne softvér, pre ktorý tento úrad vydá certifikát, pričom pre jeho vydanie bolo potrebné splniť viaceré finančne náročné kroky, ako napríklad bezpečnostný audit.[12] Proces certifikácie tak obvykle absolvovali len komerčné subjekty. Tie následne takýto certifikovaný softvér predávali verejnej správe alebo verejnosti. Až do roku 2012

12 *Certifikácia produktov* [online]. Elektronická podpis, Národný bezpečnostný úrad SR [cit. 30.11.2015].

Národný bezpečnostný úrad vydal certifikát len pre softvér pre vytváranie zaručeného elektronického podpisu, ktorý bol určený pre komerčný operačný systém Microsoft Windows, keďže žiaden subjekt nepožiadal o certifikáciu softvéru pre iný operačný systém.[13] V roku 2012 bol na základe žiadosti komerčnej firmy certifikovaný softvér Web Signer pre vytváranie zaručeného elektronického podpisu, a to priamo na webových stránkach v operačných systémoch Microsoft Windows, Apple Mac OS X a Linux, avšak Finančná správa a ani iná organizácia verejnej správy ho neobstarala, a tak ho nie je možné používať pre priame podpisovanie a podávanie dokumentov. V roku 2014 bola vytvorená a certifikovaná aplikácia D.Signer Java pre operačné systémy Windows, Mac OS X a Linux.[14] Pre používanie tejto verzie D.Signer je však potrebné, aby ju poskytovala samotná verejná správa ako súčasť svojich webových stránok. Finančná správa túto verziu dodnes neposkytuje.

Do roku 2012 tak bolo možné v SR so zaručeným elektronickým podpisom podpisovať dokumenty len z jediného operačného systému od jedného výrobcu. Finančná správa napriek obstarávaniu viacerých softvérových riešení nepožadovala od svojich dodávateľov dodanie certifikovaného softvéru pre zaručený elektronický podpis pre iné operačné systémy. Po verejnej kritike sa Finančná správa bránila tým, že tento problém sa týka celej verejnej správy a dodávateľov.[15]

Od roku 2014 bola napokon novelou vyhlášky č. 134/2009 Z.z. vypustená povinnosť v §3 ods. 2 písm. g) používať pre vytváranie zaručeného elektronického podpisu výlučne certifikovaný softvér a certifikácia sa vyžaduje v zmysle §57e Výnosu Ministerstva financií SR č. 55/2014 Z.z. už iba pre softvér, ktorý je súčasťou informačných systémov verejnej správy. Necertifikovaný softvér pre zaručený elektronický podpis kompatibilný s portálom finančnej správy podľa dostupných informácií zatiaľ nie je k dispozícii.

13 NBÚ nemá problém certifikovať elektronický podpis pre iné systémy. *IT NEWS* [online]. Digital Visions, spol. s.r.o., vydané 19.04.2010 [cit. 30.11.2015].

14 *Certifikované produkty pre používateľov* [online]. Elektronický podpis – Zoznam ceritifkovaných produktov, Národný bezpečnostný úrad [cit. 30.11.2015].

15 Za povinný Windows môže podľa daňového riaditeľstva NBÚ. *IT NEWS* [online]. Digital Visions, spol. s.r.o., vydané 16.04.2010 [cit. 30.11.2015].

2.1.2.2. Podávanie bez zaručeného elektronického podpisu (s tzv. elektronickou značkou)

Pri podávaní výkazov bez zaručeného elektronického podpisu platila povinnosť podpísania dohody o elektronickom doručovaní, ktorá v článku 5 označenom ako "Náležitosti elektronického doručovania" až do konca roka 2011 vyžadovala od daňového subjektu akceptovanie používania konkrétneho internetového prehliadača a technických podmienok zverejnených na webových stránkach Daňového riaditeľstva:

> „5.1 Daňový subjekt akceptuje technické podmienky pre elektronické doručovanie písomností, ktoré nebudú podpísané zaručeným elektronickým podpisom, ktoré sú zverejnené na internetovej stránke Daňového riaditeľstva SR.
>
> 5.2 Daňový subjekt akceptuje pre elektronické doručovanie písomností, ktoré nebudú podpísané zaručeným elektronickým podpisom, výhradné používanie prehliadača Internet Explorer verzia minimálne 5.5.“

Až v roku 2012 Finančná správa vytvorila novú dohodu o doručovaní, ktorá už priamo nepredpisovala používanie konkrétneho internetového prehliadača. Vyžaduje už len dodržiavanie technických podmienok zverejnených na webových stránkach Finančnej správy.[16]

Finančná správa pre elektronické podávanie výkazov bez zaručeného elektronického podpisu vyžadovala do roku 2012 v podmienkach používania elektronických služieb používanie rovnakej aplikácie D.Signer, ktorá bola vyžadovaná aj pre vytváranie zaručeného elektronického podpisu. Ako dôvod Finančná správa uvádzala potrebu certifikácie softvéru Národným bezpečnostným úradom. Po stanovisku Národného bezpečnostného úradu, že pre podanie bez zaručeného elektronického podpisu certifikácia softvéru nie je potrebná,[17] Finančná správa na žiadosť uviedla, že dôvodom vyžadovania rovnakého softvéru je „unifikácia riešenia

16 *Dohoda o elektronickom doručovaní uzatvorená podľa §13 ods.5 zákona č. 563/2009 Z.z. v znení neskorších predpisov* [online]. Portál ďanovej správy SR (archivovaná stránka) [cit. 30.11.2015].

17 *Zaslanie odborného stanoviska.* č. 3856/2010/KÚ/SOdOP-007 [online]. Vytovrené 16.06.2010 [cit. 30.11.2015].

postupov pre elektronické doručovanie daňových dokumentov“ a „zabezpečenie efektívneho vynakladania finančných prostriedkov v daňovej správe SR“.[18]

2.1.2.3. Softvérové riešenia poskytované pre splnenie povinného elektronického podávania výkazov

a) Systém eTax

Systém eTax fungoval od roku 2004 do konca 2013. Podľa dostupných informácií bol systém eTax obstaraný a financovaný Ministerstvom financií Dánskeho kráľovstva, a to v rámci pomoci Slovenskej republike pred vstupom do Európskej únie. Následne bol odovzdaný do majetku Daňového riaditeľstva SR.[19]

Problematickým momentom fungovania systému eTax bola nutnosť inštalácie aplikácie „D.Signer/XML“, ktorá je určená na vytváranie zaručeného elektronického podpisu. Aplikácia bola funkčná výlučne na operačnom systéme Microsoft Windows a len vo webovom prehliadači Internet Explorer – vďaka používaniu technológií, ktoré v iných operačných systémoch a webových prehliadačoch nebolo možné využívať.

Do polovice roku 2010 bol systém eTax jediným technickým riešením pre splnenie zákonnej povinnosti elektronického podania súhrnných výkazov DPH. Bez ohľadu na to, či povinná osoba komunikovala s daňovou správou prostredníctvom zaručeného elektronického podpisu alebo mala so správcom dane uzatvorenú dohodu o elektronickom doručovaním, v oboch prípadoch prebiehalo podávanie súhrnných výkazov prostredníctvom systému eTax a vyžadovalo sa použitie komerčného operačného systému. V samotnej dohode o spôsobe doručovania si daňová správa vynucuje použitie prehliadača Internet Explorer vo verzii 5.5. alebo vyššej, ktorý bol dostupný len pre jediný komerčný operačný systém od spoločnosti Microsoft.[20]

b) Externý klient DR SR

18 *Odpoveď Daňového riaditeľstva na žiadosť o sprístupnenie informácií* . č. I/252/9847-68834/2010/Mal. [online]. [cit. 30.11.2015].

19 *Čo je to eTax* [online]. Portál daňovej správy SR (archivovaná stránka) [cit. 30.11.2015].

20 Bod 5.2. dohody - *Dohoda o spôsobe doručovania písomností doručovaných elektronickými prostriedkami, ktoré nebudú podpísané zaručeným elektronickým podpisom uzatvorená podľa § 20 ods. 8 zákona č. 511/1992 Zb. v znení neskorších predpisov* [online]. Portál daňovej správy SR (archivovaná stránka) [cit. 30.11.2015].

Aplikácia Externý klient DR SR bola spustená v polovici roka 2010 a fungovala popri systéme eTax ako alternatíva pre podávanie súhrnných výkazov k DPH bez nutnosti navštíviť portál daňovej správy a bez potreby používania internetového prehliadača.[21] Fungovala tak i v prípade nedostupnosti portálu, čo bol v danom období opakovaný problém. Zahŕňala v sebe aj aplikáciu pre podpisovanie – D.Signer. Rovnako ako eTax však aplikácia pre svoje spustenie vyžadovala od používateľov operačný systém Microsoft Windows.[22]

c) eDane

V polovici roka 2011 spustila Daňová správa SR ďalšiu aplikáciu pod názvom eDane. Aplikácia nahradila Externého klienta DR SR a takisto umožňovala podávanie výkazov bez potreby použitia portálu daňovej správy a internetového prehliadača. Na rozdiel od Externého klienta DR SR, ktorý slúžil len pre súhrnné výkazy k DPH, aplikácia eDane obsahovala viacero vybraných daňových dokumentov, výkazov a priznaní, ktoré bolo možné cez ňu vyplniť a podať.

Aplikácia eDane – tak, ako všetky predchádzajúce technické riešenia, vyžadovala, resp. v sebe integrovala aplikáciu D.Signer a bola opäť spustiteľná len na jedinom operačnom systéme.[23] K náprave došlo v decembri 2012, keď popri pôvodnej aplikácii eDane bola spustená verzia eDane Java využívajúca odlišnú technológiu a fungujúcu nezávisle od operačného systému či prehliadača.[24] Táto aplikácia slúžila pre podávanie bez zaručeného elektronického podpisu. V polovici roku 2014 bola sprístupnená verzia eDane Java 2014 pre podávanie so zaručeným elektronickým podpisom aj bez zaručeného elektronického podpisu. Táto v sebe zahŕňa aj aplikáciu D.Signer Java.[25]

d) EZU

21 *Náhradná stránka* [online]. Portál ďanovej správy SR (archivovaná stránka) [cit. 30.11.2015].
22 *Postup inštalácie offline aplikácie Súhrnný výkaz* [online]. Portál ďanovej správy SR (archivovaná stránka) [cit. 30.11.2015].
23 *eDane – Používateľská príručka* [online]. Portál ďanovej správy SR (archivovaná stránka) [cit. 30.11.2015].
24 *Elektronické podávanie dokumentov* [online]. Finančná správa SR (archivovaná stránka) [cit. 30.11.2015].
25 Aplikácia eDane [online]. Finančná správa SR (archivovaná stránka) [cit. 30.11.2015].

Na začiatku roka 2012 bol spustený systém „Elektronický zber údajov“ (EZU), ktorý mal nahradiť systém eTax a ponúkal na vyplnenie rôzne daňové dokumenty, vrátane výkazov.[26] Bol určený pre podávanie bez zaručeného elektronického podpisu a neobsahoval softvér, ktorý by bol certifikovaný Národným bezpečnostným úradom. Bol funkčný z rôznych operačných systémov vďaka používaniu prostredia Java. Systém EZU však bol vypnutý na konci roka 2012 a väčšina používateľov bola presunutá do aplikácie eDane a na portál Finančnej správy. Namiesto pôvodne vydaného prístupového privátneho kľúča im bolo zaslané prístupové meno a heslo.[27]

e) Nový portál Finančnej správy

V roku 2014 Finančná správa sprístupnila nový portál, ktorý nahrádza systém eTax a poskytuje možnosť vypĺňania a podávania rôznych daňových dokumentov. Systém síce je funkčný v rôznych webových prehliadačoch na rôznych operačných systémoch, avšak pre podávanie dokumentov opäť vyžaduje inštaláciu aplikácie D.Signer, ktorú ponúka výlučne pre operačný systém Microsoft Windows.[28]

Od roku 2014 tak môžu používatelia podávať výkazy prostredníctvom dvoch typov aplikácie – Portál Finančnej správy a eDane vo verzii Windows a vo verzii Java. Nemožnosť použiť aplikáciu eDane na mobilných zariadeniach naďalej pretrváva, nakoľko tieto aplikácie nie je možné priamo spúšťať v najrozšírenejších operačných systémoch pre mobilné zariadenia ako je Android či iOS.

2.1.3. Zhrnutie problému

So vstupom SR do Európskej únie v roku 2004 bola zavedená povinnosť podávať súhrnné výkazy v režime zákona o dani z pridanej hodnoty. Do roku 2009 bola popri elektronickej možnosti zachovaná možnosť podávať výkazy aj v papierovej forme. Napriek mnohým protestom bola novelizáciou v 2009 zrušená možnosť podávať výkazy v papierovej forme. Elektronická forma sa stala jediným zákonným spôsobom na splnenie si svojej povinnosti odovzdať súhrnné výkazy.

26 EZU/eTax [online]. Finančná správa SR (archivovaná stránka) [cit. 30.11.2015].
27 *Oznámenie k elektronickému doručovaniu* [online]. Finančná správa SR (archivovaná stránka) [cit. 30.11.2015].
28 *Overenie splnenia podmienok AES* [online]. Elektronické služby, Finančná správa SR [cit. 30.11.2015].

Napriek tomu, že zákon odlišoval dve formy komunikácie – elektronickú komunikáciu so zaručeným elektronickým podpisom alebo elektronickú komunikáciu na základe dohody s finančnou správou – obe formy si vynucovali použitie operačného systému od spoločnosti Microsoft a prehliadača Internet Explorer. Zákonodarca a verejná správa nútila občanov v období 2010 – 2012 používať konkrétny komerčný softvér pre splnenie svojich zákonných povinností, a to napriek tomu, že v tomto časovom horizonte sa vystriedali tri odlišné technické riešenia podávania výkazov.

Právna úprava a správanie daňovej správy mali citeľne negatívny dopad, a to najmä v podnikateľskom prostredí. Spor známy ako EURA[29] je ukážkovým príkladom toho, ako štát zasiahol do slobody podnikania a znemožnil podnikateľskému subjektu splnenie jeho zákonných povinností, pričom zároveň za nesplnenie povinností udelil subjektu viacero vysokých pokút. Ak podnikateľ používal iný zakúpený alebo bezplatný operačný systém ako je napríklad Apple OS X alebo GNU/Linux, bol v dôsledku postupu daňovej správy nútený investovať do konkurenčného komerčného softvérového produktu spoločnosti Microsoft.[30]

2.2. Register zverejňovania ponúk prevodu vlastníctva poľnohospodárskeho pozemku

Od júna 2014 sú vlastníci poľnohospodárskej pôdy, ktorí chcú previesť vlastníctvo na inú osobu (najmä ak iná osoba nie je poľnohospodárom v danej obci alebo blízka či príbuzná osoba), povinní zverejniť ponuku v elektronickom registri, ktorý je na webovom sídle ministerstva pôdohospodárstva. Podobnú povinnosť majú osoby, ktoré chcú vlastníctvo k takémuto pozemku nadobudnúť a musia v tomto registri elektronicky zaznamenať záujem o ponuku. Túto povinnosť nie je možné splniť inak než elektronicky. Webové sídlo ministerstva pôdohospodárstva je pritom technicky vytvorené tak, že pre splnenie uvedenej povinnosti vyžaduje použitie

29 Pozri aj kapitolu 3.1. Na tomto mieste sa patrí upozorniť, že v prípade EURA intervenovalo priamo aj European Information Society Institute, o.z. na strane podnikateľa. Viac informácií o prípade na *Štát zanedbal otvorené štandardy, podnikateľ ho teraz žaluje* [online]. Súdy a občianska spoločnosť, European Information Society Institute [cit. 30.11.2015].

30 Viac k prípadu pozri tiež *Odmietol Windows. Zažaloval štát, teraz čiastočne vyhral* [online]. Súdy a občianska spoločnosť, European Information Society Institute [cit. 30.11.2015].

elektronického občianskeho preukazu s aktivovaným čipom a aplikácie eID klient, ktorá až do konca júna 2015 bola k dispozícii len pre jediný komerčný operačný systém.

2.2.1. Vznik a história problému

V júni 2014 vstúpil do účinnosti zákon č. 140/2014 Z.z. o nadobúdaní vlastníctva poľnohospodárskeho pozemku a o zmene a doplnení niektorých zákonov (ďalej len „zákon o nadobúdaní vlastníctva“). Podľa slov predkladateľov právneho predpisu má zákon posilniť ochranu poľnohospodárskej pôdy pred špekulatívnymi nákupmi a zneužívaním vlastníctva. Zákon má zabezpečiť, aby poľnohospodárske pozemky slúžili naďalej svojmu účelu a aby ich nadobúdali primárne osoby, ktoré podnikajú alebo vykonávajú poľnohospodársku výrobu.[31] Samotný zákon, jeho účel a spôsob obmedzenia nakladania s vlastníctvom nevyvoláva pochybnosti len vo vzťahu k elektronizácii verejnej správy. Zákon bol napadnutý na Ústavnom súde SR poslancami Národnej rady SR, ktorí navrhli preskúmať jeho súladnosť s právom vlastniť majetok a z dôvodu protiústavnej diskriminácie.[32]

Jedným z konkrétnych prostriedkov zavedených zákonom je povinnosť zverejniť svoj úmysel previesť vlastníctvo poľnohospodárskeho pozemku aspoň na obdobie 15 dní v Registri zverejňovania ponúk prevodu poľnohospodárskeho pozemku (ďalej len „register“) nachádzajúcom sa na webovom sídle Ministerstva pôdohospodárstva a rozvoja vidieka SR (ďalej len „MPSR“). Zároveň musí túto ponuku zverejniť v rovnakom čase aj na úradnej tabuli v obci, kde sa poľnohospodársky pozemok nachádza.[33] Osoba, ktorá chce prejaviť záujem o nadobudnutie pozemku tak musí učiniť rovnako prostredníctvom registra na stránkach MPSR.

Povinné elektronické zverejnenie úmyslu či prejavenie záujmu nie je možné

31 *Dôvodová správa* [online]. Vládny návrh zákona o nadobúdaní vlastníctva poľnohospodárskeho pozemku a o zmene a doplnení niektorých zákonov, parlamentná tlač 977, Národná rada SR [cit. 30.11.2015], s. 1.

32 *Návrh na začatie konania na preskúmanie súladu zákona č. 140/2014 Z.z.* [online]. Vyhľadávanie rozhodnutí, Ústavný súd SR [cit. 30.11.2015].

33 Tento postup je vlastník povinný použiť v prípade, ak neprevádza vlastníctvo na osoby podnikajúce alebo vykonávajúcej poľnohospodársku výrobu, spoluvlastníkov alebo osoby blízke. Presné definície pozri § 4 ods. 1 zákona č. 140/2014 Z.z.

vykonať žiadnym iným spôsobom a elektronické zaznamenanie úmyslu do registra MPSR je jedinou možnou formou. Pritom však v ďalšej fáze prevodu vlastníctva o splnení podmienok na prevod rozhoduje okresný úrad v tom okrese, v ktorom sa nachádza predmetný pozemok. Okresný úrad vydáva o tejto skutočnosti osvedčenie v správnom konaní. Odmietnutie vydať osvedčenie je preskúmateľné súdom. Je teda zrejmé, že vo fáze, ktorá bezprostredne nasleduje zverejnenie záujmu o predaj pozemku, je možné činiť návrhy v papierovej forme.

2.2.2. Technické pozadie problému

Register je dostupný na webovom sídle MPSR – na adrese https://pozemky.mpsr.sk/. Je verejne prístupný, každý návštevník webového sídla môže prezerať a vyhľadávať v zozname zverejnených pozemkov.

Ak chce používateľ zverejniť svoj úmysel previesť vlastníctvo k pozemku, musí sa v prvom rade prihlásiť na portáli prostredníctvom položky „Prihlásiť“ v menu. Po kliknutí je používateľ vyzvaný, aby spustil aplikáciu eID klient slúžiacu na prihlásenie s použitím elektronického občianskeho preukazu. Samotná stránka upozorňuje, že bez tejto aplikácie nie je možné pokračovať v prihlásení.[34]

Z vyššie uvedeného je zrejmé, že technické riešenie zverejňovania ponúk v registri pozemkov vyžaduje, aby občan vlastnil občiansky preukaz s aktivovaným elektronickým čipom, ktorý sa používa ako autentifikátor osoby. V súčasnosti má takýto občiansky preukaz (s aktivovaným elektronickým čipom) len menšie percento Slovákov.[35] Z technického hľadiska je tak predaj pozemkov v situáciách stanovených zákonom o nadobúdaní vlastníctva znemožnený mnohým občanom.

Navyše, celé zverejňovanie pozemkov fungovalo len na jedinom operačnom systéme, a to od spoločnosti Microsoft. Aplikácia eID klient, ktorá je nutná pre komunikáciu s elektronickým občianskym preukazom, bola až do leta 2015 dostupná

34 Obrazovka „Spustite aplikáciu eID klient“ - Pozri na https://eidas.minv.sk/TCTokenService/jsp/startEIDClient.jsp?tcTokenId

35 Približne 10% v auguste 2015 – má ísť o približne polovicu z približne 1 milióna vydaných občianskych preukazov s čipom – štatistika z článku KOLLÁROVÁ, Zuzana. 6 rád ako vybaviť e-občiansky a elektronický podpis. *Trend.sk* [online]. © 2015 News and Media Holding, vydané 23.07.2015 [cit. 1.12.2015].

len pre operačný systém Windows.[36] Občania používajúci iné populárne operačné systémy (napr. pre osobné počítače ako GNU/Linux alebo Mac OS X alebo pre mobilné zariadenia – Android a iOS) zostali bez možnosti zverejňovať svoje ponuky v registri, a to aj v prípade, ak mali aktivovaný elektronický občiansky preukaz.

Z vyššie uvedeného vyplýva, že systém zverejňovania pozemkov v registri MPSR mal dva zásadné technické nedostatky: 1. aby mohol občan zverejniť svoju ponuku, musí mať aktivovaný elektronický občiansky preukaz, čo pre občanov, ktorí ešte majú platný starý občiansky preukaz, znamená povinnosť vybaviť si nový preukaz s čipom (finančná záťaž – správny poplatok 4,50 €[37] – môže byť v tomto ohľade pre niektoré skupiny občanov taktiež nie zanedbateľná okolnosť); 2. aby mohol občan zverejniť svoju ponuku, musí vlastniť komerčný operačný systém od konkrétnej spoločnosti.

Od konca júna 2015 čiastočne odpadol problém s eID klientom, ktorý bol konečne zverejnený aj pre operačné systémy Apple OS X a GNU/Linux – distribúcie Debian, Ubuntu a Mint. Riešenie pre operačné systémy pre mobilné zariadenia (ako sú smartfóny či tablety) však stále absentuje. Príkladom riešenia môže byť Estónsko, kde sú od roku 2012 poskytované aplikácie pre operačné systémy Android a iOS.[38]

2.2.3. Zhrnutie problému

Majitelia pozemkov a záujemcovia o kúpu musia od júna 2014 v prípadoch stanovených zákonom o nadobúdaní vlastníctva poľnohospodárskeho pozemku povinne oznámiť svoj úmysel pozemok predať či kúpiť. Povinnosť si môžu občania splniť len elektronicky a len v prípade, že majú nový typ občianskeho preukazu s čipom. Do leta 2015 bolo povinnosť možné splniť iba ak mal používateľ nainštalovaný komerčný operačný systém od konkrétneho výrobcu. Naďalej však pretrváva absencia možnosti používať operačné systémy na mobilných zariadeniach.

36 *eID klient už aj pre Mac a Linux* [online]. Oznamy, Slovensko.sk – ústredný portál verejných služieb ľuďom, vydané 30.06.2015 [cit. 30.11.2015].

37 Od decembra 2013 vydáva Slovenská republika elektronické občianske preukazy - eID karty [online]. Tlačové správy, Ministerstvo vnútra SR [cit. 01.12.2015].

38 *Digital Signing Now Possible on Android Smartphones and Tablets* [online]. News, Mobiil-Id, ID.ee [cit. 01.12.2015].

V dôsledku zákonného príkazu splniť si povinnosť elektronicky a obmedzujúceho technického riešenia systému majú mnohí vlastníci značne sťažené možnosti disponovať so svojim majetkom. Problém sa citeľne dotýka najmä skupín obyvateľstva, ktoré je viac zraniteľné z ekonomického či vedomostného hľadiska (napr. dôchodcovia alebo občania zo sociálne slabších pomerov). Tieto skupiny obyvateľstva si v mnohých prípadoch buď nevedia, alebo – v dôsledku finančných obmedzení – nemôžu dovoliť zaobstarať osobný počítač a komerčný operačný systém. Občania sú tak zásadne obmedzení pri nakladaní so svojimi pozemkami. Vynára sa otázka, či je obmedzovanie vlastníckeho práva týmto spôsobom v poriadku.

2.3. Mobilná aplikácia „Superkolky“

V máji 2015 vydala Finančná správa SR (ďalej len „FS SR“) aplikáciu „Superkolky“ ktorá má slúžiť na overovanie pravosti alkoholu. FS SR si od aplikácie sľubuje zníženie obsahu nelegálneho alkoholu v obehu. „Superkolky“ fungujú na zdanlivo jednoduchom princípe – používateľ aplikácie môže naskenovať QR kód na kontrolnej známke výrobku a overiť tak pravosť výrobku. V prípade, že informácia na kolku nezodpovedá obsahu výrobku, môže používateľ túto informáciu oznámiť FS SR. Aplikácia však zbiera podstatne viac údajov, než je potrebné na splnenie jej cieľa (napr. poloha alebo údaje o telefonátoch). Nejasný rozsah zberu informácií vzbudzuje podozrenie, že zozbierané osobné údaje by mohli byť zneužité a mohlo by dôjsť k zásahu do súkromia používateľov aplikácie.

2.3.1. Vznik a história problému

Od roku 2015 nadobudli kontrolné známky (ľudovo nazývané tiež „kolky“) na alkohole, tabaku a tabakových výrobkoch novú podobu. Zmena vyplýva z novelizácie právneho rámca spotrebnej dane z alkoholu, tabaku a tabakových výrobkov. Podľa novej úpravy musia kolky povinne obsahovať aj jedinečný alfanumerický kód a tzv. QR kód.

V prípade oboch druhov výrobkov zákon ukladá povinnosť označovať ich kontrolnou známkou.[39] Podrobnosti o podobe kontrolnej známky ustanovil nový

39 § 51 zákona č. 530/2011 Z.z., o spotrebnej dani z alkoholických nápojov; § 9 zákona č. 106/2004 Z.z.,

podzákonný predpis Ministerstva financií SR (ďalej len „MF SR“).[40] S účinnosťou od roku 2015 kontrolné známky povinne musia obsahovať jedinečné číslo pozostávajúce aspoň z 12 alfanumerických znakov, vyjadrené zároveň aj vo forme dvojrozmerného kódu[41] – QR kódu, ktorý je strojovo čitateľný. Na základe týchto údajov je potom možné priradiť ku konkrétnemu výrobku konkrétne informácie (napr. že vo fľaši, na ktorej je kontrolná známka s jedinečným číslom „254687482326“, sa nachádza alkoholový výrobok s objemom 0,5 l a s obsahom 40% alkoholu).

Myšlienka a história vzniku samotnej aplikácie „Superkolky“ nie je z informácií na webovom sídle MF SR zrejmá. Informácie o pripravovaní aplikácie, ktorá by mala takúto funkcionalitu, sa postupne objavili v médiách v priebehu roku 2014.[42] Aplikácia bola publikovaná FS SR v marci 2015, a to bez predchádzajúcich oficiálnych správ, ktoré by prípravu takejto aplikácie avizovali.[43]

O tom, že aplikácia by mohla zasahovať do súkromia používateľov a zbierať ich osobné údaje, informovala spoločnosť Nethemba na sociálnych sieťach.[44] Nethemba zaoberajúca sa IT bezpečnosťou analyzovala aplikáciu a zistila, že zbiera mnohé osobné údaje (napr. hardvérové sériové číslo telefónu alebo GPS polohu). Informácia bola prevzatá ďalšími slovenskými médiami, ktoré o týchto zisteniach ďalej informovali. V jednom z článkov potvrdila zber údajov aj samotná FS SR a svoj postoj obhajovala predovšetkým poukazovaním na fakt, že potrebuje informácie o polohe falošného alkoholu (dôvod pre zber údajov o polohe zariadenia) alebo z dôvodu predchádzania zneužitia aplikácie (dôvod pre prístup k telefonickým hovorom, aby bolo možné vystopovať poskytovateľa falošných informácií).[45]Z informácií v médiách

o spotrebnej dani z tabakových výrobkov.

40 Vyhláška č. 256/2014 Z.z. Ministerstva financií SR z 18. septembra 2014 o označovaní balení kontrolných známok určených na označovanie spotrebiteľského balenia liehu a o oznamovaní a zverejňovaní údajov o týchto kontrolných známkach; Vyhláška č. 252/2014 Z.z. Ministerstva financií SR z 10. septembra 2014, ktorou sa ustanovujú náležitosti, vyhotovenie a cena kontrolnej známky určenej na označovanie spotrebiteľského balenia liehu.

41 Ibid. , § 1 ods. 1 písm. a) vyhlášky č. 256/2014; § 1 ods. 6 vyhlášky č. 252/2014.

42 KRAJANOVÁ, Daniela. Tlačiareň v Kremnici môže tlačiť superkolky. *SME.sk* [online]. Petit Press, a.s., vydané 09.10.2014 [cit. 30.11.2015].

43 *Superkolky [*online]. Archív noviniek, Finančná správa SR, 24.03.2015 [cit. 30.11.2015].

44 Status na sociálnej sieti Facebook, 14.04.2015 - https://www.facebook.com/nethemba/posts/1065162120180938

45 KERN, Miro. Štátna aplikácia na alkohol a cigarety sleduje ľudí, nechtiac môžete skončiť na súde. *Denník N* [online]. N press s.r.o., vydané 11.05.2015 [cit. 30.11.2015].

nie je zrejmé, ktorý konkrétny orgán finančnej správy údaje zbiera (k fungovaniu aplikácie sa ale vyjadrovalo Finančné riaditeľstvo SR). Zároveň nie je známy ani konkrétny rozsah zbieraných údajov či podmienky ich uchovávania.

2.3.2. Technické pozadie problému

Hlavnou funkciou aplikácie je možnosť skenovať QR kód na výrobku prostredníctvom fotoaparátu mobilného zariadenia alebo ručne zadať alfanumerický kód kontrolnej známky. Aplikácia obratom poskytne údaje o výrobku, ktoré má k dispozícii FS SR (napr. druh alkoholu, obsah alkoholu, gramáž výrobku a pod.). Ak sa informácie nezhodujú, aplikácia umožňuje kontaktovať priamo FS SR a oznámiť údaje o falošnom tovare.

Aplikácia „Superkolky“ je dostupná pre tri najpoužívanejšie mobilné platformy – Android, iOS a Windows Mobile.[46] Podľa údajov dostupných o aplikácii si len Android verziu nainštalovalo medzi 5 – 10-tisíc používateľov[47] (s prihliadnutím na skutočnosť, že spoločnosti Apple ani Microsoft informácie o počte stiahnutí nezverejňujú, je používateľská základňa aplikácie nepochybne podstatne väčšia).

Vo verzii nižšej ako 2.0. aplikácia žiadala povolenie prístupu k informáciám – 1. poloha, 2. fotky, médiá, súbory, 3. fotoaparát, 4. identifikátor zariadenia a informácie o hovoroch.[48] Potvrdzuje to aj správa spoločnosti Nethemba, podľa ktorej aplikácia pristupuje k údajom o hardvérovom sériovom čísle telefónu a GPS pozícii (funkcia „getLastKnownLocation“, ktorá umožňuje získať údaje o poslednej známej polohe zariadenia) a zároveň má aplikácia oprávnenie preposielať údaje FS SR. Takisto aplikácia vo verzii nižšej ako 2.0. umožňovala zadať svoje osobné údaje – meno a priezvisko, e-mail, telefónne číslo.

V októbri 2015 bola vydaná nová verzia aplikácie – 2.0. V tejto verzii aplikácia žiada oprávnenie na prístup k údajom v menšom rozsahu než pôvodne – poloha a prístup k fotoaparátu.[49] Do aplikácie už tiež nie je možné zadávať osobné údaje (meno,

46 Superkolky, 2015, op.cit.
47 *Superkolky* [online] Google Play, © 2015 Google [cit. 30.11.2015].
48 Snímka inštalačnej obrazovky pre staršiu verziu – dostupné tu: http://www.eisionline.org/images/Superkolky_1.png
49 Snímka inštalačnej obrazovky pre verziu 2.0 – dostupné tu:

e-mail a ani telefónne číslo).

2.3.3. Zhrnutie problému

Finančná správa publikovala aplikáciu, ktorou sa rozhodla zapojiť používateľov mobilných zariadení do boja s nelegálnymi tabakovými a alkoholickými výrobkami v snahe znížiť množstvo falošných výrobkov na trhu. Pochybnosti však vyvoláva spôsob, ktorým tak finančná správa činí. Podľa zverejnených informácií (ktoré boli potvrdené predstaviteľmi finančnej správy) aplikácia zbierala radu osobných údajov – o polohe zariadenia, o jeho hardvérových údajoch či o telefonických kontaktoch používateľa.

Súkromie a ochrana osobných údajov patria k ústavne chráneným hodnotám. Narušovať súkromie alebo zbierať osobné údaje nesmie bez zákonného dôvodu ani samotný štát. Ak chce finančná správa zbierať údaje o nič netušiacich používateľoch, je nutné kriticky sa opýtať, či tak koná v súlade so zákonom a ústavou.

2.4. Jednotný informačný systém v cestnej doprave a sledovanie žiakov autoškoly

V novembri 2015 bol prijatý zákon o jednotnom informačnom systéme v cestnej doprave. Projekt má zaviesť systém, „ktorý zabezpečí efektívne riadenie, evidenciu a kontrolu výkonu štátnej správy na úseku dopravy, konkrétne v oblasti správy autoškôl, v oblasti správy technických služieb a v oblasti riadenia odborných spôsobilostí v cestnej doprave“.[50] V rámci zavedeného systému budú podrobne monitorovaní aj účastníci kurzov autoškôl a lektori v priebehu výuky a praktických jázd. Hrozí, že taký extenzívny zber údajov, aký je navrhovaný v predkladanom zákone, by mohol byť v rozpore s ústavne garantovaným právom na súkromie a ochranou osobných údajov.

http://www.eisionline.org/images/Superkolky_2-0.png

50 *Národný projekt: Jednotný informačný systém v cestnej doprave - Elektronické služby v doprave* [online] Informatizácia.sk, Ministerstvo financií SR [cit. 30.11.2015].

2.4.1. Vznik a história problému

Jednotný informačný systém v cestnej doprave (ďalej len „JISCD“) je projekt, ktorý je súčasťou Operačného programu informatizácie spoločnosti (ďalej len „OPIS“).[51]Na čele projektu JISCD je Ministerstvo dopravy, výstavby a regionálneho rozvoja SR (ďalej len „MDVRR“).[52]

Z pohľadu legislatívneho rámca bol návrh právnej úpravy – zákon o jednotnom informačnom systéme cestnej dopravy – predložený do NR SR v auguste 2015. Súčasťou zákona je jednak formálne nový predpis, ktorý stanovuje zavedenie informačného systému, zároveň ale návrh zákona novelizuje iné právne predpisy z oblasti dopravy. Jedným z novelizovaných predpisov je aj zákon č. 93/2005 Z.z., o autoškolách, ktorý vo svojom novom znení ukladá povinnosť zbierať niektoré osobné údaje o lektoroch a žiakoch autoškoly.[53]

V rámci pripomienok k návrhu sa v medzirezortnom pripomienkovom konaní objavilo aj niekoľko pripomienok týkajúcich sa ochrany osobných údajov. K časti novelizačného predpisu, ktorý navrhuje povinnosť namontovať na výcvikové vozidlo autoškoly zariadenie schopné zaznamenať osobné údaje žiaka a lektora, vyjadril Úrad na ochranu osobných údajov obavy o nezákonné zbieranie údajov bez pevne stanoveného účelu.[54]

Napriek obavám o ochranu osobných údajov zostali vyššie uvedené pripomienky plne nezapracované. K problematickému bodu, ktorý zavádza sledovanie žiakov a učiteľov, vzniesla v priebehu legislatívneho procesu námietku aj skupina

51 OPIS je referenčným dokumentom, na základe ktorého je poskytovaná podpora zo štrukturálnych fondov EÚ. Cieľom OPISu je vybudovať modernú, občiansky orientovanú elektrizovanú verejnú správu, vrátane starších, hendikepovaných alebo sociálne znevýhodnených občanov – viac na *Čo je OPIS?* [online] Informatizácia.sk, Ministerstvo financií SR, aktualizované 30.04.2014 [cit. 30.11.2015].

52 *„Jednotný informačný systém v cestnej doprave – Elektronické služby v doprave (JISCD-ESD)“* [online] JEDNOTNÝ INFORMAČNÝ SYSTÉM V CESTNEJ DOPRAVE, © MDVaRR SR [cit. 30.11.2015]. Dostupné z: http://www.e-doprava.sk/index.html

53 *Návrh zákona* [online]. Vládny návrh zákona o jednotnom informačnom systéme v cestnej doprave a o zmene a doplnení niektorých zákonov, Parlamentná tlač 1721, Národná rada SR [cit. 30.11.2015]. Pozri čl.VIII zákona, najmä bod 16.

54 *Vzesené pripomienky v rámci medzirezortného pripomienkového konania - Návrh zákona o jednotnom informačnom systéme v cestnej doprave a o zmene a doplnení niektorých zákonov* [online] Úrad vlády SR [cit. 30.11.2015], s. 80.

poslancov, ktorá žiadala jeho vypustenie, avšak neúspešne.[55] Zákon bol v NR SR schválený a následne podpísaný Prezidentom SR. Jeho účinnosť sa predpokladá od 1. januára 2016.

Zmenený zákon o autoškolách zavedie niekoľko nových povinností, ktoré sa môžu javiť ako problematické z pohľadu ochrany osobných údajov. Novelizovaný zákon ukladá povinnosť vybaviť každé výcvikové vozidlo, trenažér či učebňu zariadeniami schopnými zaznamenať údaje o identite vyučujúceho aj žiaka autoškoly, o dĺžke trvaní jazdy, o trase jazdy a o čase strávenom v učebni a na trenažéri.[56]Zo znenia zákona nie je zrejmé to, ako dlho sa môžu tieto údaje uchovávať.[57]

2.4.2. Technické pozadie problému

Samotný zákon neobsahuje podrobnosti technického zabezpečenia systému. Pravdepodobne bude každému účastníkovi kurzu autoškoly pridelený identifikátor, ktorý bude následne používať pri vstupe do/výstupe z vozidla či učebne. Dôvodová správa k zákonu vysvetľuje: „Účastník kurzu pred začiatkom kurzu bude mať autoškolou pridelený identifikátor (napr. RFID čip; bude záležať od technologického vybavenia jednotlivých schválených identifikačných zariadení), prostredníctvom ktorého sa bude zaznamenávať absolvovanie teoretickej prípravy, ako aj praktického výcviku“.[58] Všetky údaje zo zariadení sa budú automaticky preposielať do informačného systému tak, ako to predpisuje zákon.[59]

V prípade zariadení vo výcvikových vozidlách pôjde o GPS (zo slovného spojenia „Global Positioning System“) zariadenia, ktoré budú výrobcom špecificky upravené pre potreby splnenia zákonných povinností.[60] Výrobca (alebo jeho zástupca)

55 *Pozmeňujúce a doplňujúce návrhy* [online]. Vládny návrh zákona o jednotnom informačnom systéme v cestnej doprave a o zmene a doplnení niektorých zákonov, Parlamentná tlač 1721, Národná rada SR [cit. 30.11.2015].

56 Pozri poznámku č. 45.

57 Pozri aj Vzesené pripomienky… (poznámka č. 56), kedy sa voči tomuto ohradil aj Úrad na ochranu osobných údajov, no vo finálne upustil od svojej pripomienky.

58 *Dôvodová správa* [online]. Vládny návrh zákona o jednotnom informačnom systéme v cestnej doprave a o zmene a doplnení niektorých zákonov, Parlamentná tlač 1721, Národná rada SR [cit. 30.11.2015], s. 43.

59 Návrh zákona, op. Cit. (pozri poznámku č. 45) - Pozri čl VIII zákona, bod 16 - „ktoré budú zo zariadenia automaticky zasielané do informačného systému“.

60 *Zverejnenie rozhrania pre prenos údajov z identifikačného zariadenia do JISCD* [online]. JEDNOTNÝ INFORMAČNÝ SYSTÉM V CESTNEJ DOPRAVE, © MDVaRR SR [cit. 30.11.2015]; takisto návrh

bude povinný pred uvedením zariadenia na trh písomne požiadať ministerstvo o schválenie spôsobilosti zariadenia. Zariadenie musí pred schválením prejsť testovaním kompatibility na komunikáciu s JISCD.

Zo zatiaľ zverejnených technických špecifikácií (v tzv. integračnej dohode[61]) vyplýva, že zariadenie bude preposielať údaje do JISCD prostredníctvom poskytovateľa služieb identifikačného zariadenia vozidla (alebo tiež „GPS provider“). Údaje najprv budú prenesené medzi GPS zariadením a GPS providerom. GPS provider údaje následne pošle do JISCD, pričom celé preposielanie bude prebiehať automaticky.

Integračná dohoda určuje množinu minimálnych údajov, ktoré bude GPS zariadenie preposielať GPS providerovi. Podľa dohody sa budú povinne odosielať 1. VIN číslo vozidla, 2. dátum a čas vzniku záznamu, 3. poloha (zemepisná šírka a dĺžka), 4. rýchlosť, 5. prejdená vzdialenosť, 6. pripojený príves, 7. identita inštruktora a žiaka.[62] GPS zariadenie musí byť povinne schopné ukladať minimálne 5000 záznamov o polohe a stave vozidla.[63] Okrem posielaných údajov musia byť k GPS zariadeniu povinne pripojené aj zariadenia na snímanie identifikačného prvku vodiča a inštruktora (napr. RFID kariet) a zariadenie na snímanie prítomnosti prívesu.[64]

Priamo do JISCD zasiela údaje samotný poskytovateľ služieb identifikačného zariadenia vozidla. Predpokladá sa posielanie údajov v dvoch režimoch – on-line s minimálnym oneskorením a off-line, v ktorom sa posielajú už ďalej spracované a agregované údaje (napr. údaje o polohe v prípade off-line posielania už budú „vyhladené“ a zohľadnia nepresnosti vzniknuté počas posielania údajov v priebehu jazdy).[65]

2.4.3. Zhrnutie problému

V roku 2016 chce štát spustiť nový informačný systém, ktorý

zákona v čl. VIII, bod 16, § 5a.

61 *Integračná dohoda medzi JISCD a tretími stranami* [online]. JEDNOTNÝ INFORMAČNÝ SYSTÉM V CESTNEJ DOPRAVE, © MDVaRR SR [cit. 30.11.2015].

62 Ibid., s. 4; Technická špecifikácia obsahuje aj ďalšie nepovinné údaje a rozšírenú množinu údajov, ktoré môžu byť preposielané GPS providerovi.

63 Ibid., s. 5.

64 Ibid., s. 6.

65 Ibid., s. 7 a nasl.

má zmodernizovať rezort dopravy. Súčasťou systému má byť aj novelizácia zákona o autoškolách a niekoľko noviniek vo vyučovacom procese autoškôl. Zákonodarca pridal autoškolám novú povinnosť – musia mať vo výcvikových vozidlách, trenažéroch i vyučovacích triedach pevne nainštalované zariadenia na zaznamenávanie osobných údajov. Účastníci kurzov i lektori budú povinne vybavení identifikačnými prvkami v podobe RFID čipov alebo porovnateľnej technológie, ktorými sa budú musieť povinne preukázať pri vstupe alebo opustení automobilu či vyučovacích priestorov. Okrem informáciách o tom, kto sa kedy a kde zúčastňuje vyučovania a kedy opúšťa vyučovacie priestory, budú zbierané aj podrobné údaje o jazde, vrátane identifikačného čísla vozidla, prejdenej vzdialenosti a informácií o polohe vozidla a prejdenej trase. Všetky informácie budú automaticky preposielané do informačného systému MDRVV.

Zákonodarca obhajuje zbieranie osobných údajov a sledovanie účastníkov kurzu zvyšovaním transparentnosti vyučovacieho procesu v autoškolách. Na mieste je však otázka, či sú podobné opatrenia potrebné pre naplnenie cieľa sledovaného zákonom a či neexistujú prostriedky, ktoré by do súkromia dotknutých osôb zasahovali s menšou intenzitou.

3. Analýza prípadových štúdií

3.1. Povinnosť elektronickej komunikácie so štátom

„Štátna moc pochádza od občanov, (..)“

Čl. 2 ods. 1 Ústavy SR

Elektronizácia výkonu verejnej moci je želateľný jav. Občanom umožňuje častejší, lacnejší a rýchlejší prístup k orgánom verejnej moci, zatiaľ čo štátu umožňuje efektívnejšie, transparentnejšie a kontrolovateľnejšie vykonávať svoje vlastné úlohy.[66] Aby to tak bolo, musí však fungovať elektronizácia. Predovšetkým jej implementácia nesmie byť vedená osobnými záujmami v oblasti tendrovaných technických riešení, ale musí sledovať v prvom rade záujem svojho zákazníka – občana. Nie je to totiž štát kto „dáva“ technické možnosti občanom, ale sú to občania, ktorí poverujú štát ich vytvorením. Elektronizácia, ktorá neprihliada na potreby a možnosti svojho zákazníka – občana – nemá zmysel.

Elektronizácia verejnej moci prostredníctvom technologického dizajnu vytvára nový druh noriem. Tieto normy nie sú nevyhnutne súčasťou právnych predpisov, ale sú priamym dôsledkom nastavenia technických riešení. Ak štátny orgán svojím technickým riešením napríklad obmedzí možnosti občanov splniť zákonnú povinnosť len na určitý typ softvéru, súbor týchto technických bariér je taktiež súčasťou normotvorby štátu. Na rozdiel od právnej normy, občan nemôže túto technickú normu ani porušiť. Ak totiž jeho softvér nefunguje na platforme štátu, nič s tým nenarobí. Štát preto netvorí normy len prostredníctvom zákonodarných orgánov alebo exekutívy, ale aj svojím jednoduchým správaním sa pri elektronizácii. Zdalo by sa, že táto situácia nie je unikátna, keďže aj bez elektronizácie štát faktickou dostupnosťou svojich služieb

66 Pozri napr. *E-government benefits study* [online]. Canberra: NOIE, 2003. ISBN 1740820258.

obmedzuje prístup občanov k štátu (napr. otváracie hodiny, množstvo pobočiek a pod.). Ani tieto de facto prekážky z fyzického sveta by však neostali úplne bez povšimnutia ústavného práva. Ak by napríklad štátny orgán umožnil plnenie určitej zákonnej povinnosti len osobne, pričom by poskytol len jednu pobočku na plnenie (napr. podanie daňového priznania), a to len jeden deň v týždni, je zrejmé, že takéto správanie štátu by bolo neprípustné. To isté bude platiť aj v on-line prostredí.

Ak štát ukladá povinnosti, nezdá sa preto nijako sporné, že je súčasne jeho aktívnou úlohou vytvoriť podmienky na to, aby ich adresát mohol splniť. Štátna moc, ktorá koná v dobrej viere totiž logicky má záujem na tom, aby uložené zákonné povinnosti boli splnené. Len štátna moc, ktorá koná v zlej viere sa snaží splnenie uložených povinností občanom znemožniť, aby tak mohla prípadne siahnuť k represii. Samozrejme, v skutočnosti existuje mnoho modalít ako sa štát môže správať, pričom ústavnoprávne neprípustný výsledok nemusí byť vždy vedený len zlými úmyslami. Cieľom tohto textu je poodhaliť odlišné situácie elektronizácie a poukázať aj na odlišné kvality a rozsah povinností štátu v nich, a to z pohľadu ústavného práva.

3.1.1. Forma technických obmedzení

Technické bariéry spôsobené elektronizáciou môžu mať *explicitný* alebo *implicitný* charakter. Prípadová štúdia k daňovej výkazovej povinnosti ukazuje, že štát za istých okolností dokonca vyžaduje, aby sa občan „zmluvne zaviazal“ k rešpektovaniu určitých technických obmedzení. V iných prípadoch, ako ukazuje štúdia o prevode poľnohospodárskej pôdy, sú tieto obmedzenia len „nepísaným“ dôsledkom implementácie určitého technického riešenia (napr. vyžadovanie elektronického občianskeho preukazu s čipom). V oboch prípadoch je však podstata problému rovnaká. Štát nad rozsah mandátu zákona, sčasti aj nevyhnutne, obmedzuje možnosť správania sa adresáta jeho služieb. Pokiaľ základné obmedzenia plynúce z týchto technických opatrení nemusia byť obsiahnuté v normatívnom právnom akte (právnom predpise), Ústavný súd SR ich môže preskúmavať len z pozície individuálnych aktov aplikácie práva.[67]

67 Čl. 127 Ústavy SR.

Odlíšenie o aký akt ide však nemusí byť jednoduché. Ak si zoberieme príklad Finančného riaditeľstva SR, ktoré v našej prípadovej štúdii vyžadovalo podpísanie osobitnej dohody pred používaním jedného z technických riešení, naskytá sa otázka, či táto „dohoda“ je normatívny alebo individuálny právny akt. Ako bolo uvedené, ustanovenie § 80 ods. 9 ZoDPH[68] dáva orgánu verejnej moci právomoc na formulovanie dohody, ktorá má verejnoprávny charakter a až na základe ktorej bude môcť povinný podnikateľ následne využívať tento spôsob splnenia zákonnej povinnosti. Inými slovami, právna norma dáva právomoc orgánu verejnej moci na vydanie istého právneho aktu, ktorým má dôjsť k bližšej špecifikácii náležitostí, spôsobu overovania podania a preukazovania doručenia. Obsah tohto právneho aktu, t.j. práva a povinnosti v ňom zakotvené, nie je možné ovplyvniť zo strany žalovaného formou kontraktačnej slobody. Ide teda o prejav mocenských oprávnení štátu. Tu sa totiž takáto „dohoda“ odlišuje od súkromnoprávnych dohôd, ktorými štát zabezpečuje riadnu správu vecí verejných (napr. nákup počítačov). V prípade § 80 ods. 9 ZoDPH platí, že ak povinný subjekt neakceptuje obsah dohody, pripraví sa zároveň o spôsob splnenia zákonnej povinnosti bez zaručeného elektronického podpisu.

Je otázne, či štát vôbec môže uzatvárať takéto dohody verejnoprávneho charakteru, ktoré sú prejavom jeho mocenských oprávnení v danej forme. Z ústavnoprávneho hľadiska treba pripomenúť *štyri princípy*:

- (1) Štátne orgány môžu konať iba na základe ústavy, v jej medziach a v rozsahu a spôsobom, ktorý ustanoví zákon (čl. 2 ods. 1 Ústavy);(
- 2) Každý môže konať, čo nie je zákonom zakázané, a nikoho nemožno nútiť, aby konal niečo, čo zákon neukladá (čl. 2 ods. 1 Ústavy);
- (3) Povinnosti možno ukladať a) zákonom alebo na základe zákona, v jeho medziach a pri zachovaní základných práv a slobôd, b) medzinárodnou zmluvou podľa čl. 7 ods. 4, ktorá priamo zakladá práva a povinnosti fyzických osôb alebo právnických osôb, alebo c) nariadením vlády podľa čl. 120 ods. 2

68 Znenie: „Súhrnný výkaz podaný elektronickými prostriedkami nemusí byť podpísaný zaručeným elektronickým podpisom, ak osoba, ktorá podáva súhrnný výkaz, má s daňovým úradom uzavretú písomnú dohodu, ktorá obsahuje najmä náležitosti elektronického doručovania, spôsob overovania podania urobeného elektronickými prostriedkami a spôsob preukazovania doručenia ..“.

(čl. 13 ods. 1 Ústavy);

- (4) Medze základných práv a slobôd možno upraviť za podmienok ustanovených touto ústavou len zákonom (čl. 13 ods. 2 Ústavy);

Už z kombinácie prvého a druhého princípu podľa nášho názoru vyplýva, že štát nemôže vyžadovať, aby občania pre realizáciu svojho práva alebo splnenie svojej povinnosti najprv museli vyhovieť určitej podmienke, ktorá nemá podklad v zákone, t.j. nie je uložená zákonom alebo na základe zákona. V minulosti aj Najvyšší súd SR napríklad odmietol, aby daňová správa zakazovala vydávanie väčšieho počtu dokladov z elektronickej registračnej pokladnice v situácii, keď to žiadny predpis výslovne nezakazoval[69]. Je teda zrejmé, že prax orgánu verejnej moci musí byť striktne orientovaná na zákonný podklad, ktorý umožňuje jeho činnosť. Vytváranie dodatočných „úradníckych“ podmienok bez opory v zákone, hoc aj dobre mienených, môže ľahko naraziť na problém v rámci ústavnoprávneho prieskumu.

Ak sa vrátime k príkladu „dohody“, ktorú naoktrojovalo Finančné riaditeľstvo SR v prípade daňových výkazov, je zrejmé, že prax nie je bezproblémová. V prvom rade, ak zákon chce umožniť orgánu verejnej moci, aby mohol vydať právny akt, ktorý sa vyznačuje až takou mierou všeobecnosti z hľadiska osobnej, vecnej a časovej pôsobnosti[70], je potrebné aby siahol k jednému z uznávaných prameňov normatívnych právnych aktov[71]. Správne preto podľa nášho názoru malo príslušné ustanovenie znieť ako splnomocňovacie na vydanie takéhoto predpisu, na čo mu však chýba presnosť.[72]

69 Rozhodnutie Najvyššieho súdu, sp. zn. 5Sžf/19/2009: „S prihliadnutím na čl. 59 Ústavy SR a zásady správneho trestania (najmä relevantné odporúčanie Rady Európy) pre Najvyšší súd vyplýva záver, že verejný záujem na riadnom výbere daní a poplatkov vrátane daňových sankcií je opodstatnený len vtedy, ak má legálny základ. Inak je nutné každý úkon správy daní a poplatkov vyhodnotiť ako nezákonný zásah do oprávnenia jednotlivcov konať všetko, čo im zákon nezakazuje. Za danej situácie sa preto Najvyšší súd stotožnil s argumentáciou žalobcu, že mu žiadny právny predpis výslovne nezakazuje vydávať doklady z elektronickej registračnej pokladnice vo vyššom počte.“

70 “Pre individuálny právny akt je naopak charakteristická individualizácia a konkretizácia subjektov a predmetu, na ktoré sa vzťahuje.” (PRUSÁK, Jozef. *Teória práva*. Vydavateľské oddelenie PFUK, Bratislava: 2001, s. 190).

71 Pozri zákon č. 1/1993 Z.z. o Zbierke zákonov SR (napr. vo forme vyhlášok ministerstiev a ostatných ústredných orgánov štátnej správy SR, resp. iných orgánov štátnej správy).

72 PRUSÁK, 2001, op.cit. uvádza: “Podľa legislatívnych pravidiel musí byť splnomocnenie na vydanie vykonávacieho právneho predpisu vždy určité. Musí z neho jasne vyplývať, ktorý orgán je splnomocnený, aké otázky a v akom rozsahu môže vo vykonávacom právnom predpise upraviť. Nie je možné akceptovať neurčité splnomocnenie na úpravu „podrobností." V súlade s legislatívnymi pravidlami je celkom neprípustné presúvať do neskorších vykonávacích právnych predpisov úpravu otázok, ktoré sa nepodarilo vyriešiť alebo dohodnúť pri príprave zákona. Zákony musia totiž upravovať

Pritom je však nutné zároveň pamätať na to, že „povinnosti“ môže verejná moc ukladať len vo vybraných prameňoch práva (čl. 13 ods. 1), vrátane na základe zákona, pričom tieto pramene sú ešte viac obmedzené ak je dôsledkom primárne obmedzenie základných práv a slobôd (čl. 13 ods. 2)[73]. Ako judikoval už aj Ústavný súd SR, „pokiaľ ide o realizáciu ústavného príkazu povinnosti ukladať zákonom alebo na základe zákona, v jeho medziach a pri zachovaní základných práv a slobôd vyplývajúceho z čl. 13 ods. 1 písm. a) ústavy, *nemôže byť vo všeobecne záväznom nariadení uložená nová povinnosť, ktorá neexistuje v zákone*. Nerešpektovanie uvedeného príkazu ústavy by znamenalo negáciu zvrchovanosti zákona, a tým popretie samotného princípu právneho štátu“[74]. Podzákonný predpis by preto napríklad nemohol obsahovať sám o sebe povinnosť elektronickej formy. Taktiež nie je možné, aby takýto podzákonný predpis, vydaný hoci aj na základe splnomocňovacieho ustanovenia, rozširoval oblasť právnej regulácie nad rámec zákona, vypĺňal medzery v zákone, menil alebo korigoval ustanovenia zákona.[75]

Navyše, ako zdôrazňuje aj Ústavný súd SR, „zákonodarca je (..) povinný formulovať ním vydávané právne predpisy s takou vysokou mierou určitosti, aká je v danom prípade možná so zreteľom na účel a osobité črty právnej úpravy, ako aj ústavné limity“.[76] Pritom je požiadavkou právneho štátu, „aby zákony v právnom štáte boli pochopené dostatočne a aby *umožňovali ich adresátom urobiť si aspoň predstavu o svojej právnej situácii*“.[77] Právna istota, a to „predovšetkým právna istota ex ante (vopred) vychádza z predvídateľnosti rozhodnutí orgánov verejnej moci, pričom pre občanov, iné fyzické osoby a právnické osoby predstavuje princíp právnej istoty predovšetkým ich *orientačnú istotu*, od ktorej sa odvíja aj ich dôvera v právny poriadok. Občianska sloboda ako imanentný znak demokratického a právneho štátu vyžaduje spoľahlivosť právneho poriadku, *pretože sloboda znamená predovšetkým*

všetky základné vzťahy v oblasti, ktorá je predmetom právnej úpravy.”

73 “Orgány výkonnej moci nesmú svojimi všeobecne záväznými právnymi predpismi obmedziť základné práva a slobody určením povinností, ani akokoľvek inak.“ (Nález Ústavného súdu SR, sp. zn. II. ÚS 8/97, s. 81).

74 Nález Ústavného súdu SR, sp. zn. III. ÚS 100/02.

75 PRUSÁK, 2001, op. cit.; V prípade daňových výkazov, orgán verejnej moci sa však rozhodol, že § 80 ods. 9 ZoDPH interpretuje čo najširšie, pričom povinným subjektom uložil aj také povinnosti, ktoré zákon nepredpokladá, a ktoré odporujú právnemu poriadku na iných miestach.

76 Nález Ústavného súdu SR, sp. zn.PL. ÚS 29/05-161.

77 Nález Ústavného súdu SR, sp.zn. PL. ÚS 19/98.

možnosť usporiadať si život podľa vlastných predstáv“.[78]

3.1.2. Elektronická možnosť a povinnosť

Elektronizácia verejnej správy dopadá na občanov rôznym spôsobom podľa toho, ako sa k nej stavia právny rámec, t.j. povinnosť alebo právo občana, na ktoré je naviazaný. Je rozdiel, ak elektronická komunikácia predstavuje len (1) *ďalšiu možnosť* splnenia zákonných povinností či realizovania práva, alebo (2) je *určená ako výlučný spôsob* splnenia zákonných povinností (prípad daňových výkazov), resp. realizovania práva (prípad pozemky). Je len logické, že štát, ktorý vnucuje občanom elektronickú formu komunikácie ako jedinú možnú, dlží občanom oveľa viac čo do vytvorenia podmienok na splnenie týchto „elektronických zákonných povinností“. Ak je totiž popri elektronickej forme možná aj iná forma komunikácie, resp. naplnenia litery zákona, vylučujúci efekt elektronizácie je nižší, pretože adresát má stále k dispozícii iné alternatívy (napr. ísť na úrad, plniť poštou a pod.).

Ak by ústavné právo nekládlo žiadne nároky na vytvorenie podmienok splnenia povinností alebo realizovania práv, občania by boli vystavení jeho svojvôli neustále. Jedna vláda by sa tak mohla rozhodnúť, že občania, len aby mohli rešpektovať zákon, resp. uplatniť svoje práva, si musia povinne zaobstarať produkty od spoločnosti A, zatiaľ čo druhá o pár mesiacov zase produkty od spoločnosti B. Občan by tak bol zmietaný svojvôľou štátu od dverí jednej firmy k druhej. Pre ústavné právo musí byť takáto situácia neakceptovateľná.

Spôsob, akým ústavné právo dokáže aspoň čiastočne *moderovať* správanie štátu spočíva v tom, že orgány verejnej moci v kontexte elektronizácie musí zaťažovať *pozitívnou obligáciou vytvoriť podmienky* pre splnenie zákonných povinností, resp. realizovanie práv. Koncept pozitívnej obligácie sa v ústavnom práve objavuje v kontexte mnohých práv[79]. Štát má tak povinnosť vytvoriť *právne a faktické podmienky* jednotlivcom, aby mohli uplatňovať svoje právo na súkromie[80], novinárom, aby mohli

78 Nález Ústavného súdu SR, sp.zn. PL. ÚS 29/05.

79 V kontexte Európskeho Dohovoru o ochrane ľudských práv – pozri AKANDJI-KOMBE, Jean-François. *Positive obligations under the European Convention on Human Rights: A guide to the implementation of the European Convention on Human Rights* [online]. Human rights handbooks, No.7, Council of Europe, 1st printing, 2007 [cit. 30.11.2015].

80 Nálezy Ústavného súdu SR, sp. zn. II. ÚS 59/97 a I. ÚS 4/02

uplatňovať svoju slobodu prejavu aj v prípade ohrozenia inými jednotlivcami[81] alebo majiteľom nehnuteľností, aby mohli uplatňovať svoje vlastnícke právo.[82] Ústavnoprávny základ tejto pozitívnej obligácie bude záležať od toho, v kontexte ktorého práva sa elektronizácia práva alebo povinnosti objavuje.

V analyzovanom prípade EURA, v ktorom podnikateľ musel na splnenie daňovej povinnosti použiť jeden konkrétny operačný systém a internetový prehliadač, je dotknutým základným právom jeho právo podnikať (čl. 35 ods. 1 Ústavy). V prípade poľnohospodárskych pozemkov, kde majitelia poľnohospodárskej pôdy musia v rámci predaja realizovať čas transakcie elektronicky a dokonca za použitia osobitného autentifikátora, je zase týmto právom ich právo vlastniť majetok (čl. 20 Ústavy). Samozrejme, elektronizácia sa môže dotknúť v podstate ktoréhokoľvek iného ľubovoľného práva. Predstaviť si možno rôzne obmedzenia slobody prejavu (čl. 26 Ústavy), práva na prístup k informáciám (čl. 26 ods. 5 Ústavy), slobody zhromažďovania (čl. 28 Ústavy), petičného práva (čl. 27 Ústavy) alebo slobody vierovyznania (čl. 24) a pod.

Ak by napríklad štát predpísal elektronickú formu alebo jedinú štátnu platformu ako výlučný spôsob realizovania petičného práva, išlo by o jeho zásadné obmedzenie, ktoré by následne muselo byť posudzované podľa princípov uvedených nižšie. Rovnako by to platilo ak by sa štát rozhodol pre povinnú elektronickú komunikáciu v kontexte ohlasovania zhromaždení alebo pri podávaní žiadosti o informácie voči štátu.

Ako už vyššie uvedené príklady naznačujú, aj samotné kreovanie čisto *elektronických zákonných povinností*, t.j. situácie, v ktorej povinnosť nemožno splniť

81 Özgür Gündem v Turecko (č. 23144/93, §§ 42-43), Dink v. Turecko (č. 2668/07, § 137) - “States are obliged to create, while establishing an effective system of protection for authors and journalists, *a favorable environment for the participation in public debates of all concerned* allowing them to express their opinions without fear and ideas, even if they are contrary to those held by official authorities or by a significant section of public opinion, or even have irritating or offensive to the past“.

82 Broniowski v Poľsko (č. 31443/96, § 184) - “The rule of law underlying the Convention and the principle of lawfulness in Article 1 of Protocol No. 1 require States not only to respect and apply, in a foreseeable and consistent manner, the laws they have enacted, but also, as a corollary of this duty, *to ensure the legal and practical conditions for their implementation* (..) it was incumbent on the Polish authorities to remove the existing incompatibility between the letter of the law and the State-operated practice which hindered the effective exercise of the applicant's right of property.”)

alebo právo riadne realizovať inak ako elektronicky, môže predstavovať problém. Ústavnoprávna prípustnosť plnej elektronizácie takéhoto druhu podľa nášho názoru závisí od:

- (1) okruhu osôb, ktoré budú dotknuté opatrením,
- (2) stupňa informačnej vyspelosti skupín (1) a
- (3) stupňa náročnosti uplatňovaného riešenia.

Uveďme si v tomto smere príklad. Ak štát zavedie povinnosť podávať všetky petície iba elektronickou formou, dopad tohto riešenia je veľmi široký. V podstate sa bude dotýkať všetkých osôb, ktorým prislúcha petičné právo. Okruh dotknutých osôb (1) bude zahŕňať ako osoby maloleté, tak aj seniorov. Pre porovnanie v prípade daňovej výkazovej povinnosti je okruh dotknutých osôb podstatne užší – profesionálni podnikatelia, a to aj len tí, ktorí sú platcami DPH. Je zrejmé, že stupeň informačnej vyspelosti (2) profesionálov a seniorov je neporovnateľný. Preto, zatiaľ čo výlučná elektronická povinnosť má v zásade malý vylučujúci účinok pri profesionáloch (napr. drobní postarší podnikatelia bez počítača) – a to aj preto, že mnoho podnikateľov si necháva viesť účtovníctvo tretími osobami – jej vylučujúci účinok pri penzistoch, ktorí chcú uplatniť svoje petičné právo je zásadný. Napokon, ústavnoprávna prípustnosť musí zohľadniť aj stupeň náročnosti uplatňovaného riešenia (3). Nie je totiž jedno či sa výlučnou elektronickou komunikáciou skrýva povinnosť použiť email, alebo zaobstarať si elektronický podpis, konkrétny operačný systém ako aj nainštalovať osobitný softvér. Aj voči profesionálom môže totiž riešenie, ktoré sa zdá prípustné z hľadiska bodov (1) a (2), naraziť na neodôvodnene vysoké nároky v bode (3). Hoci totiž môže byť proporcionálnym obmedzením slobody podnikať to, aby si podnikateľ zaobstaral elektronické prostriedky komunikácie, to isté nemusí platiť ak mu orgán verejnej moci navyše „nabalí“ ďalšie obmedzenia.

V rozsahu stupňa náročnosti uplatňovaného riešenia musí štát sledovať zásadu minimalizácie zásahu do základných práv, ktorých sa dotýka. Podľa tejto zásady si štát, aj vtedy ak mu je dovolené obmedziť práva (napr. elektronizáciou), musí vybrať taký spôsob obmedzenia základných práv, ktorý je voči nim najviac šetrný. Ako uvádza sám

Ústavný súd SR, „právna norma totiž v podmienkach materiálneho právneho štátu nemôže obmedzovať základné právo alebo slobodu viac, než je nevyhnutné na dosiahnutie cieľa ňou sledovaného, resp. právna norma by mala dosahovať sledovaný cieľ najmenej drastickým spôsobom“.[83]Ak teda štát zavádza elektronickú povinnosť v kontexte, ktorý z bezpečnostného alebo autentifikačného hľadiska nevyžaduje nevyhnutne požadovanie elektronického podpisu, pretože existujú inkluzívnejšie technologické alternatívy, alebo pretože len málo adresátov pravidla má samotný elektronický podpis, je povinnosťou štátu vybrať čo najviac *inkluzívnejšie technologické riešenie*.

To, samozrejme, neznamená, že štát absolútne nemôže vyžadovať elektronický podpis, ak je jeho difúzia medzi občanmi nízka. Naopak, možné to je, no voľba technicky obtiažnejšieho riešenia zaťažuje potom štát širšou *pozitívnou obligáciou* vytvoriť podmienky, a teda postarať sa o to, aby technické riešenie bolo dostupné. Štát tak môže napríklad zriadiť kontaktné miesta, na ktorých zraniteľné skupiny obyvateľstva, ktoré sú taktiež dotknuté riešením, môžu za asistencie štátneho orgánu realizovať svoje práva. Prípustnosť elektronizácie v kontexte navrhnutých kritérií (1) až (3) preto môže byť vyvažovaná zo strany samotného štátu tým, že aktívnejšie koná v rozsahu svojej pozitívnej obligácie vytvoriť faktické a právne podmienky pre adresátov svojich noriem.

Treba pamätať na to, že „nevyhnutnosť“ v judikatúre Ústavného súdu SR, „znamená, že neexistuje iný stav, ktorý štát bez veľkej námahy môže rovnako vytvoriť, ktorý občana zaťažuje menej a ktorý súvisí so stavom, v ktorom treba sledovaný účel pokladať za uskutočnený. Inými slovami, cieľ nesmie byť dosiahnuteľný rovnako účinným, ale menej zaťažujúcim prostriedkom.“ Táto zásada by sa mala priamo premietať do voľby technického riešenia na strane orgánu verejnej moci. Cieľom by malo byť čo najinkluzívnejšie technické riešenie. To možno dosiahnuť predovšetkým tým, že štát bude sledovať zásadu *technologickej neutrality*, t.j. implementovanie technických riešení, ktoré umožňujú prístup občanov všeobecne bez ohľadu na to, od akého výrobcu aké konkrétne softvérové alebo hardvérové produkty používajú.

83 Nález Ústavného súdu SR, sp. zn. PL. US 23/06.

Väčšinou je najistejším spôsobom ako dosiahnuť technologickú neutralitu a zároveň širokú inkluzívnosť technologického riešenia používanie *otvorených štandardov*.[84] Sčasti to však závisí od definície samotného otvoreného štandardu, ako aj od procesu, akým došlo k jeho vytvoreniu. Rešpektovanie otvorených štandardov preto nemusí vždy automaticky viesť aj k technologickej inkluzívnosti. Samozrejme, v prvom rade preto, že už samotná elektronizácia niekedy nemusí byť inkluzívna dostatočne, ale aj z dôvodu obmedzenej implementácie existujúcich štandardov v reálnych produktoch dostupných jednotlivcom. Navyše, ako samotná elektronizácia, tak aj uplatňované technické riešenie musia byť v rozsahu obmedzovania základných práv a slobôd súladné so zákazom diskriminácie (čl. 12 ods. 3 Ústavy). A preto by malo vždy byť pamätané aj na inkluzívnosť vo vzťahu k znevýhodneným skupinám obyvateľstva, akými sú napríklad zrakovo alebo sluchovo postihnutí spoluobčania, ale aj sociálne znevýhodnení.

3.1.3. Formy realizácie pozitívnej obligácie štátu

V predchádzajúcej časti sme ustálili to, že štát má pozitívnu povinnosť vytvoriť právne a faktické podmienky na splnenie jeho „elektronických požiadaviek“. Táto pozitívna obligácia štátu sa pritom prejavuje dvojako:

- (1) povinnosťou uplatňovať a interpretovať existujúce právne mechanizmy čo najviac na podporu tohto cieľa,
- (2) povinnosťou zaviesť nové mechanizmy ak tie existujúce (1) nie sú

84 Metodický pokyn (MF/014235/2008-132) definuje pojem otvorený štandard nasledovne: „Otvorený štandard je taká technická špecifikácia, ktorá je (1) prijatá a udržovaná neziskovou organizáciou alebo konzorciom, (2) jej ďalší vývoj a modifikácie vychádzajú z otvoreného rozhodovacieho procesu, prístupného všetkým záujemcom, na základe zhody alebo rozhodovania väčšinovým hlasovaním, (3) je zverejnená a príslušné dokumenty sú prístupné buď volne, alebo za nominálny poplatok a (4) prípadné súvisiace duševné vlastníctvo – patenty – sú neodvolateľne bezplatne sprístupnené pre všetkých rovnako." Táto definícia pochádza z European Interoperability Framework (EIF 1.0), prijatého Európskou úniou v roku 2004. Okrem neho sa podobný princíp objavuje aj v Koncepcii využívania softvérových produktov vo verejnej správe schválená 15. júla 2009, č. uznesenia vlády 523/2009, ktorá uvádza: „Otvorené štandardy sú špecifikácie softvérových rozhraní, protokolov, dát, formátov súborov a pod., ktoré sú detailne popísané a publikované bez obmedzení, ktoré by mohli limitovať ich implementáciu alebo umožňovať skrytú konkurenčnú výhodu. (6 Príloha - 6.1 Základné pojmy používané v dokumente), alebo tiež: „Súčasná politika EÚ preferuje softvér založený na otvorených štandardoch, ktorý je plne interoperabilný s ktorýmikoľvek aplikáciami využívajúcimi tie isté štandardy. Konštatuje, že používanie proprietárnych štandardov vedie k zvýšenej závislosti od vybraných dodávateľov softvéru a potláča konkurenciu na trhu.“ (4.2.1.4 Interoperabilita).

dostatočné na riešenie vzniknutej situácie.

Prípad (1) v podstate znamená, že existujúce právne predpisy (napr. o štandardoch, elektronickom podpise, verejnom obstarávaní, o ochrane hospodárskej súťaže a pod.) musia orgány verejnej moci pokiaľ možno čo najviac *vykladať* v súlade s cieľom umožniť čo najširšiu participáciu dotknutého obyvateľstva. Vo svojej podstate ide „len“ o bežnú povinnosť ústavnoprávneho výkladu jednoduchého práva.[85] V ďalšej časti preto poukáže na už existujúce právne predpisy, ktoré k čo najširšej inklúzii adresátov takýchto noriem prispievajú už dnes. Jej súčasťou by mala byť aj ústavnoprávna povinnosť aktívne *uplatňovať* tieto inštrumenty (napr. vymáhať predpisy a pod.). Táto povinnosť znamená ale aj to, že ak orgán verejnej moci má na základe zákonného podkladu na výber medzi viac a menej inkluzívnym technickým riešením, je jeho ústavnoprávnou povinnosťou obmedziť dopad na základné práva a slobody a zvoliť technologicky viac inkluzívne riešenie (viď anti-príklad z prípadu poľnohospodárska pôda).

Do situácie (2) sa štát dostáva vtedy, ak jeho existujúce riešenia nie sú dostatočné. V takom prípade musí prijať dodatočné opatrenia, ako napríklad zriadenie obslužných miest pre zraniteľné časti obyvateľstva (napr. seniorov, zrakovo postihnutých a pod.). Táto obligácia zahŕňa aj povinnosť vykonať už samotné verejné obstarávanie tak aby sa dosiahlo čo najviac technologicky inkluzívne riešenie. Nie je možné aby v rámci niekoľko miliónovej zákazky na elektronizáciu určitého riešenia, nedokázal štát zároveň aj obstarať prípadne nevyhnutné multiplatformové certifikáty za niekoľko tisíc eur.

3.1.3.1. Predpisy o štandardoch

Podľa zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy (ďalej aj „ZoISVS“) a Výnosu o štandardoch pre ISVS č. 55/2014 Z. z. (ďalej aj „Výnos“) majú orgány verejnej moci povinnosť zabezpečiť, aby bol nimi spravovaný informačný systém verejnej správy v súlade s určitými vopred predpísanými štandardmi informačných systémov verejnej správy. Cieľom týchto štandardov je okrem iného čo najširšia inkluzívnosť technických riešení, ktoré používa štát.

85 Napríklad rozhodnutia PL. ÚS 21/2008; III. ÚS 52/2009; III. ÚS 36/2009; II. ÚS 161/2009.

Podľa § 3 ZoISVS, za „vytváranie, správu a rozvoj informačného systému verejnej správy zodpovedá povinná osoba, ktorá je správcom, zabezpečujúca výkon verejnej správy na určenom úseku verejnej správy podľa osobitného predpisu“. Povinná osoba má za úlohu „zabezpečovať, aby bol informačný systém verejnej správy v súlade so štandardmi informačných systémov verejnej správy“ (§ 3 ods. 4 písm. i) ZoISVS). Zákon následne definuje štandardy v § 6 ods. 1 ZoISVS nasledovne:

> „Štandardom je súbor pravidiel spojených s vytváraním, rozvojom a využívaním informačných systémov verejnej správy, ktorý obsahuje charakteristiky, metódy, postupy a podmienky, najmä pokiaľ ide o bezpečnosť a integrovateľnosť informačných systémov verejnej správy. *Štandardy musia byť otvorené a technologicky neutrálne.*“

Ustanovenie § 1 Výnosu následne špecifikuje, že výnosom sa ustanovujú štandardy pre nasledovné informačné systémy verejnej správy:

> „a) technické štandardy, vzťahujúce sa na technické prostriedky, sieťovú infraštruktúru a programové prostriedky, a to:
> 1. štandardy pre prepojenie,
> *2. štandardy pre prístup k elektronickým službám,*
> *3. štandardy pre webové služby,*
> 4. štandardy pre integráciu dát,
> *b) štandardy prístupnosti a funkčnosti webových stránok, vzťahujúce sa na aplikačné programové vybavenie podľa zákona,*
> …
> *g) štandardy elektronických služieb verejnej správy, vzťahujúce sa na údaje, registre, číselníky a aplikačné programové vybavenie podľa zákona.*“

Z týchto ustanovení teda vyplýva, že požiadavky na používanie „otvorených a technologicky neutrálnych“ štandardov sa vzťahujú na všetky bežne uplatňované elektronické služby v rámci e-Governmentu, či už majú podobu webových stránok alebo aplikácií. Ustanovenie § 14 Výnosu následne stanovuje okruh funkčností, ktoré musia byť zabezpečené (1) vždy, alebo (2) „ak je funkčnosť dôležitá a zároveň nie je prezentovaná ako prístupné riešenie aj na nejakom inom mieste“, t.j. nemá alternatívu

spĺňajúcu technické požiadavky prístupnosti webových stránok. Štandardy prístupnosti webových stránok sú dôležité jednak pre osoby s rôznymi typmi postihnutia, ale zároveň pre všetkých používateľov, keďže ich dodržiavanie garantuje poskytovanie informácií vo forme spracovateľnej na rôznorodých softvérových a hardvérových produktoch. Napríklad jedno zo základných povinných pravidiel prístupnosti, podľa bodu 1 Prílohy č. 1.1 Výnosu, je poskytovať textové alternatívy k netextovým prvkom ako sú napríklad obrázky, animácie, audio, video, interaktívne či programové objekty, umožňuje slabozrakým a nevidiacim, aby im softvér na čítanie textov nahlas prečítal obsah vizuálnych objektov, ktorý by pre nich inak zostal skrytý. V praxi sa totiž často informácie poskytujú vo forme naskenovaných dokumentov, obrázkových grafov a podobne, čím sa úplne znemožňuje prístup k týmto informáciám pre zrakovo postihnuté osoby. Tieto informácie sú však dôležité pre všetkých používateľov vzhľadom na potrebu textového vyhľadávania v obsahu a ďalšieho spracúvania informácií. Rovnaké pravidlo je vyžadované aj pre všetky dokumenty zverejňované verejnou správou v §18 písm. d) Výnosu, ktoré požaduje spracovanie a rozoznávanie textových informácií v spracovateľnej textovej forme a poskytovanie textových opisov k netextovým prvkom. Jeden z veľkých problémov totiž predstavujú súbory PDF, ktoré často znemožňujú čítačkám nevidiacich prístup k zverejneným informáciám – a to najmä kvôli vytváraniu týchto súborov s rôznymi obmedzeniami oprávnení, nevhodnému nastaveniu softvéru pre vytváranie týchto súborov, poskytovaniu dokumentov iba v skenovanej forme a podobne.

Pre nepočujúcich a nedoslýchavých má prístupnosť zabezpečovať napríklad povinné pravidlo 1.3 a 1.4 Prílohy č. 1 Výnosu, poskytovať titulky alebo „zápisy“ k vizuálnym alebo zvukovým záznamom. Povinné pravidlo 2.1 a 2.2 prílohy č. 1 Výnosu má zaručovať prístupnosť informácií aj pre osoby bez schopnosti rozoznávať farby či jemné odtiene. Zároveň je však dôležité pre používateľov s displejmi s obmedzeným rozsahom farieb.

Medzi povinnosť z posledne menovaného okruhu patria aj povinnosti podľa bodu 8.1 Prílohy č. 1 Výnosu, ktorý znie nasledovne:

„8.1 – Príloha č.1 Výnosu

Programové prvky ako sú skripty a applety sa robia priamo prístupné alebo

kompatibilné s pomocnými technológiami. *Nie je vhodné, aby obsah ani kód webovej stránky predpokladal, prípadne vyžadoval konkrétny spôsob použitia ani konkrétne vstupné alebo výstupné zariadenie*. Ak to nie je možné, poskytuje sa prístupné alternatívne riešenie.

8.1.1 *Kód ani obsah webovej stránky nepredpokladá alebo nevyžaduje, aby mal používateľ konkrétny operačný systém, konkrétny prehliadač, aktívny zvukový výstup a podobne*."

Z vyššie uvedeného je zrejmé, že v prípade daňových výkazov išlo o jasné porušovanie predpisov o štandardoch[86]. Ako vidieť, zákonná úprava o štandardoch je zároveň veľakrát formulovaná tak, aby zaručila, že najmä (nie však iba) ak štátny orgán používa určité technické riešenie ako výlučný kanál, štát je zaviazaný používať technologicky neutrálne riešenia. Bohužiaľ však dodnes existuje len málo konkrétnych príkladov, v ktorých by takéto štandardy boli aj následne vynucované voči porušujúcim organizáciám verejnej moci. Je zreteľné, že právne predpisy o štandardoch v skutočnosti pomáhajú realizovať pozitívny záväzok štátu v oblasti technologickej inkluzívnosti. Majú teda zásadný ústavnoprávny rozmer.

3.1.3.2. Predpisy o elektronickom podpise

Ďalším druhom legislatívy, ktorý sa vzťahuje na komunikáciu orgánov verejnej moci s občanom, je zákon č. 215/2002 Z.z. o elektronickom podpise, ktorý je transpozíciou smernice o elektronickom podpise[87]. Za formu „elektronického podpisu" tak, ako ho definuje čl. 2 ods. 2 smernica, sa považujú „dáta v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k ostatným elektronickým dátam a ktoré slúžia ako metóda overovania pravosti". Ako ďalej špecifikuje čl. 3 smernice, „Členské štáty môžu používanie elektronického podpisu vo verejnom sektore podmieniť splnením ďalších možných požiadaviek. *Tieto požiadavky budú objektívne, transparentné, primerané a nediskriminačné a budú sa vzťahovať výlučne na*

86 Technológia použitá v prípade „eDane" a „eTax", používa produkt D.Signer/XAdES a prvok ActiveX. Riešenie Active X je podľa slov samotného Finančného riaditeľstva SR viazaný na prostredie OS Windows a interntové prehliadače, ktoré podporujú aktívne prvky kódu.

87 Smernica Európskeho Parlamentu a Rady 1999/93/ES z 13. decembra 1999 o rámci spoločenstva pre elektronické podpisy; Smernica vo svojom čl. 19 uvádza, že „elektronické podpisy sa budú používať vo verejnom sektore v rámci orgánov štátnej správy krajín a správy spoločenstva a v styku takýchto orgánov s občanmi a hospodárskymi subjektami, napríklad v systémoch verejného obstarávania, daňovej správy, sociálneho zabezpečenia, zdravotníctva a justície".

špecifické znaky príslušného použitia. Také požiadavky nesmú byť prekážkou cezhraničných služieb pre občanov“. Okrem tejto všeobecne formulovanej požiadavky bude od 1. 7. 2016 podstatná aj obligácia štátu za istých okolností uznávať kvalifikované elektronické podpisy, pečate a časové pečiatky vydané v iných členských štátoch. Vzhľadom na aktuálnosť témy a jej zásadný dopad na povinnosti verejnej správy v oblasti elektronizácie, sme sa rozhodli zaradiť do obsahu tejto publikácie osobitnú kapitolu o očakávaných zmenách, na ktoré ešte len musí čiastočne reagovať aj slovenský zákonodarca.[88]

3.1.4. Ochranný mechanizmus

Nateraz sme sa venovali predovšetkým otázke povinností štátu pri elektronizácii. Lenže ako je možné vidieť aj v našej prípadovej štúdii daňových výkazov, štát veľakrát nedodržiava svoje ústavnoprávne zakotvené povinnosti. Naskytá sa preto otázka, ako sa postaviť k situácii, v akej bola napríklad spoločnosť EURA Slovakia, ktorá pre porušovanie povinností na strane štátu nemohla podať daňový výkaz elektronicky a bola následne aj sankcionovaná za jeho nedodanie, hoc ho dodala v papierovej podobe. Otázka ochranných mechanizmov však vzniká aj v obrátenom garde, a síce keď znevýhodnený občan nepotrebuje len „štít“ pred konaním štátu (napr. jeho pokutou), ale aj „meč“ proti jeho neaktivite. Prípadová štúdia prevodu poľnohospodárskych pozemkov poskytuje dobrý príklad v tomto smere. Občan, ktorý nemôže previesť pôdu, potrebuje „meč“, aktívny prostriedok ochrany proti protiprávnemu správaniu štátu, ktorý v čase spustenia znemožnil predaj pôdy približne 97 % obyvateľom Slovenska[89].

Aké právne inštrumentárium teda môže poskytnúť štít a meč? Jedna z možností pre poskytnutie sebaobrany občana proti štátu v situácii, keď si štát vynucuje splnenie elektronickej podmienky, hoc nevytvoril právne a faktické podmienky na jej splnenie, je možnosť považovať takúto situáciu za *okolnosť vylučujúcu protiprávnosť*. Správanie orgánu verejnej moci, ktoré vedie k uloženiu sankcie je totiž nedielnou

88 pozri časť publikácie Exkurz, s. 66.

89 Ministerstvo pôdohospodárstva si nový zákon o nadobúdaní vlastníctva poľnohospodárskeho pozemku totiž vysvetlilo tak, že pri prevode poľnohospodárskej pôdy sa musí používať výlučne elektronický občiansky preukaz (tzv. eID). Z vydaných viac ako tristo tisíc preukazov, bol čip aktivovaný avšak len u približne polovice, a teda, že dnes reálne previesť pôdu môže orientačne len 150.000 občanov.

súčasťou skutkovej podstaty správneho deliktu, keďže jeho objektívnu stránku (nesplnenie elektronickej povinnosti) priamo vyvolalo (podmienilo). Protiprávne *nevytvorenie podmienok na splnenie povinnosti*, na ktorú sa sankcia vzťahuje, by malo byť v dobre spravovanom štáte považované za okolnosť vylučujúcu protiprávnosť správneho deliktu. Zoberme si nasledovný jednoduchý príklad na demonštráciu. Ak zákon predpisuje, že koncoročné daňové priznanie možno podať iba elektronicky do konca marca, pričom systém daňovej správy nebude niekoľko mesiacov pred týmto termínom funkčný, je nielen spoločensky neprípustné, ale aj (ústavno)právne nekonformné, aby daňová správa následne za nepodanie daňových priznaní ukladala akékoľvek sankcie. Dostupnosť jediného zákonom uznaného spôsobu splnenia povinnosti (napr. webovej stránky) je totiž podmienkou splnenia tejto povinnosti a zlyhanie štátu nemôže byť v neprospech adresáta právnej normy. Ak by preto aj štát následne udelil pokutu, občan by sa mal vyhnúť akejkoľvek sankcii, pretože nevytvorenie faktických a právnych podmienok na splnenie zákonnej povinnosti zo strany štátu vylučuje protiprávnosť jeho následného nesplnenia daňovej povinnosti – je jej zmarením. Samozrejme, aby sa predišlo možnému zneužívaniu takéhoto inštitútu, je možné vyžadovať aby adresát právnej normy preukázal, že naozaj mal úmysel splniť uloženú povinnosť (napr. pripravením daňového priznania alebo doručením jeho papierovej verzie, hoc to zákon neumožňuje).

O niečo náročnejšia otázka je ako pristupovať k prípadom, keď je potrebné takpovediac „pohnúť štát“ k tomu aby vytvoril ústavnoprávne konformné podmienky. Jednou z možností je využiť možnosti správneho súdnictva, v rámci ktorého možno namietať aj na nečinnosť orgánu verejnej moci. Inou možnosťou je obrátiť sa priamo na Ústavný súd SR v rámci individuálnej sťažnosti podľa čl. 127 Ústavy SR. S poukázaním na to, že ide o prípad hodný osobitného zreteľa (napr. záujem presahuje záujem navrhovateľa), môže totiž Ústavný súd SR prijať sťažnosť na ďalšie konanie, aj keď neboli vyčerpané iné opravné prostriedky (§ 53 ods. 2 zákona o ústavnom súde), ktoré zákon poskytuje (napr. správne súdnictvo, sťažnosť a pod.). Súd potom môže v prípade vyhovenia žiadosti prikázať, aby ten, kto základné právo alebo slobodu porušil svojou nečinnosťou, vo veci konal (§ 56 ods. 3 písm. a) zákona o ústavnom súde). Len v niektorých prípadoch bude možné, aby spotrebiteľské organizácie uplatnili § 39

zákona o ochrane hospodárskej súťaže[90] v rámci ich oprávnení podávať žalobu v prospech spotrebiteľstva[91]. Pokiaľ sa štát zároveň dopúšťa porušovania predpísaných štandardov, je možné sťažovať sa aj na Ministerstve financií SR, ktoré má však len možnosť ukladať pokuty[92] a nemôže teda zjednať nápravu pre dotknutého jednotlivca. Existujúce prostriedky teda, zdá sa, sú dosť obmedzené. O to viac by sa mal preto o prípady zaujímať samotný Ústavný súd SR.

Zároveň by mal zákonodárca zvážiť zavedenie nových, resp. objasnenie existujúcich neštátnych kolektívnych mechanizmov na vynucovanie predpisov o štandardoch. Jednou z možností je vyjasniť v rámci zákona o informačných systémoch verejnej správy, že ide o predpis s cieľom ochrany spotrebiteľa, a to minimálne na účely § 3 ods. 5 zákona č. 250/2007 Z.z. o ochrane spotrebiteľa. Takýmto krokom by spotrebiteľské organizácie jednoznačne mali možnosť podávať kolektívne zdržovacie žaloby na orgány verejnej moci, ktoré predpisy o štandardoch nedodržujú.

3.1.5. Zhrnutie

V tejto časti sme poukázali na to, že ani rozhodnutie orgánu verejnej moci o elektronizácii nie je bez ústavnoprávnych konzekvencií. V prvom rade elektronizáciu nemožno vykonávať „len tak“, teda bez riadneho zákonného podkladu. K ukladaniu právnych povinností, resp. obmedzovania základných práv a slobôd musí dochádzať v súlade s požiadavkami čl. 13 Ústavy. Preto by nebolo možné napríklad zaviesť povinnosť výlučnej elektronickej komunikácie len v rámci podzákonných predpisov, alebo takto riadne zavedenú povinnosť ďalej obmedziť len svojou administratívnou praxou. Ústavnoprávna prípustnosť plnej elektronizácie takéhoto druhu podľa nášho názoru závisí od: (1) okruhu osôb, ktoré budú dotknuté opatrením, (2) stupňa informačnej vyspelosti skupín (1) a (3) stupňa náročnosti uplatňovaného riešenia. Štát

90 Znenie: “Orgány štátnej správy pri výkone štátnej správy, obce a vyššie územné celky pri výkone samosprávy a pri prenesenom výkone štátnej správy a záujmová samospráva pri prenesenom výkone štátnej správy nesmú zjavnou podporou zvýhodňujúcou určitého podnikateľa alebo iným spôsobom obmedzovať súťaž.”

91 § 3 ods. 5 zákon č. 250/2007 Z.z. o ochrane spotrebiteľa.

92 § 10 zákona o ISVS; MF SR v roku 2015 opakovane na žiadosť o informácie odpovedalo, že vynucovalo štandardy – napríklad pre eID klienta pre Mac OS X a Linux – a to tým, že pozastavilo financovanie projektu. Podľa zákona o IS VS však má udeľovať finančné sankcie, žiadne iné tento zákon nepozná. A finančné sa skutočne dodnes žiadne neudelili. Preto je na zváženie, čo sem napísať.

má povinnosť zvoliť čo najviac šetrné riešenie vo vzťahu k dotknutým základným právam a slobodám. Zároveň má pozitívnu povinnosť vytvoriť faktické a právne podmienky adresátom takto formulovaných elektronických povinností, aby si mohli usporiadať život v súlade s právom. Pri implementovaní technologických riešení štát má ústavnú povinnosť usilovať sa o čo najväčšiu inkluzívnosť. Na tento účel už dnes slúži niekoľko právnych predpisov, ktoré napríklad určujú formu štandardov, ktoré je potrebné dodržiavať pri elektronických riešeniach v kontexte výkonu verejnej moci. V poslednej časti textu boli krátko predstavené možné obranné mechanizmy, ktoré môže dnes jednotlivec voči štátu uplatniť. Predovšetkým, pokiaľ ide o možnosť „pohnúť“ orgány verejnej moci k zlepšeniu situácie, sa tieto mechanizmy zdajú dosť obmedzené.

3.2. Zbieranie osobných údajov zo strany štátu

Prechod z papierovej formy vykonávania verejnej správy na elektronickú nesie so sebou aj zvýšenú intenzitu informácií, ktoré orgány verejnej správy zbierajú, uchovávajú a spracovávajú v podobe dát v elektronickej forme. Informatizácia prináša nesporné množstvo výhod vo forme okamžitého prístupu k informáciám, možnosti jednoducho kombinovať rôzne informácie a preposielať ich medzi jednotlivými orgánmi v rádoch sekúnd. Aj keď je využitie informačných technológií „dobrým sluhom“, môže byť zároveň „zlým pánom“. Svet mal možnosť presvedčiť sa o obrovskej výpočtovej sile, ktorou oplývajú vlády niektorých krajín a o tom, s akou jednoduchosťou dokážu zbierať údaje v nepredstaviteľných rozsahoch, a to všetko bez vedomia občanov. Odhalenia Edwarda Snowdena,[93] ktoré v prvom rade upriamili pozornosť na tieto skutočnosti, potvrdili obavy mnohých a šokovali svojou závažnosťou.

Vo svete po odhaleniach o zneužití osobných údajov tajnými službami je potrebné pýtať sa štátu na každé uchovávanie a spracovávanie údajov. Nielen tajné sledovanie je nebezpečné – vytváranie akéhokoľvek systematického prehľadu o osobných údajoch a živote občanov nesie so sebou zásah do ich súkromia. Pokiaľ teda

93 GREENWALD, Glen, POITRAS, Laura, MACASKILL, Ewen. *Edward Snowden: the whistleblower behind the NSA surveillance revelations | US news*. [online]. The Guardian, 11.06.2013. [cit. 30.11.2015].

štát nemá riadny dôvod na vytváranie databáz údajov o fyzických osobách a nekoná tak len s rešpektom k ústavným obmedzeniam, nemôže zásah do práv občanov obstáť. V tejto časti sa preto budeme venovať podmienkam zberu osobných údajov zo strany štátu a na pozadí prípadov predstavených v prvej časti publikácie. Vysvetlíme, aké sú základné predpoklady pre zber osobných údajov zo strany štátu a budeme ich konfrontovať s prípadmi aplikácie „Superkolky“ a zberu údajov do JISCD. Pokúsime sa určiť, či je takýto zber v súlade so základnými právami občanov, príp. upriamiť pozornosť na problematické momenty zberu údajov a vytýčiť niekoľko bodov, na ktoré si musí dať štát pozor, ak chce zbierať osobné údaje. Bude tak učinené najmä hodnotením z pohľadu ustanovení Ústavy SR a judikatúry Ústavného súdu SR. V neposlednom rade má text slúžiť ako upozornenie pre orgány verejnej správy a teoretické meradlo pre hodnotenie prípadov zberu údajov do budúcna.

3.2.1. Úvodné úvahy – Ochrana osobných údajov ako základné právo a súčasť práva na ochranu súkromia

Právo na súkromie patrí vo svojom najširšom zmysle k základným ľudským právam. Právo „byť ponechaný osamote“ bolo pôvodne reakciou na technologický rozvoj na konci 19. storočia a príchod všadeprítomných fotoaparátov.[94] Ako ľudskému právu tzv. prvej generácie sa ochrane súkromia dostalo uznanie vo Všeobecnej deklarácii ľudských práv.[95] V priebehu 20. storočia sa postupne právo na súkromie stalo pevnou súčasťou katalógov ľudských práv, ako na medzinárodnej, tak aj na európskej a národnej úrovni. V podmienkach SR dnes k najvýznamnejším prameňom práva na súkromie, ktorými je viazaná, patria čl. 8 Európskeho dohovoru o ochrane ľudských práv (ďalej len „Dohovor“), ktorý ustanovuje právo každého na rešpektovanie jeho súkromného a rodinného života, čl. 7 Charty základných práv Európskej únie (ďalej len „Charta“), ktorý ustanovuje právo na rešpektovanie súkromného a rodinného

94 WARREN, Samuel D. and BRANDEIS, Louis D. *The Right to Privacy.* Harvard Law Review, 15.12.1890 [online]. Vol. 4, no. 5, p. 193. [cit. 30.11.2015].

95 čl. 12 Všeobecnej deklarácie ľudských práv.

života, čl. 16 Ústavy SR, ktorý zaručuje nedotknuteľnosť osoby a jej súkromia.[96] [97]

Na druhej strane, právne nástroje hovoriace o *základnom* práve na ochranu osobných údajov sú doménou len posledných desaťročí. Podobne ako pri technologickom pokroku na konci 19. storočia, zvyšujúca sa automatizácia administratívnych úkonov a čoraz častejšie používanie počítačov v druhej polovici 20. storočia vyvolali obavy zo zneužitia „informačnej moci“ vo vzťahu k informáciám uchovávaným o jednotlivcoch.[98]V Európe sa v roku 1981 jedným z prvých nadnárodných nástrojov na ochranu osobných údajov stal Dohovor č. 108 o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov.[99]Osobné údaje sa stali späté nerozlučne s definíciou obsiahnutou v čl. 2 písm. a) dohovoru: „informácie, ktoré sa vzťahujú na nejakého identifikovaného alebo identifikovateľného jednotlivca“.[100]Neskôr sa osobným údajom venovala pozornosť na pôde Európskeho spoločenstva, ktoré postupne prijalo niekoľko právnych nástrojov na zabezpečenie práv na ochranu osobných údajov. Posledný vývoj, ktorý jednoznačne „povýšil“ právo na ochranu osobných údajov na základné právo bolo prijatie Lisabonskej zmluvy.[101]Uznanie práva každého na ochranu osobných údajov sa preto nachádza už aj v zakladateľských dokumentoch samotnej Európskej únie. Najabsolútnejším vyjadrením *základného* práva na ochranu osobných údajov sa stal čl. 8 Charty základných práv Európskej únie (ďalej len „Charta“). Na rozdiel od Dohovoru, ktorý

96 Zaradiť sem možno aj čl. 17 Medzinárodného paktu o občianskych a politických právach. Pozri – Vyhláška č. 120/1976 Zb. ministra zahraničných vecí z 10. mája 1976 o Medzinárodnom pakte o občianskych a politických právach a Medzinárodnom pakte o hospodárskych, sociálnych a kultúrnych právach.

97 Je na mieste vysvetliť vzťah medzi Chartou a Dohovorom – čoby medzinárodnými nástrojmi a Ústavou SR – ako národným prameňom práva. Dohovor a rovnako i Charta sú medzinárodnou zmluvou o ľudských právach v zmysel čl. 7 ods. 5 Ústavy SR a majú teda prednosť pred zákonom. Na druhú stranu, pozornosť vyžaduje aj čl. 51 ods. 1 Charty, ktorý obmedzuje jej aplikovateľnosť len na prípady kedy sa vykonáva právo Únie. Bližšie pozri napr. nález Ústavného súdu SR, sp. zn. PL. ÚS 10/2014,§ 64.

98 Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. *European Treaty Series - No. 108* [online]. Council of Europe, 1981. [cit. 25.11.2015].

99 Oznámenie č. 49/2001 Z. z. Ministerstva zahraničných vecí SR o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov.

100 Podobne definuje sú definované osobné údaje aj v predpisoch Európskej únie. Pozri – čl. 2 písm. a) Smernice Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov

101 Bližšie vysvetlenie k tomu čo sú zmluvy EÚ a čo je Lisabonská zmluva pozri napr. http://europa.eu/eu-law/decision-making/treaties/index_sk.htm

pozná iba právo na rešpektovanie súkromného života v čl. 8, Charta – čo by modernejší nástroj – explicitne chráni a uznáva ochranu osobných údajov ako základné právo.[102]Charta, ako predtým nezáväzný dokument, získala prostredníctvom Lisabonskej zmluvy postavenie rovné so zakladateľskými dokumentmi EÚ.[103]Tvorí tak právne jednu z najsilnejších záruk základného práva na ochranu osobných údajov v únii.

Vyššie predostretý vývoj pôsobí mätúco. Z výkladu sa zdá, že ochrana jednotlivca v oblasti súkromia sa vykryštalizovala do dvoch separátnych základných práv – práva na súkromie a práva na ochranu osobných údajov. Do popredia sa tlačí otázka, aký zmysel má delenie ochrany v oblasti súkromia na dva samostatné celky.

3.2.1.1. Základné právo na ochranu osobných údajov v podmienkach Dohovoru a Charty

Právo na ochranu súkromného života, garantovaného čl. 8 Dohovoru, je potrebné vnímať ako široko koncipované. Nemôžeme o ňom uvažovať ako o singulárnom práve. Vhodnejšie zvolenou rétorikou je predstaviť si právo na ochranu súkromného života ako akési „dáždnikové“ právo, ktoré chráni niekoľko odlišných, i keď súvisiacich záujmov.[104]Ochrana súkromného života pod čl. 8 Dohovoru tak zahŕňa ochranu dobrého mena a cti, ochranu obydlia, ochranu korešpondencie a tajomstva dopravovaných správ a neposlednom rade zahŕňa zákaz uschovávať a zhromažďovať osobné údaje.[105]Výpočet tu uvedených hodnôt nemožno považovať za vyčerpávajúci – definovať všetky hodnoty chránené právom na súkromný život by nebolo možné z dôvodu rozmanitosti prípadov a chránených záujmov.[106]

Ako je zrejmé, ochrana osobných údajov je jednou zo súčastí práva na súkromný život. Vyplýva to z početnej judikatúry ESĽP, v ktorej potvrdil,

102 Nutné však upozorniť, že sa aplikuje len v prípade použitia práva EÚ – pozri čl. 51 ods. 1 Charty.

103 Pozri poznámku č. 10.

104 Pozri známu taxonómiu – SOLOVE, Daniel J. A Taxonomy of Privacy. *University of Pennsylvania Law Review*. 2006, roč. 154, č. 4, s. 558- ktorý zhodnotil, že síce právo na súkromie chráni do určitej miery súvisiace záujmy, nie je možné ich spojiť jednou spoločnou črtou.

105 Takýto príkladmí výpočet uvádza SVÁK, Ján. *Ochrana ľudských práv v troch zväzkoch.* Bratislava: Eurokódex, 2011, 3 sv., s. 425 (príkladmo vymedzuje obsah práva na súkromie; jedna z oblastí je aj zber a uchovávanie osobných údajov).

106 KMEC, Jiří; KOSAŘ, David; KRATOCHVÍL, Jan a BOBEK, Michal. *Evropská úmluva o lidských právech: komentář*. 1. vyd. Praha: C.H. Beck, 2012, s. 867.

že zbieranie a uchovávanie osobných údajov je spôsobilé zasiahnuť do práva na súkromný život podľa čl. 8 Dohovoru.[107] Ak sú teda údaje osôb chránené v režime čl. 8 Dohovoru, aký zmysel má presadzovanie osamoteného práva na ochranu osobných údajov? Túto otázku v súčasnosti rieši odborná literatúra nejednoznačne.[108] V súvislosti s prijatím Charty, ktorá ako jeden z prvých ľudskoprávnych nástrojov priznáva základné právo k osobným údajom, nie je možné s istotou povedať to, aký cieľ sledoval normotvorca.[109]

Napriek panujúcej neistote ohľadom pôvodu samostatnej normy nemožno súhlasiť so záverom, že čl. 8 Charty je čisto formálnym oddelením od práva na súkromie, alebo že by malo ísť iba o *ex post* potvrdenie legitimity právneho rámca EÚ na ochranu osobných údajov. Naopak, rozsah základného práva na súkromie a základného práva na ochranu osobných údajov nie sú totožné.[110] Obe práva je potrebné vnímať ako čiastočne prekrývajúce sa, nie však s rovnakým obsahom. Je možné predostrieť imaginárne prípady, v ktorých by nedošlo nutne k zásahu do základného práva na súkromie, avšak základné princípy práva na ochranu osobných údajov by porušené boli.[111] Informácie a spôsoby spracovania, ktoré chráni právo na osobné informácie, nebudú vždy aj zásahom do práva na súkromie.[112]

Napriek plodným teoretickým úvahám o existencii dvoch odlišných práv zostáva ale faktom, že súdna prax tento rozdiel doposiaľ neadresovala úplne a obe

107 Napr. S a Marper proti Spojenému kráľovstvu (č. 30562/04 a 30566/04), Peck proti Spojenému kráľovstvu (č. 44647/98), P.G. a J.H. proti Spojenému kráľovstvu (č. 44787/98).

108 LYNSKEY, Orla. Deconstructing Data Protection: The "Added-Value" Of A Right To Data Protection In The EU Legal Order. *International and Comparative Law Quarterly* [online]. 2014, vol. 63, no. 03, s. 570 a nasl. [cit. 26.11.2015].(Zhrňuje niektoré súčasné názory).

109 Ibid.

110 LYNSKEY, 2014, op.cit., s. 582 a nasl.;LEMMENS, Paul. Relations between the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights - Substantive Aspects. *Maastricht J. Eur. & Comp. L.* 2001, vol. 8, s. 57 – 58; KOKOTT, Juliane a Christoph SOBOTTA. The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*. 2013, roč. 3, č. 4, s. 225; PEERS, Steve; HERVEY, Tamara K; KENNER, Jeff a WARD, Angela. *The EU Charter of fundamental rights: a commentary*. First edition. Oxford: Hart publishing, 2014,, s. 229

111 LYNSKEY, 2014, op.cit., s. 585 – Príklad s atlétkou školy, o ktorej zverejnili informácie.

112 LYNSKEY, 2014, op.cit., s. 582 a nasl.; KOKOTT, SOBOTTA, 2013, s. 225; DE HERT, Paul a Serge GUTWIRTH. Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In: GUTWIRTH, Serge ; POULLET, Yves; P. DE HERT, Paul (eds.). *Reinventing data protection?* Springer Science, Dordrecht, 2009, s. 23.

základné práva zlučuje pod jeden režim prieskumu.[113]Bez ohľadu na túto skutočnosť považujeme za dôležité neignorovať teoretické oddeľovanie oboch práv, ktoré môže byť v budúcnosti pretavené aj do rozhodovacej činnosti súdov.

3.2.1.2. Základné právo na ochranu osobných údajov v podmienkach Ústavy SR

V podobnom duchu ako je Charta istou anomáliou medzi právnymi inštrumentmi na ochranu osobných údajov, sa štandardu na národnej úrovni vymyká Ústava SR. Ústava SR, popri samotnom práve na súkromie (v čl. 16 ods. 1 a čl. 19 ods. 2), zaručuje výslovne v čl. 19 ods. 3 ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe a v čl. 22 ods. 3 ochranu osobných údajov.[114]V rovine komparácie s inými ústavnými poriadkami sú ustanovenia čl. 19 ods. 3 a 22 ods. 3 nadčasové a európske ústavy bežne neobsahujú zmienku o ochrane osobných údajov.[115]Obvykle je právo na ochranu osobných údajov v rovine národných garancií základných práv koncipované ako súčasť iných základných práv – či už práva na súkromie (podobne ako je to v Dohovore), alebo práva na ľudskú dôstojnosť.[116]Nie je celkom zrejmé to, z akého dôvodu bola slovenská ústava rozšírená aj o explicitnú ochranu osobných údajov. Niektorí komentátori považujú opakované prízvukovanie hodnôt súvisiacich s ochranu súkromia za duplicitné a komplikujúce.[117]

Vzťahom medzi rôznymi ustanoveniami sa zaoberal aj samotný Ústavný súd SR v niekoľkých rozhodnutiach. Súd robí rozdiely medzi ochranou podľa čl. 16 ods. 1 a čl. 19 ods. 2 v tom, aký druh hodnoty chránia – prvé menované chráni *telesnú*

113 LYNSKEY, 2014, op.cit., s. 573.

114 Čl 19 ods. 3 znie: „Každý má právo na ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe“; Čl. 22 ods. 1 znie: „Listové tajomstvo, tajomstvo dopravovaných správ a iných písomností a ochrana osobných údajov sa zaručujú“.

115 Nejde však o úplnú výnimku, ochranu osobných údajov výslovne presadzuje aj napr. ústavný poriadok Portugalska či Belgicka.

116 Pozri napr. Česká republika (WAGNEROVÁ Eliška; ŠIMÍČEK Vojtěch; LANGÁŠEK Tomáš; POSPÍŠIL Ivo. Listina základních práv a svobod: komentář. Vyd. 1. Praha: Wolters Kluwer Česká republika, 2012,s. 343) alebo Nemecko (ROUVROY, Antoinette a Yves POULLET. The right to informational self-determination and the value of self-development. Reassessing the importance of privacy for democracy. In: GUTWIRTH, Serge ; POULLET, Yves; P. DE HERT, Paul (eds.). *Reinventing data protection?* Springer Science, Dordrecht, 2009, s. 45 – 76).

117 Ústava chráni súkromie v podstate až na troch miestach – DRGONEC, Ján. *Ústava SR: komentár*. 3. vydanie. Šamorín: Heuréka, 2012, s. 441.

integritu a materiálne hodnoty, druhé zasa *nemateriálne hodnoty.*[118] Je teda zrejmé, že v oblasti elektronizácie bude dominovať koncept ochrany súkromia podľa čl. 19 ods. 2 ústavy. Podľa súdu je čl. 19 ods. 2 všeobecnou úpravou v porovnaní s čl. 19 ods. 3 chrániacim pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov, ktorý považuje za *lex specialis*. V tomto ohľade sa tak súd stotožnil s praxou ESĽP a podradil ochranu osobných údajov pod všeobecné právo na súkromie.[119] Naopak, pri interpretovaní čl. 22 ods. 1 zúžil jeho aplikovateľnosť len na prípady súvisiace s listovým tajomstvom a tajomstvom dopravovaných správ.[120] V podobnom duchu sa nesie aj novšia judikatúra ústavného súdu. Podľa súdu nie je separácia a oddelenie ustanovení o ochrane súkromia namieste a je potrebné vnímať všetky ustanovenia ucelene ako jednotný systém.[121] Z tónu ústavného súdu sa zdá, že na ochranu osobných údajov neprikladá extra dôraz a považuje ju za systematickú súčasť práva na súkromie.[122] Prehľad systému ochrany súkromia a osobných údajov Ústavy SR by teda vyzeral nasledovne:

- čl. 19 ods. 2 – Predstavuje ochranu súkromia vo všeobecnosti (chráni nemateriálne hodnoty),
- čl. 19 ods. 3 – Predstavuje ochranu osobných údajov ako *lex specialis* k čl. 19 ods. 2,
- čl. 22 ods. 1 – Predstavuje ochranu osobných údajov, ale len v kontexte listového tajomstva, tajomstva dopravovaných správ a iných písomností.

Vyššie uvedenú diskusiu je teda možné zhrnúť tak, že zber, uchovávanie alebo rozširovanie osobných údajov je jedným zo spôsobov, ktoré sú spôsobilé zasiahnuť do základných práv jednotlivcov – či už je ochrana osobných údajov chránená explicitnými ustanoveniami (ako je to v prípade Charty a Ústavy SR), alebo spadá pod širší rámec práva na ochranu súkromného života (v čl. 8 Dohovoru). Pri diskusii o

118 Nález Ústavného súdu SR, sp. zn. III. ÚS 88/01.
119 Nález Ústavného súdu SR, sp. zn. I. ÚS 33/95, s. 5 – 7.
120 Ibid.; Nález Ústavného súdu SR, sp. zn. II. ÚS 19/97.
121 Nález Ústavného súdu SR, sp. zn. I. ÚS 290/2015, s. 25.
122 Avšak pozri nález Ústavného súdu SR, sp. zn. PL. ÚS 10/2014, kde súd vykladá rozdiel medzi čl. 7 (právom na súkromie) a čl. 8 (právo na ochranu osobných údajov) Charty (s. 43); nevyjadruje sa však k systematike slovenskej ústavy.

základnom práve na ochranu osobných údajov je potrebné odlišovať – ochrana osobných údajov je jednak súčasťou ochrany súkromného života (v zmysle čl. 8 Dohovoru), ale môže byť takisto chápaná ako samostatné základné právo (v zmysle čl. 8 Charty). Ak bude ďalej použitý pojem „právo na súkromie“, myslí sa tým ochrana osobných údajov v rámci práva na ochranu súkromného života.

3.2.2. Ochrana osobných údajov ako negatívny záväzok štátu

Ochrana osobných údajov ako súčasti práva na súkromie znamená ochranu pred zásahom od akéhokoľvek subjektu. Povinnosť rešpektovať právo na ochranu osobných údajov sa dotýka tak jednotlivcov, ako aj štátu. V tomto ohľade možno konštatovať, že štát má dvojaké záväzky – na jednej strane ide o *negatívne záväzky* štátu, t.j. povinnosť nezasahovať do práva na súkromie a ochranu osobných údajov, no zároveň *pozitívne záväzky* štátu, čo znamená zavedenie takých opatrení, aby k porušovaniu práva na súkromie nedochádzalo ani zo strany súkromných osôb.[123]

Pre diskusiu o zbieraní osobných údajov verejnou správou a štátnymi orgánmi má zásadný význam rozhodovacia prax ESĽP a jeho výklad čl. 8 Dohovoru. Judikatúra súdu v Štrasburgu ukazuje, že dominantnými porušovateľmi sú práve samotné štáty, ktoré zbierajú osobné údaje prostredníctvom vlastných aktivít a orgánov. Súd deklaroval porušenie práva na ochranu súkromného života hneď v niekoľkých typovo obdobných situáciách.

Zber a spracovávanie osobných údajov súvisí predovšetkým s činnosťou bezpečnostných zložiek štátu. Polícia a tajné služby potrebujú pre svoje fungovanie veľakrát pracovať s citlivými a utajovanými informáciami, ktoré obsahujú aj osobné údaje. Nie je preto prekvapením, že najčastejšími previnilcami pri porušovaní ochrany súkromného života sú práve policajné zbory alebo spravodajské služby.[124] Ako sa však ESĽP vyjadril, žiaden cieľ nie je natoľko dôležitý, aby mohol ospravedlniť ľubovôľu

123 STRÁŽNICKÁ, Viera. *Medzinárodná a európska ochrana ľudských práv*. Bratislava: Paneurópska vysoká škola, 2013, s. 371 a nasl.

124 Pozri prípady ako Amann proti Švajčiarsku (č. 27798/95), Peck proti Spojenému kraľovstvu (č. 44647/98), S. a Marper proti Spojenému kráľovstvu (č. 30562/04 a 30566/04).

orgánov a bezbrehé zasahovanie do súkromia.[125]Bezpečnostné zložky musia takisto rešpektovať limity, ktoré pre nich predstavuje základné právo na súkromie.

Obmedzovanie výkladu len na prípady bezpečnostných zložiek by bolo príliš zužujúce. Nezáleží na tom, ktorá zložka štátu alebo akým spôsobom uchováva údaje. Porušenia sa môže dopustiť ktorýkoľvek orgán. K negatívnym záväzkom štátu v najvšeobecnejšej rovine ESĽP uviedol, že:

> „Uchovávanie údajov týkajúcich sa súkromného života jednotlivca zo strany štátnych orgánov sa rovná zásahu do práva v zmysle článku 8. Následne použitie uložených údajov nemá žiaden vplyv na vyššie uvedené konštatovanie.“[126]

Z pohľadu ESĽP už len samotné uchovávanie údajov zo strany orgánov predstavuje zásah do práva na súkromie a musí byť ospravedlniteľné v rámci limitov určených čl. 8 Dohovoru.[127] V opačnom prípade dochádza k porušeniu základného práva jednotlivca zo strany štátu. Pre hodnotenie z hľadiska Dohovoru teda nie je dôležité akým spôsobom orgán údaje získava – či ide o tajné sledovanie alebo štát zbiera údaje „otvorene“. Môže ísť dokonca aj o uchovávanie údajov, ktoré sú voľne dostupné z otvorených zdrojov, t.j. údaje, ktoré sa nenachádzajú priamo v súkromnej sfére osoby.[128]Koniec koncov, nedávne zrušenie plošného uchovávania dát jasne ukazuje, že aj presné určenie typov uchovávaných údajov je stále zásahom do súkromia.[129]Akýkoľvek *spôsob* zbierania a uchovávania údajov je schopný zasiahnuť do práva na súkromie.

V staršej judikatúre ESĽP – resp. v tomto prípade Európskej komisie pre ľudské práva – sa objavili prípady, v ktorých použitie osobných údajov orgánom verejnej správy nebolo považované za zásah do práva na súkromie. V prípade *Friedl*, v ktorom rakúska polícia odfotila a poznamenala si osobné údaje demonštranta, nedošlo

125 Klass a ostatní proti Nemecku (č. 5029/71, § 49) – tu v zmysle boja proti špionáži a terorizmu.
126 Amann proti Švajčiarsku (č. 27798/95, § 69).
127 A tento právny názor si osvojil aj Ústavný súd SR, pozri nálezy III. ÚS 204/02, s. 10 a I. ÚS 290/2015, s. 44.
128 Pozri prípad P.G. and J.H. proti Spojenému kráľovstvu (č. 44787/98).
129 Rozsudok Súdneho dvora EÚ, Vec C-293/12; pozri aj nález Ústavného súdu SR, sp. zn. PL. US 140/2014.

podľa názoru komisie k zásahu do súkromia.[130]Svoj postoj komisia obhajovala predovšetkým skutočnosťou, že údaje neboli zaznamenané do žiadneho systému a neboli ďalej spracovávané automaticky.[131]Do istej miery prízvukuje systematickosť zbierania a uchovávania údajov ako jednu z čŕt zásahu do súkromia aj neskoršia judikatúra.[132]Pri diskusii o zbieraní údajov v digitálnom prostredí ale stráca význam rozlišovať medzi *ad hoc*, jednorazovým získaním údaju a systematickým zbieraním – automatické zbieranie údajov je zo svojej povahy systematické a nejednorazové, údaje sú automaticky uchovávané v databázach orgánov a sú ďalej okamžite spracovateľné a využiteľné. Preto, ak vyššie uvedené aplikujeme na prípady ako je mobilná aplikácia Superkolky alebo JISCD, pôjde o zásah do práva na súkromie vždy.

3.2.3. Dovolené obmedzenia práva na ochranu osobných údajov

Právo na súkromie a ochranu osobných údajov nie je právom absolútnym. Ustanovenie čl. 8 Európskeho dohovoru o ľudských právach obsahuje v druhom odseku limitnú klauzulu, ktorá umožňuje obmedziť právo na súkromie za tam stanovených okolností.[133] Rovnako nepovažuje právo na súkromie za neobmedziteľné ani Charta[134] a Ústava SR.[135]

Premietnuté do diskusie o role štátu teda limitácia znamená, že v určitých prípadoch môžu štátne orgány porušiť právo na ochranu osobných údajov, ale len ak je tento zásah ospravedlniteľný dohovorom. V literatúre i judikatúre ESĽP dominuje test zložený z troch krokov, prostredníctvom ktorého súd určuje to, či došlo k porušeniu čl. 8 Dohovoru. Tradične musia byť splnené:[136]

130 Friedl proti Rakúsku (Prípad č. 28/1994/475/556).
131 Ibid, § 8.
132 Kopp proti Švajčiarsku (Prípad č. 13/1997/797/1000) alebo Leander proti Švédsku (č. 9248/81).
133 Čl. 8 ods. 2 Dohovoru stanovuje: „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“.
134 Ktoré je obmedzené princípmi v čl. 8 ods. 2 a čl. 52 Charty.
135 Pozri vysvetlenie v náleze Ústavného súdu SR, sp. zn. I. ÚS 33/95, s. 6 a I ÚS 290/2015, s. 30, 38 - 39.
136 STRÁŽNICKÁ, 2013, op.cit., s. 372; Niekedy sa test uvádza ako 5-krokový – t.j. ako krok testu sa počíta aj zisťovanie, či je daný článok aplikovateľný a či dané (ne)konanie napáda hodnotu chránenú článkom. Takto vymedzuje KMEC, Jiří; KOSAŘ, David; KRATOCHVÍL, Jan a BOBEK, Michal, 2012, op.cit., s. 866.

- Legalita – obmedzenie musí byť stanovené na základe zákona (príp. iného všeobecne záväzného predpisu), ktorý musí byť verejne dostupný, ktorý jasne špecifikuje práva a povinnosti jednotlivcov a orgánov a ktorého následky musia byť dostatočne predvídateľné.
- Legitimita – zásah musí sledovať Dohovorom aprobovaný záujem; tieto záujmy vymenúva čl. 8 ods. 2 Dohovoru.
- Proporcionalita – zásah musí byť nevyhnutný v demokratickej spoločnosti.

Podobne sa k testovaniu zásahov z pohľadu základných práv stavia aj Súdny dvor Európskej únie (ďalej len „SDEÚ“). Vo veci *Rundfunk* súd zvolil postup zhodný s postupom s ESĽP.[137] Nasledovanie princípov obmedzenia práva na súkromie podľa čl. 8 ods. 2 Dohovoru vyplývajú z právneho poriadku únie.[138] SDEÚ teda rovnako aplikoval test o troch krokoch (legalita, legitimita, nevyhnutnosť). Pozícia SDEÚ sa nezmenila ani po prijatí Charty ako nástroja špecificky oddeľujúceho právo na súkromie (čl. 7 Charty) a právo na ochranu osobných údajov (čl. 8 Charty).[139]

Napokon, všímajúc si pôsobenie na národnej úrovni, Ústavný súd SR takisto konštantne zdôrazňuje význam Dohovoru ako medzinárodného nástroja, ktorý viaže Slovenskú republiku a jej silu v slovenskom právnom poriadku. V rozhodnutí *Data retention* ústavný súd uviedol: „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“.[140] Preto, podobne ako ESĽP, aj ústavný súd skúma, či došlo k zásahu do práva na súkromie a následne či sa tak udialo na základe zákona, s legitímnym cieľom a či bol primeraný.[141]

137 Rozsudok Súdneho dvora EÚ, veci C-465/00, C-138/01 a C-139/01 (Österreichier Rundfunk).
138 Bod 70 rozhodnutia poukazuje na čl. 1 smernice o ochrane osobných údajov (95/46/EC), ktorý považuje ochranu základného práva na súkromie za jeden z cieľov úpravy.
139 Pozri napr. rozhodnutie Volker und Markus Schecke (C-92/09 a C-93/09), bod. 50 a nasl.
140 Nález Ústavného súdu SR, PL. ÚS 140/2014 (vec Data retention), s. 38.
141 Konkrétnu aplikáciu v kontexte ochrany súkromia pozri napr. v nálezoch PL. ÚS 140/2014, II. ÚS 53/2010, I. ÚS 114/2012.

3.2.4. Legalita zbierania osobných údajov – má finančná správa právomoc zbierať údaje?

V jednej z predchádzajúcich častí sme predstavili problém mobilnej aplikácie „Superkolky“, ktorá zbiera niekoľko druhov osobných údajov o jej používateľoch – meno používateľa, jeho polohu či informácie o jeho zariadení. Už na prvý pohľad je zrejmé, že pôjde o zber a uchovávanie údajov, ktoré zasahujú do práva na ochranu osobných údajov. Ako ukázala analýza odborníkov na informačné technológie, aplikácia je schopná odoslať rôzne osobné údaje Finančnej správe SR. Je teda nutné považovať ju za schopnú automaticky a systematicky zbierať údaje, ktoré sú následne uchovávané Finančnou správou SR.

Okolnosti vzniku aplikácie z nej robia exemplárny príklad problému, čo znamená legalita zásahu do práva na súkromie. ESĽP v prvej polohe skúmania dovoleného obmedzenia stanovuje, že sa tak vždy musí udiať na základe zákona (resp. iného všeobecne záväzného právneho predpisu, pričom sem možno zaradiť aj súdne rozhodnutia). Zákonnosťou obmedzenia sa nerozumie len formálne konštatovanie, že zákon obmedzujúci právo existuje. Čl. 8 Dohovoru kladie na obmedzujúci predpis určité kvalitatívne kritériá. Predpis musí byť predovšetkým adekvátne dostupný a dostatočne precízny, aby umožnil adresátovi regulovať svoje chovanie.[142]Treba však pripomenúť, že táto podmienka neznamená úplnú predvídateľnosť toho, aké údaje sú zbierané a uchovávané.[143]

Čo vzbudzuje otázky pri aplikácii „Superkolky“, je jej základ v zákonnej úprave. V časti venujúcej sa faktickému pozadiu vzniku aplikácie sme uviedli, že vznikla zrejme z vlastnej iniciatívy finančnej správy. Ak nebol vznik aplikácie a následný zber údajov o jej používateľoch predpísaný konkrétnou právnou normou, je na mieste otázka legality takéhoto zberu.

Dôležitým prvkom ústavnej ochrany práva na súkromie v Slovenskej republike je jej obmedziteľnosť iba právnym predpisom o sile zákona. ESĽP síce túto otázku

142 The Sunday Times proti Spojenému kráľovstvu (č. 6538/74), podobne aj Ústavný súd SR, pozri nižšie poznámku č. 68 a prislúchajúci text.

143 Weber a Saravia proti Nemecku (č. 54934/00, § 93).

doposiaľ vyslovene neriešil, no Ústavný súd SR jednoznačne stanovil za jediný prípustný spôsob obmedzenia len zákon.[144]Osobné údaje nie je možné obmedziť nariadením vlády, vyhláškou a ani všeobecne záväzným nariadením. Neprípustné je i delegovanie právomoci na orgán verejnej moci a o to viac nemôže orgán obmedziť právo na ochranu súkromia vlastným interným predpisom.[145]Striktná podmienka obmedzenia zákonom nemôže byť v podmienkach slovenského právneho poriadku nijako zľahčená.

Podmienku zákonnosti potom treba v podmienkach slovenského ústavného práva spojiť so zásadou „*Čo nie je dovolené, je zakázané*“, vtelenej do ustanovenia čl. 2 ods. 2 Ústavy SR.[146]Jej účelom je vytvoriť právnu istotu jednak voči občanom a ďalším subjektom, že orgán verejnej správy nebude voči nim konať v rozpore so svojou právomocou, ale takisto nastolenie istoty v tom, aká právomoc sa priznáva určitému orgánu.[147]Premietnuté do diskusie o zbieraní osobných údajov, orgán verejnej správy si nemôže bez patričného zmocnenia ani pri najlepšej vôli sám určiť, že bude zbierať osobné údaje či viesť ich v databázach a informačných systémoch. Prekračoval by tak hranice čl. 2 ods. 2 Ústavy SR. Na vymedzenie právomocí orgánov môžu slúžiť len zákon a ústava, nie svojvôľa osôb konajúcich v mene orgánu.[148]

V najvšeobecnejšej rovine upravuje spracovávanie osobných údajov zákon o ochrane osobných údajov.[149]Ten sa vzťahuje na spracovanie osobných údajov *každým*, tzn. i orgánmi verejnej správy.[150]Spracovávať osobné údaje je možné len: „[…] na základe priamo vykonateľného právne záväzného aktu Európskej únie, medzinárodnej

144 Nález Ústavného súdu SR, sp. zn. I. ÚS 290/2015, s. 31; cituje názora Drgonca, ktorý sa síce vyjadruje prostriedkov sledovania občanov, súd však tento názor rozšíril všeobecne na akúkoľvek aplikáciu čl. 16 ods. 1 Ústavy SR.

145 Ibid,s. 30.

146 Tú je potrebné vykladať v súčinnosti s čl. 152 ods. 4 Ústavy SR, ktorý ukladá: „*Výklad a uplatňovanie ústavných zákonov, zákonov a ostatných všeobecne záväzných právnych predpisov musí byť v súlade s touto ústavou.*“

147 DRGONEC, 2012, op.cit., s. 200.

148 Ibid, s. 200.

149 Zákon č. 122/2013 Z.z, o ochrane osobných údajov.

150 Pozri vysvetlenie k § 2 – Dôvodová správa k zákonu č. 122/2013 Z.z.: „Preto sa pristúpilo k vypusteniu slovného spojenia „orgány štátnej správy, orgány územnej samosprávy, iné orgány verejnej moci, ako aj ostatné právnické osoby a fyzické osoby" a nahradilo sa slovom „každý", ktoré ho plnohodnotne nahrádza, čím sa zjednodušuje a sprehľadňuje právna úprava.“ - *Dôvodová správa* [online]. Vládny návrh zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, Parlamentná tlač 358, Národná rada SR [cit. 30.11.2015], s. 2.

zmluvy, ktorou je Slovenská republika viazaná, ustanovení tohto zákona alebo osobitného zákona, alebo na základe súhlasu dotknutej osoby“.[151]Črtajú sa dve základné možnosti ako môže byť vyhovené podmienke legálnosti – buď je zber údajov ustanovený na základe osobitného zákona, alebo je možné použiť inštitút súhlasu.

3.2.4.1. Právomoc na základe osobitného zákona

Základ pre zber osobných údajov finančnou správou na základe osobitného zákona možno hľadať v predpisoch ustanovujúcich štruktúru orgánov verejnej správy na vymedzenom úseku a ich pôsobnosť. Pre finančnú správu je týmto predpisom zákon č. 333/2011 Z.z., o orgánoch štátnej správy v oblasti daní, poplatkov a colníctva.[152]Zákonodarca myslel na osobné údaje hneď v niekoľkých ustanoveniach. Najdetailnejšie upravuje právomoci Ministerstva financií SR, ktorému umožňuje spracovávať osobné údaje pre účely správneho alebo daňového konania a druhy spracovávaných údajov špecifikuje.[153]S podobnou detailnosťou zákonodarca predostiera právomoc Kriminálneho úradu finančnej správy.[154]Na druhej strane, špecifikácia právomocí ostatných orgánov finančnej správy v detailnosti zaostáva. Zákon sa obmedzuje na všeobecné konštatovanie: „Finančné riaditeľstvo, daňové úrady, colné úrady a Kriminálny úrad finančnej správy tvoria finančnú správu, ktorá spracúva informácie a osobné údaje podľa osobitných predpisov“.[155]

Vo svetle judikatúry ESĽP je nevyhnutné položiť otázku, či môžu takto všeobecne vymedzené právomoci vyhovieť kvalitatívnym požiadavkám legality. S poukazom na prvú podmienku – dostupnosť zákona – možno konštatovať, že je splnená. Ustanovenia umožňujúce zber a spracovanie osobných údajov sa nachádzajú v dostupnom a verejne publikovanom právnom predpise, zákone o orgánoch štátnej

151 § 9 ods. 1, Zákon č. 122/2013 Z.z, o ochrane osobných údajov.

152 Iným vhodným začiatkom analýzy zákonnosti by mohol byť daňový poriadok (zákon č. 563/2009 Z. z.; ustanovenie § 164) – na koľko však spracovávanie údajov nie je vykonávané na účely správy daní, tento zákon ako legitímny podklad na zber údajov vylučujeme.

153 § 3 ods. 2; spracovávané údaje sú konkretizované v prílohe k zákonu

154 Môže uchovávať a spracovávať údaje o „o osobách, ktoré porušili daňové predpisy alebo colné predpisy alebo je dôvodné podozrenie, že porušujú daňové predpisy alebo colné predpisy, alebo ktoré v oblasti pôsobnosti finančnej správy narušili alebo je dôvodné podozrenie, že narúšajú verejný poriadok a ďalšie informácie o takýchto porušeniach daňových predpisov alebo colných predpisov alebo narušeniach verejného poriadku; takéto informácie a osobné údaje poskytne alebo sprístupní finančnému riaditeľstvu, daňovému úradu alebo colnému úradu v rozsahu potrebnom na plnenie ich úloh“ - § 5 ods. 3 písm. b) zákona o orgánoch štátnej správy v oblasti daní, poplatkov a colníctva.

155 § 2 ods. 2. zákona o orgánoch štátnej správy v oblasti daní, poplatkov a colníctva.

správy v oblasti daní, poplatkov a colníctva. Zákon je publikovaný v Zbierke zákonov a je teda možné považovať ho za ľahko dostupný a verejne známy.[156]

Vo vzťahu k podmienke predvídateľnosti zákona pre jeho adresátov do uspokojivej miery nie je odpoveď zďaleka priamočiara. Vo veci *The Sunday Times proti Spojenému kráľovstvu* súd uviedol nasledovný štandard pre predvídateľnosť: „[Občan] musí byť schopný […] predvídať, do miery ktorá je daných podmienkach rozumná, následky ktoré môže dané konanie obnášať".[157]Obzvlášť v kontexte tajného sledovania súd uviedol, že stupeň predvídateľnosti nemôže ísť až tak ďaleko, aby bola sledovaná osoba schopná na základe právnej úpravy prispôsobiť svoje správanie – no zároveň jedným dychom dodáva, že zákon musí byť prinajmenšom natoľko zrejmý, aby občanom „dostatočne indikoval" podmienky, za ktorých štát môže siahnuť po sledovacích opatreniach.[158]

Istým vodidlom je aj rozhodnutie Ústavného súdu SR v kauze *Biele kone*.[159]Súd sa extenzívne zaoberal podmienkou zákonnosti v kontexte zbierania údajov finančnou správou. Podľa súdu sú ustanovenia umožňujúce spracovávanie údajov finančnou správou (odkazované a citované vyššie) príliš všeobecné. V hodnotení šírky ustanovení súd skonštatoval, že:

> „Medzi priznanou právomocou a ochranou osobných údajov per se existuje vzťah nepriamej úmery. Čím je právomoc orgánu verejnej moci disponovať údajmi o osobe všeobecnejšia, a preto dostupná na rozšírenie interpretáciou práva, tým väčšiu pozornosť treba venovať skúmaniu podmienok, obsahu a rozsahu zverenej dispozície a splneniu materiálnych podmienok".[160]

Ak má byť preto ustanovená právomoc orgánu zbierať a uchovávať osobné údaje na základe všeobecnejšej normy, musí byť o to väčší dôraz kladený na materiálne podmienky úpravy – t.j. jej legitímny účel a proporcionalitu.[161]

Urobiť jednoznačný záver k zákonnosti na základe judikatúry ESĽP a

156 Publikovaný ako čiastka 107/2011.
157 The Sunday Times proti Spojenému kráľovstvu (č. 6538/74, § 49).
158 Pozri poznámku č. 50.
159 Nález Ústavného súdu SR, sp. zn. I. ÚS 290/2015.
160 Ibid., s. 36.
161 Ibid., s. 40. - najmä body 65 a 66.

Ústavného súdu SR nie je jednoduché. ESĽP sa pri skúmaní podmienok zákonnosti orientuje najmä na tajné sledovanie, o ktoré však v prípade aplikácie „Superkolky“ nejde. Judikatúra ústavného súdu na druhej strane obsahuje určité pomôcky, sú však príliš všeobecne formulované a je ťažké ich aplikovať na konkrétny prípad. Je zrejmé, že pre zber a uchovávanie údajov finančnou správou existuje určitý základ v zákone o orgánoch štátnej správy v oblasti daní, poplatkov a colníctva. Pochybnou ale zostáva prílišná šírka právomoci a otázka, či je na základe takéhoto ustanovenia možné zbierať údaje takým spôsobom, akým je aplikácia „Superkolky“. Z dôvodu právnej istoty je v každom prípade vhodné, aby sa zákonodarca vyvaroval široko formulovaným právomociam k spracovávaniu osobných údajov. Zároveň, z pohľadu samotných orgánov, tieto by sa nemali pokúšať testovať hranice široko vymedzených právomocí. Z princípu trojdelenia mocí vyplýva, že zákonodarná moc obmedzuje a brzdí moc verejnú, preto nemôžu orgány verejnej správy bez ďalšieho považovať ani širšie vytýčené právomoci ako signál pre „divokejšie“ zbieranie údajov.

3.2.4.2. Spracovanie so súhlasom dotknutej osoby

Osobitnú pozornosť treba venovať funkcii *súhlasu so spracovaním osobných údajov*. Ústavný súd pri niekoľkých príležitostiach uviedol, že spracovávať osobné údaje je možné buď na základe zákona, alebo so súhlasom dotknutej osoby.[162] Nie je teda vylúčené, že namiesto ustanovenia právomoci v osobitnom zákone by orgán verejnej správy spracovával údaje na základe súhlasu dotknutej osoby v režime všeobecného zákona o ochrane osobných údajov.

Spracovávanie osobných údajov na základe súhlasu však nemožno vykonávať bez ďalšieho. So spracovávaním na základe súhlasu je spojených niekoľko špecifických podmienok zákona o osobných údajoch ohľadom súhlasu a určenia účelu spracovania osobných údajov, ktoré by v prípade aplikácie „Superkolky“ neboli splnené.[163] Navyše, súhlas nemožno v prípade interakcie medzi občanom a orgánom

162 Nálezy Ústavného súdu SR, sp. zn. III. ÚS 204/02 a I. ÚS 290/2015.

163 Súhlas umožňujúci prístup k údajom v telefóne daný pri inštalácii takisto nemožno bez ďalšieho považovať za súhlas podľa zákona o ochrane osobných údajov – ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 02/2013 on apps on smart devices* [online]. 2013, 00461/13/EN, WP 202, Adopted on 27 February [cit. 30.11.2015], s. 14. Okrem požiadaviek na súhlas (§ 11 a nasl.) by však neboli splnené ani napr. požiadavky na vymedzenie účelu spracovania osobných údajov (§ 6 ods. 2).

verejnej správy, medzi ktorými je vzťah podriadenosti a nadriadenosti, považovať za plnohodnotné riešenie. Orgán by bol veľakrát z pozície moci schopný vynútiť si súhlas od dotknutej osoby. V tomto ohľade je možné poukázať na nemeckú právnu úpravu, ktorá v prípade spracovávania osobných údajov orgánmi obmedzuje použitie súhlasu.[164]Dospieť k takémuto záveru možno aj na základe slovenskej ústavy – ak by orgány verejnej správy „obchádzali“ podmienky uchovávania osobných údajov vynucovaním súhlasu, takéto chovanie by nebolo v súlade so zásadami právneho štátu a výkladu ústavy.[165]Preto ak by si finančná správa vynucovala súhlas so spracovaním údajov získaných aplikáciou – najmä pre také zásadné účely, akými je trestný postih pre udávateľov falošných informácií – je potrebné o zákonnosti takéhoto spracovania pochybovať. Orgány verejnej moci musia myslieť na to, že v ich prípade nejde o postavenie na úrovni „súkromná osoba – súkromná osoba“, ale „štát – súkromná osoba“ a existuje tu preto nepomer síl subjektov.

3.2.5. Legitimita zbierania osobných údajov – je nedostatočná kontrola výuky v autoškolách dôvodom na sledovanie?

Ďalšou podmienkou dovoleného obmedzenia práva na súkromie je nutnosť, aby obmedzenie sledovalo legitímny cieľ. I keď je obmedzenie predpísané zákonom, stále nesmie predstavovať svojvoľné obmedzenie práva. Len vybrané ciele, ospravedlniteľné ochranou niektorých záujmov alebo hodnôt, sú schopné legitimizovať zasahovanie do súkromia. Prípad JISCD a zbierania údajov o účastníkoch a lektoroch kurzov autoškôl otvára v tomto ohľade dôležitú otázku. Po preskúmaní dôvodov pre zákonnú úpravu je zreteľné, že zákonodarca chce dosiahnuť vyššiu transparentnosť výučby tak, aby účastníci kurzov dostali taký výcvik, aký predpisujú učebné osnovy.[166]Ministerstvo dopravy ako pripravovateľ zákona si od neho sľubuje predchádzanie falšovania dochádzky a absolvovania predpísaných hodín a jázd a vyššiu bezpečnosť na cestách s poukazom na fakt, že zaistením transparentnejšej

164 DOWTY, Terri a Douwe KORFF. P*rotecting The Virtual Child: The Law and Children's Consent to Sharing Personal Data* [online]. Action on Rights for Children, 2009 [cit. 30.11.2015], s. 32.
165 Najmä s čl. 1 ods. 1, čl. 2 ods. 2 a čl. 152 ods. 4 Ústavy SR.
166 Dôvodová správa, op. cit. (pozri poznámku č. 49).

výučby zníži nehodovosť nových vodičov.[167]Je však takýto cieľ dostatočne dôležitý do tej miery, aby mohol obmedzovať právo žiakov a lektorov na súkromie?

Európsky dohovor o ľudských právach ako ospravedlniteľné záujmy stanovuje:

- národná bezpečnosť,
- verejná bezpečnosť,
- hospodársky blahobyt krajiny,
- predchádzanie nepokojov,
- predchádzanie zločinnosti,
- ochrana zdravia alebo morálky,
- ochrana práv a slobôd iných.

Zoznam záujmov je taxatívny a nie je ho možné rozšíriť.[168]Podobne ako ESĽP, pri skúmaní legitimity zásahu sa aj Ústavný súd SR riadi týmto vymedzením.[169]Z hľadiska porovnania textov Ústavy SR a Dohovoru ale ústava neobsahuje výpočet konkrétnych záujmov.

Napriek tomu, že uzatvorený počet záujmov by mohol nasvedčovať pomerne úzkym možnostiam obmedziť právo na súkromie, v skutočnosti sú jednotlivé kategórie dostatočne široké na to, aby pod ne bolo možné podradiť väčšinu záujmov štátu. Ako naznačuje prípad *Mentzen alias Mencena proti Lotyšsku*, aj taký zdanlivo vzdialený cieľ ako ochrana úradného jazyka môže byť podradený pod zoznam čl. 8 ods. 2 Dohovoru – v tomto prípade ochrana práv a slobôd iných.[170]V niektorých iných prípadoch súd, naopak, uviedol, že výnimky poskytnuté pod čl. 8 ods. 2 Dohovoru

167 KRÁĽ, Milan. Vodičské kurzy budú len pod dohľadom satelitu. *Pravda.sk* [online]. PEREX, a.s., vydané 29.07.2015 [cit. 30.11.2015].

168 napr. Parillo proti Taliansku (č. 46470/11).

169 Pozri nález Ústavného súdu SR, sp. zn. Pl. US 140/2014.

170 KMEC, Jiří; KOSAŘ, David; KRATOCHVÍL, Jan a BOBEK, Michal, 2012, s. 882 - 883; Ako však Kratochvíl upozorňuje, tento konkrétny prípad je potrebné považovať za zvláštnosť, na koľko má historický a politický nádych a je možné, že ESĽP sa v predmetnej veci nechcel miešať do citlivých záležitostí Lotyšska. V každom prípade aj takéto obmedzenie je platným precedentnom a ukazuje flexibilitu obmedzení čl. 8 Dohovoru.

musia byť vykladané úzko a že *potreba výnimky musí byť presvedčivo určená.*[171]

Bez ohľadu na to, či ESĽP zdôrazňuje v texte niektorých rozhodnutí presvedčivosť potreby výnimky, rozhodol o nelegitímnosti obmedzení len v prípadoch, v ktorých zjavne chýbal obmedzeniu akýkoľvek rozumný cieľ. Tak to bolo napr. v prípade obmedzení návštev väzňov na jedenkrát v mesiaci alebo poskytovaní fotografií väzňov médiám.[172]Inak majú členské štáty relatívne voľné ruky pri vtesnaní svojich cieľov pod zoznam záujmov v čl. 8 ods. 2 Dohovoru.

Odporovať cieľom JISCD a novej úpravy zákona o autoškolách by preto bolo možné len ťažko. Obavy o bezpečnosť premávky a zabránenie podvádzaniu pri príprave potrebnej na získanie vodičského oprávnenia sú bezpochyby cieľom, o ktorom možno povedať, že je v záujme verejnej bezpečnosti, ochrany zdravia či ochrany práv a slobôd iných. Ustanovenie výnimky dovoľujúcej podrobné sledovanie a kontrolu účastníkov kurzu má určitý rozumný základ v sledovaní cieľa zlepšiť bezpečnosť premávky. Z hľadiska predchádzajúcej judikatúry ESĽP by bolo o úplnej nelegitímnosti opatrení ťažké hovoriť, aj keď môžeme mať pochybnosti o presvedčivosti potreby mať navrhovaný systém zbierania a uchovávania osobných údajov.

3.2.6. Proporcionalita zbierania osobných údajov – sú použité nástroje primerané?

Ak obmedzenie práva na súkromie prekoná prvé dve prekážky – legalitu a legitímnosť – zostáva zhodnotiť jeho proporcionalitu. Základné právo na ochranu súkromia smie byť porušené len do tej miery, ktorá je nevyhnutná na dosiahnutie sledovaných cieľov. S poukazom na nami analyzovaný prípad – sledovanie žiakov autoškôl – musí byť skúmané, či by nebolo možné dosiahnuť stanovený cieľ s inými nástrojmi alebo nástrojmi, ktoré majú nižšiu intenzitu zásahu do práva.

Slovenský ústavný súd hodnotí primeranosť zásahu na základe „klasického“ testu proporcionality vytvoreného nemeckou judikatúrou a doktrínou po prelome

171 M.N. a ostatní proti San Marínu (č. 28005/12).

172 KMEC, Jiří; KOSAŘ, David; KRATOCHVÍL, Jan a BOBEK, Michal, 2012, s. 883;citujúc rozhodnutia Nowicka proti Poľsku (Žiadosť č. 30218/96) a Khuzhin a ostatní proti Rusku (13470/02).

polovice minulého storočia.[173]Tradične sa test skladá z troch komponentov[174] – kritérium vhodnosti, pri ktorom sa posudzuje schopnosť obmedzujúceho opatrenia dosiahnuť vytýčený cieľ; kritérium nevyhnutnosti (potrebnosti), ktoré hodnotí opatrenia z hľadiska komparácie s alternatívnymi nástrojmi, ktoré by základné právo obmedzovali v menšej miere a kritérium proporcionality *stricto sensu* – zisťovanie, či „príslušná právna norma je primeraná vo vzťahu k zamýšľanému cieľu, t. j. či príslušné legislatívne opatrenie obmedzujúce základné práva alebo slobody nemôže svojimi negatívnymi dôsledkami presahovať pozitíva stelesnené v presadení verejného záujmu sledovaného týmto opatrením "[175].Test sa používa spôsobom „všetko alebo nič", t.j. nesplnenie čo i len jedného kritéria vedie k neústavnosti obmedzenia základného práva a vo väčšine prípadov znamená zároveň ukončenie testovania z dôvodu uplatnenia zásady hospodárnosti.[176]

Nie vždy je ale test používaný ústavným súdom jednotný a vo vyššie predpísanej forme. Niekedy sa ako súčasť prvého kroku skúma existencia dostatočne dôležitého cieľa a následne *racionálnej väzby* medzi normou a cieľom – t.j. hodnotenie, či ustanovenie smeruje k naplneniu cieľa.[177]V iných prípadoch sa už v samotnom teste proporcionality neskúma to, k akému cieľu norma smeruje, ale zisťuje sa len jej previazanosť s daným zámerom. Tak to bolo napríklad vo veci *Data Retention*, keď súd skúmal dôležitosť cieľa v samostatnej analýze po vzore ESĽP.[178]Vylúčenie skúmania dôležitosti cieľa je potom v takýchto prípadoch potrebné chápať tak, že bola preskúmaná už mimo testu proporcionality v rámci skúmania legitimity obmedzenia.

Vychádzajúc z formy, v ktorej sme test proporcionality predstavili, musia byť v

173 HOLLÄNDER, Pavel. *Filosofie práva*. 1. vydání. Plzeň: Aleš Čeněk, 2006, s. 161 a nasl.
174 Ibid., s. 162.
175 Nález Ústavného súdu SR, sp. zn. Pl. US 3/09-378; viac k testu proporcionality vo všeobecnosti pozri tamtiež. Takto – ako štvorkrokový – predstavuje test napr. aj BARAK, Aharon. *Proportionality: Constitutional Rights And Their Limitations*. Cambridge: Cambridge University Press, 2012, časť III; alebo ŠUŠNJAR, Davor. *Proportionality, fundamental rights, and balance of powers*. Leiden: Martinus Nijhoff Publishers, 2010, s. 121 (ktorý rozoberá nemeckú judikatúru).
176 Napr. ak obmedzenie nie je ani schopné dosiahnuť predkladaný cieľ, nie je potrebné skúmať či existuje alternatívne obmedzenie; nie je to však pravidlo a niekedy súd pokračuje ďalej – napr. nález Ústavného súdu SR, sp. zn. Pl. US 3/09-378.
177 Nález Ústavného súdu SR, sp. zn. PL. US 3/09-378.
178 Nález Ústavného súdu SR, sp. zn. PL. US 140/2014, s. 51.

nami skúmaných prípadoch zhodnotené nasledujúce kritériá.

3.2.6.1.Kritérium vhodnosti

Kritériom vhodnosti sa zisťuje schopnosť a možnosť normy dosiahnuť stanovený cieľ. Toto kritérium by nemalo byť chápané ako absolútna podmienka. Obmedzujúce opatrenie nemožno označiť za nevhodné iba z dôvodu, že obmedzenie nemôže cieľ dosiahnuť úplne alebo samostatne. Za nespôsobilé opatrenia možno považovať len tie, ktoré k danému cieľu nijakým spôsobom neprispievajú alebo naň nemajú žiaden účinok.[179]Pôjde o nástroje, v ktorých sa zákonodarca „netrafil vôbec do terča“, ak sa ale trafí – bez ohľadu na to ako presne, kritériu bude vyhovené. Príkladom na takéto zlyhanie by mohlo byť opatrenie zavádzajúce plošné sledovanie všetkých vodičov z dôvodu ochrany morálky. Prosté uchovávanie informácií o vodičoch nie je nijakým spôsobom schopné prispieť k ochrane morálky a išlo by o nezmyselný cieľ. Nástroj by sa teda úplne minul svojmu vytýčenému cieľu.

V nami predloženom prípade autoškôl by bolo náročné presadzovať tézu, že sledovanie výcviku nových vodičov nie je schopné, prinajmenšom, prispieť k znižovaniu nehodovosti a podvádzania pri testoch. Preto by bolo len ťažké oponovať hodnoteniu, že opatrenie je spôsobilé dosiahnuť na stanovené ciele.

3.2.6.2.Kritérium nevyhnutnosti

V kroku skúmajúcom nevyhnutnosť zásahu musí byť určené to, či existuje opatrenie zasahujúce do základného práva v menšej miere, pričom je ale schopné dosiahnuť určený cieľ *v rovnakej miere*. Kritérium vychádza z maximy, že v podmienkach právneho štátu nemôže byť základné právo obmedzené viac než si vyžaduje sledovaný záujem.[180]Pri porovnaní s hypotetickým, menej obmedzujúcim je potrebné si uvedomiť, že nejde o otázku, či je základné právo obmedzené len v malom rozsahu. Skúmajú sa alternatívy a má byť vybraná tá s najmenej obmedzujúcim účinkom bez ohľadu na to, ako veľmi skúmané opatrenie obmedzuje základné právo.[181]

Preto, aj keď sa *a priori* sledovanie žiakov a lektorov autoškôl len v niektorých

179 BARACK, 2012, op.cit., s. 305.
180 Nález Ústavného súdu SR, sp. zn. Pl. US 3/09-378.
181 BARACK, 2012, op.cit., s. 321.

situáciách môže javiť ako nie veľké obmedzenie práva na súkromie, nejde o obmedzenie zanedbateľné. Ak existuje jemnejší a rovnako účinný prostriedok na dosiahnutie lepšej pripravenosti čerstvých vodičov, zákonodarca je povinný ho použiť namiesto prostriedkov sledovania polohy žiakov a času strávenom na vyučovaní.

Sledovanie účastníkov kurzu je v prvom rade nutné postaviť vedľa seba s procesom ich testovania. Základným predpokladom na to, aby mohla osoba viesť motorové vozidlo, je vykonanie predpísaných skúšok (teoretických i praktických) a zisk vodičského oprávnenia. Už samotné testovanie – pod dohľadom príslušníka Policajného zboru SR – implicitne prispieva k cieľu lepšej pripravenosti vodičov a odhaleniu účastníkov autoškôl, ktorí sa prípravy patrične nezúčastnili. Podobne argumentovala aj skupina poslancov žiadajúca odstránenie uchovávania údajov v procese prijímania zákona.[182]

Samotné skúšanie účastníkov kurzu sa javí ako dostatočné a efektívne opatrenie. Ak sa účastník nezúčastní všetkých predpísaných hodín alebo nemá dostatočné znalosti a zručnosti na vedenie vozidla, ponúka sa otázka ako môže prejsť procesom testovania. Otázka by potom mala byť, či namiesto zavádzania sledovania žiakov by nebolo rovnako účinné a zároveň menej zasahujúce do súkromia novelizovať vyučovací a skúšobný proces, napr. zvoliť náročnejšie testy, ktoré by odhalili vynechanie teoretickej prípravy alebo dôslednejšie testovať praktické zručnosti, napríklad dlhšou a náročnejšou skúšobnou jazdou. Aj obavy o absenciu pri vyučovaní by mohli byť rozptýlené dôslednejšou evidenciou vyučovania vedenou autoškolami a častejšími inšpekciami na mieste zo strany orgánov dozoru. Odradiť od podvádzania by mohli aj prísnejšie tresty pre autoškoly umožňujúce obchádzanie zákonných požiadaviek, prípadne i prísnejší trestnoprávny postih zodpovedných osôb.

Ak by sme aj dospeli k záveru, že tieto opatrenia nie sú rovnako účinné ako elektronické sledovanie a uchovávanie údajov, istú inšpiráciu možno brať z podobných prípadov týkajúcich sa uchovávania metaúdajov. Vo veci *Data retention* napríklad Ústavný súd SR uviedol, že si ako menej obmedzujúce opatrenie – v porovnaní s plošným uchovávaním – vie predstaviť použitie *data freezing*-u znamenajúc, že

182 Pozmeňujúce a doplňujúce návrhy, op. cit. (pozri poznámku č. 47).

uchovávanie osobných údajov by bolo možné len selektívne, po splnení určitých podmienok.[183]Rovnako, aj v prípade zákona o autoškolách by bolo možné uvažovať o použití sledovacích prostriedkov až po tom, čo by vzniklo dôvodné podozrenie, že niektoré autoškoly produkujú nedostatočne pripravených vodičov.

Je teda zrejmé, že v nami skúmanom prípade je otvorených viacero presvedčivých argumentov, podľa ktorých by bolo možné prijať opatrenia menej obmedzujúce právo na súkromie, než to bude pri plošnom uchovávaní všetkých údajov o všetkých účastníkoch kurzu.

3.2.6.3.Kritérium primeranosti (proporcionalita v užšom zmysle)

Tretím krokom testu sa preskúmava výsledok dosiahnutý obmedzením a účinok obmedzenia na základné právo. V kritériu primeranosti sa porovnáva *pozitívny* účinok (prospech) dosiahnutý zavedením obmedzujúcej právnej úpravy a *negatívny* účinok (ujma), ktorý má úprava na základné právo.[184]V určitom zmysle ide teda o vyvažovanie „výhod“ a „nevýhod“ obmedzenia základného práva.[185]Na rozdiel od kritéria nevyhnutnosti, keď hľadáme alternatívne obmedzenie, pri skúmaní primeranosti sa pozeráme na benefity obmedzenia a zároveň ujmu, ktorú spôsobí samotnému základnému právu.

Aj v prípade, že by sme dospeli k záveru, že nový systém uchovávania údajov o účastníkoch kurzov je schopný dosiahnuť svoj cieľ a neexistuje, z pohľadu práva na súkromie, menej obmedzujúceho riešenia, niekoľko výhrad by bolo možné nájsť aj v kontexte užšieho skúmania proporcionality. Je napríklad otázne, či extra výhody získané sledovaním a zbieraním podrobných údajov o priebehu vyučovania sú natoľko významné, aby prevážili svojou pozitívnou hodnotou ujmu spôsobenú právu na ochranu súkromia.

183 Nález Ústavného súdu SR, sp. zn. PL. US 140/2014, s. 55.

184 BARACK, 2012, op.cit., s. 340, 342.

185 Užitočnou metaforou sú aj váhy, t.j. na jednu stranu pomyselných váh dáme „výhody“, na druhú „ujmu“ spôsobenú právu a tá strana váhy ktorá je ťažšia určí či je dôležitejšie obmedzenie alebo právo. Pozri – BARACK, 2012 , s. 340; cituje použitie tejto metafory z rozhodnutia Ústavného súdu Juhoafrickej republiky, Štát proti Bhulwana, 1996 (1) SA 388 – bod 18.

3.2.7. Zhrnutie

Zo zvýšenou informačnou mocou orgánov verejnej správy ide ruka v ruke aj zodpovednosť štátu za rešpektovanie a dodržovanie limitov, ktoré umožňujú obmedziť základné právo na ochranu osobných údajov. Ako bolo preukázané, právo na ochranu osobných údajov ašpiruje na status samostatného základného práva (s obsahom čiastočne sa prekrývajúcim so všeobecnejším právom na súkromie), aj keď takéto poňatie ešte možno nepreniklo naplno do súdnej praxe ESĽP či ústavných súdov.

Následne bol zhodnotený zber osobných údajov orgánmi verejnej správy, a to najmä na pozadí káuz rozoberaných v prvej časti publikácie. Bolo vysvetlené, že systematický zber a uchovávanie údajov je nutné považovať za zásah do práva na súkromie, resp. ochranu osobných údajov a že pokiaľ má byť takýto zber v súlade s ústavným poriadkom, musí byť právomoc zbierať údaje daná orgánu zákonom, musí toto zbieranie sledovať legitímny cieľ a nesmie byť svojvoľné. Obmedzenie musí byť schopné v minimálnej miere aspoň napomôcť sledovanému cieľu. Zákonodarca je zároveň povinný vybrať z množiny možných riešení vždy také, ktoré základné právo obmedzuje najmenej. Vo finálne musia byť porovnané pozitívne účinky obmedzujúcej právnej úpravy s jej negatívnymi dopadmi na základné právo.

Aplikovaním na prípady „Superkolky“ a sledovania účastníkov autoškôl bolo zistené, že nie vždy je možné spoľahlivo preukázať splnenie všetkých vyššie zhrnutých podmienok. Ako problematické sa ukázalo najmä zbieranie údajov bez zákonného podkladu v prípade aplikácie „Superkolky“, ktoré by si ideálne vyžadovalo konkrétnejšie zakotvenie v zákonnej úprave. Orgány verejnej správy by si nemali uzurpovať právomoc zbierať osobné údaje, pokiaľ na to nemajú jasné zmocnenie v texte zákona. Verejnú správu treba zároveň upozorniť, že inštitút súhlasu by nemal slúžiť ako ultimátny prostriedok na zahojenie nedostatku právomoci v osobitnom zákone. So súhlasom musia orgány operovať ako s doplnkovou možnosťou, nie ako s hlavným nástrojom.

Pochybnosti vyvoláva aj otázka, či je naozaj nevyhnutné a primerané sledovať dopodrobna priebeh výuky všetkých účastníkov autoškôl, ak by bolo možné naplniť cieľ zlepšenia výuky a bezpečnosti na cestách novelizáciou vyučovacieho procesu.

Otáznikom, ktorý nad zákonodarcami a predkladateľmi zákonov v tomto prípade visí, je potreba zdôvodnenia takéhoto kroku a najmä to, či nie je lepším prostriedkom novelizácia procesu získavania vodičských oprávnení.

Štát je povinný dať si pozor aj na aspekty elektronizácie verejnej správy súvisiace so zberom osobných údajov. Uchovávať osobné údaje nie je možné „len tak“, je potrebné ustanoviť patričnú právomoc v zákone, takéto opatrenie musí smerovať k naplneniu legitímneho cieľa a nesmie ísť nad nevyhnutnú mieru. Nezáleží pritom na tom, či ide o zber dát ľubovoľným orgánom, alebo získavanie údajov bezpečnostnými zložkami prostredníctvom tajného sledovania. Právo na ochranu osobných údajov a súkromie môže verejná správa zasiahnuť rovnako i „otvoreným“ zberom a uchovávaním. Ak chce zákonodarca umožniť správnym orgánom skutočne zasahovať do základného práva, je nutné si uvedomiť, že vyššie predostreté ústavné podmienky obmedzovania práva na súkromia musia byť bez výnimky naplnené. Ponechávanie pochybností o zákonnosti či proporcionalite opatrení posilňujú argumenty o nesplnení podmienok ústavnosti a otvárajú otázku, či sú dodržané ústavné limity práva na ochranu osobných údajov. Zároveň si podmienky a ohraničenie vlastných právomocí musia všímať i samotné orgány. Akákoľvek snaha zo strany výkonnej moci o rozširovanie právomocí alebo podrývanie limitov nastavených zákonom musí byť odsúdená ako neústavná.

Exkurz: Nariadenie eIDAS – povinnosť členských štátov uznávať služby dôvery a prostriedky elektronickej identifikácie z iných členských štátov

Od 1. 7. 2016 sa na území EÚ začne uplatňovať Nariadenie eIDAS[186], ktoré v plnom rozsahu nahradí pôvodnú smernicu o elektronickom podpise[187] implementovanú do právneho poriadku SR zákonom č. 215/2002 Z. z. o elektronickom

186 Nariadenie Európskeho parlamentu a Rady 910/2014 zo dňa 23.6.2014 o elektronickej identifikácii a službách dôvery pre elektronické transakcie na vnútornom trhu.

187 Smernica Európskeho Parlamentu a Rady 1999/93/ES z 13. decembra 1999 o rámci spoločenstva pre elektronické podpisy.

podpise (ďalej len „ZoEP“). Nakoľko je eIDAS nariadením, na území Slovenska ale aj ostatných členských štátov EÚ bude mať priamy účinok a nebude ho tak potrebné implementovať prijatím ďalšieho predpisu na národnej úrovni. Väčšina z ustanovení súčasného Zákona sa tak od účinnosti eIDAS stanú nadbytočnými, resp. sa dostanú do konfliktu s eIDAS. Z toho dôvodu momentálne prebieha príprava návrhu nového zákona, za ktorú zodpovedá Národný bezpečnostný úrad a ktorý by mal ZoEP v plnom rozsahu zrušiť a upraviť len obmedzený okruh ustanovení, ktorý mu eIDAS umožňuje[188].

eIDAS je oproti Smernici podstatne rozsiahlejším predpisom. Smernica obsahuje primárne úpravu týkajúcu sa elektronického podpisu a certifikačných služieb s ním spojených, nakoľko jej primárnym účelom bolo priznanie právnych účinkov elektronickým podpisom, ktorých platnosť bola v niektorých krajinách EÚ spochybňovaná[189]. eIDAS upravuje okrem elektronických podpisov podstatne širší okruh služieb dôvery[190], ktoré bude možné používať v elektronickom prostredí a na ktoré sa v prípade ich použitia v kvalifikovanej forme viažu významné právne účinky a prezumpcie. Novinkou v tomto smere budú elektronické pečate, časové pečiatky a služby ich validácie a uchovávania, autentifikačné služby pre webstránky, elektronická doručovacia služba pre registrované zásielky či služby spojené s uchovávaním elektronických podpisov, pečatí, časových pečiatok a ich certifikátov. eIDAS ustanovuje vo väčšine prípadov dve úrovne služieb dôvery – kvalifikovanú

188 eIDAS napríklad umožňuje členským štátom voľne definovať ďalšie druhy služieb dôvery nad rámec tých v nariadení, ktoré však budú uznávané iba na národnej úrovni. Navyše, členské štáty si môžu ponechať alebo vytvoriť dodatočné ustanovenia k službám dôvery upraveným v eIDAS (v prípade Slovenska by takouto službou mohli byť mandátne alebo autentifikačné certifikáty) ak nie sú plne harmonizované nariadením (bod 24 a 25 prebuly eIDAS).

189 Report from the Commission to the European Parliament and the Council - Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures (COM/2006/0120) [online] In: EUR-lex [on-line informačný systém]. 2006, European Union [cit. 25.11.2015].

190 Súčasný slovenský preklad eIDAS používa na označenie týchto tzv. „trust services“ termín „dôveryhodné služby.“ Domnievam sa však, že tento preklad je nepresný a mal by byť nahradený termínom „služby dôvery“. Ako dôveryhodnú službu je totiž možné označiť akúkoľvek službu, ktorej veríme (napr. službu ubytovania od Air BnB, elektronické trhovisko, taxislužby Uber a pod.), nakoľko ju napr. poskytuje subjekt s dobrou reputáciou a/alebo ktorej pravidlá sú nastavené spôsobom, ktorý zamedzuje porušeniu našich práv (napr. nastavenie mechanizmov vracania peňazí zákazníkom pri nákupe cez eBay). V prípade služieb poskytovaných v zmysle eIDAS je však základnou podstatou týchto služieb práve zabezpečenie dôvery – či už v identitu osoby, s ktorou komunikujeme, nezmeniteľnosti obsahu tejto komunikácie, potvrdení presného času komunikácie a pod. Dôvera teda nie je iba prívlastok popisujúci tieto služby ale vyjadruje ich obsah a podstatu.

a nekvalifikovanú[191], pričom právne prezumpcie viaže vždy na ich kvalifikovanú formu. Slovenský ZoEP ako aj národné predpisy niektorých ďalších členských štátov už aj v súčasnosti upravovali viac služieb dôvery, ako tie spojené s elektronickým podpisom (slovenský ZoEP pozná elektronickú pečať, časovú pečiatku aj autentifikáciu webstránok), tie sú však momentálne uznávané, a teda aj používané iba na národnej úrovni týchto štátov a ich právna úprava nie je jednotná.

Okrem rozšírenia okruhu služieb dôvery, zjednotenia ich právnej úpravy a určenia ich právnych účinkov na úrovni EÚ sú veľmi významné ustanovenia, ktoré zavádzajú povinnosť *za určitých podmienok uznávať kvalifikované elektronické podpisy, pečate a časové pečiatky vydané v jednom členskom štáte ako kvalifikované v každom členskom štáte*, a teda so všetkými relevantnými právnymi následkami. Z hľadiska občanov, ale aj orgánov verejnej správy, ktoré poskytujú svoje služby online, sú však nemenej zaujímavé úplne nové ustanovenia týkajúce sa vzájomného uznávania prostriedkov elektronickej identifikácie. Tieto nové pravidlá majú zaručiť, aby sa identifikačné prostriedky používané v jednom členskom štáte dali použiť na identifikáciu a autentifikáciu pri prístupe k službám poskytovaným verejným sektorom iného členského štátu. V nasledovnej časti tejto práce sa budem bližšie venovať *podmienkam pre uznávanie týchto identifikačných prostriedkov jednotlivými členskými štátmi a následne sa pozriem na podmienky uznávania samotných služieb dôvery*.

1. Vzájomné uznávanie prostriedkov elektronickej identifikácie

V zmysle nových ustanovení eIDAS majú členské štáty povinnosť *uznať prostriedky elektronickej identifikácie používané v iných členských štátoch pre prístup k elektronickým službám poskytovaným subjektmi verejného sektora*[192] tohto štátu v prípade, ak tieto prostriedky spĺňajú určité podmienky.[193] Túto povinnosť uznávania

191 Elektronických pečate a podpisy však môžu byť aj „zdokonalené“.

192 Subjektom verejného sektora je v zmysle čl. 3 ods. 7 eIDAS „ústredný, regionálny alebo miestny orgán, verejnoprávny subjekt alebo združenie tvorené jedným alebo viacerými takýmito orgánmi alebo jedným či viacerými takýmito verejnoprávnymi subjektmi, alebo súkromný subjekt, ktorý aspoň jeden z takýchto orgánov, subjektov alebo združení poveril poskytovaním verejných služieb, keď koná na základe takéhoto poverenia.“

193 Čl. 6 eIDAS

má členský štát vtedy, ak pre prístup k svojej online službe vyžaduje použitie určitých prostriedkov elektronickej identifikácie a autentifikáciu. Pokiaľ štát pre prístup k svojej online službe nevyžaduje použitie takýchto špeciálnych prostriedkov (napr. určitá online služba je dostupná na základe obyčajnej registrácie), nemusí pre túto službu povinne uznať prostriedky identifikácie z iných členských štátov, nakoľko osoby z týchto štátov EÚ by mali k danej službe prístup aj bez ich použitia.

1.1. Prostriedok elektronickej identifikácie

Pre lepšie pochopenie tejto novej povinnosti *vzájomného uznávania* je potrebné vysvetliť pojem *prostriedok elektronickej identifikácie*. Ten predstavuje určitú hmotnú alebo nehmotnú jednotku, ktorá obsahuje identifikačné údaje osoby a ktorá sa používa na *autentifikáciu*, teda overenie identity osoby pre prístup k online službám.[194] Znamená to, že prostriedky elektronickej identifikácie, ktoré bude po novom potrebné uznávať, slúžia na elektronické overenie totožnosti osoby pristupujúcej k online službe (t.j. na jej autentifikáciu, resp. potvrdenie jej identity). V prípade Slovenska je takýmto prostriedkom elektronickej identifikácie občiansky preukaz s čipom, t.j. eID karta, ktorá sa používa na identifikáciu občanov pre prístup k slovenským verejným online službám poskytovaným cez portál Slovensko.sk. Takéto prostriedky identifikácie používané v členských štátoch však môžu byť rôzne a môžu byť založené na rozmanitých technológiách – definícia v eIDAS ponecháva na členských štátoch to, aké prostriedky identifikácie budú používať a je teda technologicky neutrálna.

Nová povinnosť členských štátov vzájomne uznávať si prostriedky elektronickej identifikácie má zabezpečiť, aby sa napr. slovenský občan vedel s použitím svojej eID karty autentifikovať pre prístup k službám, ktoré poskytujú orgány verejnej moci v Anglicku, vo Francúzsku alebo kdekoľvek v EÚ. Nebolo by teda potrebné, aby si vybavoval ďalší prostriedok autentifikácie, napr. estónsku rezidenčnú kartu na to, aby vedel využiť elektronické služby v danej krajine, v tomto prípade Estónsku. Navyše, z vyššie uvedeného podľa nášho názoru zároveň vyplýva, že slovenský občan by sa pre prístup k slovenským alebo zahraničným verejným

194 Čl. 3 ods. 2 eIDAS.

službám mohol autentifikovať s použitím prostriedkov identifikácie vydaných inou krajinou (napr. by mohol použiť estónsku rezidenčnú kartu pre autentifikáciu do portálu Slovensko.sk). Tieto nové ustanovenia by po ich uvedení do praxe teda mali umožniť všetkým osobám, ktoré sú držiteľmi určitého identifikačného prostriedku vydaného členským štátom EÚ (ktorý spĺňa podmienky pre jeho uznanie), autentifikovať sa za účelom prístupu k elektronickej službe poskytovanej ktorýmkoľvek členským štátom EÚ (samozrejme, iba ak je pre prístup k tejto službe požadované použitie identifikačných prostriedkov a autentifikácia).

Je však nutné poznamenať, že princíp vzájomného uznávania sa vzťahuje iba k autentifikovaniu sa do online služieb poskytovanými subjektmi verejného sektora. Samotný prístup k týmto službám a ich dodanie závisí od toho, či je na ich poskytnutie žiadateľ oprávnený v zmysle národného práva danej krajiny.[195] Princíp uznávania teda zaručuje iba to, aby sa osoby z členských štátov vedeli pre prístup k službám iného členského štátu autentifikovať (v prípade, ak je autentifikácia potrebná). Nezaručuje však to, že osoba z iného členského štátu, ktorá sa autentifikovala, bude skutočne môcť aj využiť konkrétnu online službu. Ak je napr. určitá slovenská online služba vyžadujúca použitie eID určená len slovenským občanom (napr. v budúcnosti online voľby do Národnej rady), osoby z iných členských štátov by sa síce mali vedieť prihlásiť na portál Slovensko.sk, túto konkrétnu službu však nebudú vedieť využiť (nebudú môcť voliť), nakoľko na prístup k nej nie sú oprávnené. Princíp vzájomného uznávania teda odbúrava bariéru, ktorá v súčasnosti existuje pri cezhraničnom prístupe k štátnym online službám v rámci EÚ a ktorou je použitie rôznych prostriedkov identifikácie v jednotlivých členských štátoch. Zaručuje teda, že členské štáty budú akceptovať prostriedky identifikácie z iných členských štátov a že teda osoba z členského štátu vôbec bude mať možnosť pristúpiť k službám iných členských štátov. Nezaručuje však to, že osoby z celej EÚ budú mať aj právo použiť skutočne každú online službu, ktorú poskytuje určitý členský štát, nakoľko tá môže byť adresovaná (v zmysle národného práva) len určitému okruhu subjektov. Princíp vzájomného uznávania teda Slovensku neukladá povinnosť umožniť prístup a použitie každej jednej poskytovanej online služby všetkým osobám z ostatných členských štátov.

195 Bod 14 preambuly eIDAS.

1.2. Podmienky vzájomného uznávania prostriedkov el. identifikácie

Na to, aby mohol byť prostriedok identifikácie (napr. mechanizmus autentifikácie v čipe eID karty), ktorý je využívaný pre prístup k určitým slovenským verejným službám, uznaný inými členskými štátmi pre prístup k ich službám, je nevyhnutné, aby Slovenská republika tento prostriedok identifikácie oznámila Európskej komisii v rámci svojej schémy elektronickej identifikácie[196] v zmysle čl. 9 eIDAS. Komisia následne publikuje oznámené schémy elektronickej identifikácie a základné informácie k nim v Úradnom vestníku EÚ. Samotná schéma však musí spĺňať určité podmienky špecifikované v čl. 7 eIDAS – prostriedky identifikácie v nej zahrnuté musia byť vydané oznamujúcim členským štátom, na základe jeho poverenia alebo, ak sú vydané nezávisle od neho, musia ním byť uznané atď. Dôležitá je tiež podmienka, že prostriedok identifikácie je skutočne pripísateľný osobe, ktorú má identifikovať a tiež požiadavka, že členský štát má povinnosť zaručiť dostupnosť jeho online autentifikácie tak, aby si akákoľvek spoliehajúca sa tretia strana na území iného členského štátu mohla potvrdiť identifikačné údaje osoby prijaté v elektronickej forme.[197] Slovensko teda bude musieť zabezpečiť, že ak napr. slovenský občan bude chcieť s použitím eID karty pristúpiť do služby poskytovanej Nemeckom alebo Francúzskom, nemecký/francúzsky poskytovateľ služby bude mať k dispozícii určitý slovenský server, ktorý tohto občana autentifikuje (t.j. slovenský server bude vedieť potvrdiť identifikačné údaje občana, ktoré sú v jeho eID karte). Takúto cezhraničnú autentifikáciu osôb povinne poskytovanú členským štátom môžu využívať aj súkromnoprávne subjekty. V týchto prípadoch však môže členský štát stanoviť podmienky prístupu k ním poskytovanej autentifikácii.[198]

Je potrebné zdôrazniť, že eIDAS nestanovuje povinnosť Slovenska (ani iných členských štátov) oznámiť národné schémy identifikácie – závisí teda od rozhodnutia členského štátu, či ich oznámi. Slovensko má však nezávisle od oznámenia vlastnej

196 Schéma elektronickej identifikácie je v zmysle čl. 3 ods. 4 eIDAS „systém na elektronickú identifikáciu, v rámci ktorého sa fyzickým osobám alebo právnickým osobám alebo fyzickým osobám zastupujúcim právnické osoby vydávajú prostriedky elektronickej identifikácie“.

197 Členský štát navyše v zmysle čl 11 eIDAS zodpovedá fyzickým aj právnickým osobám za zavinené škody spôsobené nesplnením týchto povinností v prípade cezhraničných transakcií (v zmysle národných pravidiel zodopovednosti za škodu).

198 Súkromnoprávne subjekty z iných členských štátov musia mať k autentifikácii prístup za rovnakých podmienok ako domáci súkromní aktéri – bod 17 preambuly eIDAS.

schémy povinnosť uznať oznámené prostriedky elektronickej identifikácie ostatných členských štátov. Táto povinnosť vzájomného uznávania má zaručiť, aby sa osoby z iných členských štátov, ktoré používajú oznámené prostriedky identifikácie, vedeli s ich použitím identifikovať pre prístup k slovenským online službám.[199]

Okrem oznámenia prostriedku elektronickej identifikácie Komisii (v rámci schémy elektronickej identifikácie) stanovuje eIDAS aj ďalšiu podmienku pre povinné uznanie prostriedku identifikácie iným členským štátom.[200] Je nevyhnutné, aby úroveň zabezpečenia tohto prostriedku bola vyššia alebo rovnaká ako tá vyžadovaná daným členským štátom pre prístup k jeho službe, pričom musí spĺňať úroveň zabezpečenia „pokročilá“ alebo „vysoká“.[201] Ak ide o prostriedok elektronickej identifikácie oznámený v rámci národnej schémy, ktorý má úroveň zabezpečenia „nízka“, členský štát ho môže, ale nemusí uznať za účelom identifikácie pre ním poskytované služby. Dá sa teda predpokladať, že členské štáty budú pre svoje prostriedky elektronickej identifikácie primárne používať najvyššiu úroveň zabezpečenia (t.j. „vysoká“), aby zariadili, že ich prostriedok bude nutné uznávať pre prístup k všetkým online službám poskytovaným štátmi EÚ, ktoré použitie určitého prostriedku identifikácie vyžadujú.

Veľmi podstatná je skutočnosť, že v rámci princípu technologickej neutrality eIDAS nepredpisuje pre prostriedky elektronickej identifikácie, ktoré majú byť vzájomne uznávané, použitie žiadnych konkrétnych technológií – členské štáty majú voľnosť v určení konkrétnych prostriedkov na identifikáciu osôb pre prístup k vlastným službám[202]. Členský štát zároveň nemôže od strán spoliehajúcich sa na jeho autentifikáciu vyžadovať *žiadne neprimerané technické požiadavky, ktoré by mohli brániť alebo podstatne sťažiť interoperabilitu oznámených schém identifikácie*. Od samotných držiteľov identifikačných prostriedkov, napríklad občanov SR ako držiteľov eID kariet, však členský štát môže požadovať použitie určitých zariadení, napríklad čítačiek kariet[203].

199 Bod 13 preambuly eIDAS.
200 Čl. 8 eIDAS.
201 Čl. 6 eIDAS.
202 Bod 13 preambuly eIDAS.
203 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market (COM/2012/0238).

2. Uznávanie elektronických podpisov, pečatí a časových pečiatok

Okrem uznávania prostriedkov identifikácie pre prístup k verejným online službám upravuje eIDAS veľmi významné ustanovenia týkajúce sa uznávania služieb dôvery v rámci celej EÚ a ich právnych účinkov. Ustanovuje, že kvalifikovaný elektronický podpis[204], elektronická pečať[205] alebo časová pečiatka budú uznané ako kvalifikované v každom členskom štáte v prípade, ak sú založené na kvalifikovanom certifikáte vydanom v niektorom z členských štátov. Znamená to, že pre kvalifikované elektronické podpisy, pečate a časové pečiatky, ktoré sú založené na kvalifikovanom certifikáte vydanom kvalifikovaným poskytovateľom služieb dôvery nachádzajúcom sa v EÚ, vo všeobecnosti platí voľný obeh v rámci EÚ, a že v celej EÚ sú s ich použitím spájané rovnaké právne účinky[206]. Navyše, v zmysle čl. 14 eIDAS je možné priznať rovnaké právne účinky, a teda aj povinnosť uznávania službám dôvery poskytovaným poskytovateľmi z tretích krajín (t.j. z krajín mimo EÚ). Tie majú byť uznávané ako právne ekvivalentné kvalifikovaným službám dôvery poskytovaným kvalifikovanými poskytovateľmi v EÚ v prípade, že existuje zmluva medzi EÚ a touto treťou krajinou alebo medzinárodnou organizáciou o takomto uznaní služieb dôvery.

eIDAS zároveň v rámci tzv. princípu vnútorného trhu[207] ustanovuje, že v EÚ platí voľný obeh produktov a služieb dôvery, ktoré sú v súlade s eIDAS. Tento princíp

204 Na Slovensku sa v súčasnosti elektornický podpis na úrovni podobnej kvalifikovanému el. podpisu nazýva v zmysle Zákona zaručený elektronický podpis (ZEP) a kvalifikovaná elektronická pečať zaručená elektronická pečať. Zákon upravuje iba jednu úroveň časovej pečiatky, avšak tá je blízka tej kvalifikovanej v zmysle eIDAS.

205 Elektronickú pečať je z technického hľadiska veľmi podobná elektronickému podpisu, vyhotovuje ju však právnická, nie fyzická osoba. Na rozdiel od elektronického podpisu tak neidentifikuje konkrétnu fyzickú osobu, ktorá ju vytvorila, iba právnickú osobu, preto ani v kvalifikovanej forme nemôže mať právny účinok vlastnoručného podpisu ako je to v prípade kvalifikovaného elektornického podpisu. Jej účelom je zabezpečiť, aby text dokumentu, ku ktorému bola pripojená, nebol zmenený (t. j. integritu dokumentu) a že dokument pochádza od konkrétnej právnickej osoby (pôvod dokumentu). Súčasná slovenská právna úprava právneho účinku zaručenej elektronickej pečate v § 40 Občianskeho zákonníka sa však dostáva do rozporu s eIDAS keď zaručenej elektornickej pečati priznáva identické právne účinky ako ZEPu a hovorí o „podpísaní“ dokumentu zaručenou elektronickou prečaťou.

206 V súčasnosti sa totiž právne účinky použitia týchto služieb môžu v jednotlivých štátoch líšiť, aj keď už podľa Smernice mal mať elektronický podpis najvyššej úrovne právnu silu vlastnoručného podpisu tak, ako v zmysle eIDAS kvalifikovaný elektronický podpis. Na použitie kvalifikovanej elektronickej pečate eIDAS viaže prezumpciu integrity a pôvodu „opečateného“ dokumentu a na kvalifikovanú časovú pečiatku prezupciu správnosti dátumu a času, ktorý uvádza a integrity údajov, ku ktorým pripojila dátum a čas.

207 Pozri čl. 4 ods. 2 eIDAS.

má v rámci EÚ zabezpečiť voľný obeh nielen elektronických podpisov, pečatí a časových pečiatok v kvalifikovanej forme, ktorý vyplýva už z ustanovení popísaných v predchádzajúcom odseku, ale aj ostatných služieb dôvery a produktov k nim vo všeobecnosti. Aj tieto "ostatné" služby dôvery majú byť teda v EÚ poskytované slobodne, bez ohľadu na to, či sú alebo nie sú kvalifikované, ak spĺňajú požiadavky eIDAS.

eIDAS navyše upravuje aj špecifické ustanovenia týkajúce sa použitia elektronických podpisov a pečatí vo verejných službách. Je potrebné zdôrazniť, že tieto ustanovenia sa na rozdiel od predchádzajúcej kapitoly týkajú už samotného používania online služieb poskytovaných subjektmi verejného sektora, nie identifikáciou subjektov za účelom prístupu k nim (autentifikáciou). Tieto ustanovenia sa teda vzťahujú napr. k realizácii samotných elektronických podaní alebo iných právnych úkonov vo vzťahu k verejnej správe, pri ktorých je potrebné elektronicky podpísať dokument alebo ho opatriť pečaťou. eIDAS stanovuje, že ak členský štát vyžaduje pre použitie online služby poskytovanej subjektom verejného sektora alebo v jeho mene použitie elektronického podpisu alebo pečate určitej úrovne[208], musí tento členský štát uznať elektronické podpisy alebo pečate z iných členských štátov[209] ak sú rovnakej alebo vyššej úrovne. *Členský štát zároveň nesmie pre svoju online službu vyžadovať elektronický podpis alebo pečať vyššej ako kvalifikovanej úrovne*[210]. Toto ustanovenie by tak malo zabezpečiť, že členské štáty nebudú pre použitie svojich služieb formulovať prísnejšie požiadavky na podpisy alebo pečate na národnej úrovni, čo by mohlo znamenať obmedzenie prístupu k ich službám osobám z iných členských štátov.

3. Zhrnutie

V tejto kapitole boli vysvetlené dôležité povinnosti, ktoré členským štátom vyplynú z eIDAS od 1 .7. 2016 a ktoré sa týkajú uznávania identifikačných

208 V zmysle eIDAS existujú 3 úrovne elektronických podpisov a pečatí: základný podpis/pečať (nazývaný elektronický podpis alebo pečať), zdokonalený elektronický podpis/pečať a kvalifikovaný el. podpis/pečať, pričom v tomto ustanovení sa spomína aj zdokonalený el. podpis/pečať založený na kvalifikovanom certifikáte.

209 Bod 24 preambuly eIDAS však upresňuje, že z povinnosti uznávať služby dôvery členským štátom automaticky nevyplýva povinnosť zaobstarať si hardvér a softvér nevyhnutný na technickú čitateľnosť všetkých existujúcich služieb dôvery.

210 Čl. 27 a 37 eIDAS.

prostriedkov alebo služieb dôvery zo zahraničia. Tieto nové povinnosti členských štátov majú zabezpečiť, aby online služby poskytované verejným a do budúcna aj súkromným sektorom, mohli byť v rámci EÚ poskytované cezhranične. Povinnosť vzájomného uznávania prostriedkov elektronickej identifikácie by mala odstrániť prvú bariéru pri poskytovaní online služieb spôsobenú tým, že každý členský štát predpisuje pre prístup k svojim službám vlastné prostriedky identifikácie založené na rôznych technológiách. Z tejto pre členské štáty náročnej novej povinnosti by mali najviac očakávať benefit práve občania a firmy, ktorým by na prístup k online službám poskytovaných štátmi EÚ (a do budúcna aj súkromnoprávnymi subjektmi) mohol stačiť jediný prostriedok elektronickej identifikácie. Členské štáty by tak rozhodne mali svoje identifikačné schémy oznámiť Európskej komisii aby zaručili, že aj ich prostriedok identifikácie bude cezhranične využiteľný. Totiž aj v prípade, že členský štát svoje identifikačné prostriedky Komisii neoznámi, stále bude mať veľmi náročnú povinnosť prispôsobiť svoje informačné systémy a umožniť prístup osôb z ostatných členských štátov k vlastným službám.

Čo sa týka povinnosti vzájomného uznávania služieb dôvery[211], kvalifikované podpisy, pečate a časové pečiatky vydané v členskom štáte musia byť uznané ako kvalifikované vo všetkých členských štátoch. Táto povinnosť sa teda vzťahuje nielen na verejnoprávne, ale aj súkromnoprávne subjekty. Členské štáty majú ešte dodatočnú uznávaciu povinnosť v prípade, ak pre použitie svojej online služby vyžadujú elektronický podpis alebo pečať. V takom prípade musia uznať elektronický podpis/pečať ekvivalentného alebo vyššieho stupňa ochrany, pričom pre prístup k svojim službám nesmú vyžadovať podpis alebo pečať vyššej ako kvalifikovanej úrovne. Tieto povinnosti uznávania služieb dôvery by mali v prospech občanov a firiem odstrániť ďalšiu bariéru cezhraničného prístupu k online službám v EÚ, a to na úrovni už samotného používania služieb.

211 V zmysle bodu 23 preambuly eIDAS je službu dôvery, ku ktorej sa vzťahuje povinnosť uznávania, možné odmietnuť iba v prípade, ak jej adresát nie je schopný prečítať alebo verifikovať ju z technických príčin, ktoré sú mimo jeho kontrolu.

4. Záver

Zo zisteniach prelínajúcich sa naprieč obsahom publikácie vyplýva, že ani ľudskoprávne aspekty informatizácie verejnej správy nie sú bezproblémové a existuje priestor na zlepšenie a poučenie pre štát a vládu. Naša analýza sa zamerala na dve oblasti identifikované ako „povinnosť elektronickej komunikácie so štátom“ a „zbieranie osobných údajov zo strany štátu“.

Ako sa ukázalo, niektoré aspekty elektronizácie sú pre štát obzvlášť problematické. Štát si musí v prvom rade uvedomiť, že v podmienkach právneho štátu má verejná správa obmedzené právomoci. Ak chce štát vytvoriť určitú povinnosť občanom v elektronickej podobe alebo zbierať ich osobné údaje, môže tak byť učinené výlučne na základe zákona. Nie je možné stanovovať podmienky nad rámec zákona vnucovaním dohôd s občanmi. Orgány verejnej správy si taktiež nemôžu rozširovať či stanovovať právomoci, ktorú sú im dané zákonom.

Podmienky pre splnenie elektronických povinností musia byť stanovené tak, aby boli čo najšetrnejšie k právam a slobodám osôb. Vzhľadom na ústavnosť musí štát poskytovať také riešenia, ktoré sú čo najinkluzívnejšie (vrátane osôb so zdravotným postihnutím či inak znevýhodnených) a technologicky neutrálne. Možno tak učiniť najmä dodržiavaním predpisov o štandardoch vo verejnej správe, ktoré v slovenskom právnom poriadku už existujú.

Záver o šetrnosti a primeranosti patrí rovnako k skúmanej oblasti zberu osobných dát. Štát by mal zasahovať do základného práva na súkromie, resp. práva na osobné údaje len v prípadoch, v ktorých je to skutočne potrebné na dosiahnutie legitímnych cieľov. Tieto nástroje nesmú ísť nad rámec toho, čo je minimálne a primerané. Zákonodarca je povinný zvoliť z množiny možných riešení vždy to, ktoré je k právu na súkromie najviac šetrné. Pre orgány verejnej správy je potrebné zase zdôrazniť, že súhlas nesmie slúžiť ako vyfabrikovaný a občanovi vnútený podklad pre zber údajov.

Ku kritike o nefunkčnosti a predraženosti e-Governmentu je teda potrebné

pridať i kritiku nedôsledného dodržiavania základných práv a podmienok právneho štátu. Aj keď momentálne je informatizácia vnímaná popredne v kontexte jej technologických nedostatkov a finančnej náročnosti, nesmie do pozadia ustúpiť ani výzva na dodržiavanie základných právnych predpisov SR. Dobrá (ale hlavne ústavne konformná) elektronická verejná správa nie je len funkčná a finančne únosná, ale musí byť zároveň zákonná, inkluzívna, musí preferovať technologicky neutrálne riešenia a pokiaľ má zasahovať do základných práv, tak jedine takým spôsobom, ktorý bude tieto práva šetriť a nie ich narušovať do neprípustnej miery. Štát i orgány verejnej správy by sa mali usilovať o dosiahnutie všetkých tu uvedených atribútov, či už z pohľadu moci zákonodarnej v podobe prijímania rozumných a jasných zákonov, alebo z pohľadu moci výkonnej, ktorá nesmie trvať na použití nedovolených prostriedkov a rešpektovať rozsah právomoci jej zverenej mocou zákonodarnou. Digitálna verejná správa nerešpektujúca ľudské práva nemôže byť normou do budúcna a je žiadané, aby sa stav načrtnutý v tejto publikácii v budúcnosti zlepšil.

Použitá literatúra

a) Monografie

- BARAK, Aharon. *Proportionality: Constitutional Rights And Their Limitations*. Cambridge: Cambridge University Press, 2012, xxvi, 611 s. Cambridge studies in constitutional law. ISBN 9781107401198.
- DRGONEC, Ján. *Ústava SR: komentár*. 3. vydanie. Šamorín: Heuréka, 2012, 1620 pages. ISBN 9788089122738.
- HOLLÄNDER, Pavel. *Filosofie práva.* 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2006, 303 s. ISBN 80-868-9896-2.
- KMEC, Jiří; KOSAŘ, David; KRATOCHVÍL, Jan a BOBEK, Michal. *Evropská úmluva o lidských právech: komentář*. 1. vyd. Praha: C.H. Beck, 2012, xxvii, 1660 s. Velké komentáře. ISBN 9788074003653.
- PEERS, Steve; HERVEY, Tamara K; KENNER, Jeff a WARD, Angela.*The EU Charter of fundamental rights: a commentary*. First edition. Oxford: Hart publishing, 2014, xlii, 1893 s. ISBN 9783848704729.
- PRUSÁK, Jozef. *Teória práva*. Vydavateľské oddelenie PFUK, Bratislava: 2001, s. 308.ISBN 80-7160-146-2.
- STRÁŽNICKÁ, Viera. *Medzinárodná a európska ochrana ľudských práv*. Bratislava: Paneurópska vysoká škola, 2013, 559 s. ISBN 9788089447954.
- ŠUŠNJAR, Davor. *Proportionality, fundamental rights, and balance of powers*. Leiden: Martinus Nijhoff Publishers, 2010, xxxiv, 389 s. ISBN 978-90-04-18286-8.
- WAGNEROVÁ Eliška; ŠIMÍČEK Vojtěch; LANGÁŠEK Tomáš; POSPÍŠIL Ivo. *Listina základních práv a svobod: komentář*. Vyd. 1. Praha: Wolters Kluwer Česká republika, 2012, xxv, 906 s. Komentáře (Wolters Kluwer ČR). ISBN 9788073577506.

b) Odborné články

- CANNATACI, Joseph A. a Jeanne Pia MIFSUD-BONNICI. Data Protection Comes of Age: The Data Protection Clauses in the European Constitutional Treaty. *Information & Communications Technology Law* [online]. 2005, roč. 14, č. 1, s. 5-15 [cit. 2015-12-01]. DOI: 10.1080/136008304200032527 4. ISSN 1360-0834. Dostupné z: http://www.tandfonline.com/doi/abs/10.1080/1360083042000325274
- DE HERT, Paul a Serge GUTWIRTH. Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In: GUTWIRTH, Serge ; POULLET, Yves; P. DE HERT, Paul (eds.). *Reinventing data protection*? Springer Science, Dordrecht, 2009, s. 3-44. ISBN 978-1-4020-9498-9.

- KOKOTT, Juliane a Christoph SOBOTTA. The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law.* 2013, roč. 3, č. 4, s. 222–228.
- LEMMENS, Paul. Relations between the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights - Substantive Aspects.*Maastricht J. Eur. & Comp. L.* 2001, vol. 8, p. 49 – 67. ISSN 1023-263X.
- LYNSKEY, Orla. Deconstructing Data Protection: The "Added-Value" Of A Right To Data Protection In The Eu Legal Order. *International and Comparative Law Quarterly* [online]. 2014, vol. 63, no.03, p. 569–597 [cit. 26.11.2015]. DOI: 10.1017/S0020589314000244. Dostupné z: http://www.journals.cambridge.org/abstract_S0020589314000244
- ROUVROY, Antoinette a Yves POULLET. The right to informational self-determination and the value of self-development. Reassessing the importance of privacy for democracy. In: GUTWIRTH, Serge ; POULLET, Yves; P. DE HERT, Paul (eds.). *Reinventing data protection*? Springer Science, Dordrecht, 2009, s. 3-44. ISBN 978-1-4020-9498-9.
- SOLOVE, Daniel J. A Taxonomy of Privacy. *University of Pennsylvania Law Review.* 2006, roč. 154, č. 4, s. 477-560. ISSN 0041-9907.
- WARREN, Samuel D. and BRANDEIS, Louis D. The Right to Privacy. *Harvard Law Review* [online]. 15.12.1890, Vol. 4, no. 5, p. 193. [cit. 30.11.2015]. Dostupné z: http://www.jstor.org/stable/1321160?origin=crossref

c) Legislatívne dokumenty

- ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 02/2013 on apps on smart devices* [online]., 00461/13/EN, WP 202, Adopted on 27 February 2013 [cit. 30.11.2015]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf.
- *B. Osobitná časť* [online]. Úrad vlády SR [cit. 30.11.2015]. Dostupné z: http://www.rokovania.sk/File.aspx/ViewDocumentHtml/Mater-Dokum-179362?prefixFile=m
- *Dohoda o elektronickom doručovaní uzatvorená podľa §13 ods.5 zákona č. 563/2009 Z.z. v znení neskorších predpisov* [online]. Portál ďanovej správy SR (archivovaná stránka) [cit. 30.11.2015]. Dostupné z: http://www.drsr.sk/drsr/slovak/el_komunikacia/data/dohoda_563.doc
- *Dohoda o spôsobe doručovania písomností doručovaných elektronickými prostriedkami, ktoré nebudú podpísané zaručeným elektronickým podpisom uzatvorená podľa § 20 ods. 8 zákona č. 511/1992 Zb. v znení neskorších predpisov*[online]. Portál ďanovej správy SR (archivovaná stránka) [cit. 30.11.2015]. Dostupné z: https://web.archive.org/web/20111225023652/http://www.drsr.sk/drsr/slovak/el_komunikacia/dohoda_ek.pdf
- *Dôvodová správa* [online]. Vládny návrh zákona o jednotnom informačnom systéme v cestnej doprave a o zmene a doplnení niektorých zákonov, Parlamentná tlač 1721, Národná rada SR [cit. 30.11.2015]. Dostupné z: http://www.nrsr.sk/web/Dynamic/Download.aspx?DocID=418206

- *Dôvodová správa* [online]. Vládny návrh zákona o nadobúdaní vlastníctva poľnohospodárskeho pozemku a o zmene a doplnení niektorých zákonov, Parlamentná tlač 977, Národná rada SR [cit. 30.11.2015]. Dostupné z: https://www.nrsr.sk/web/Default.aspx?sid=zakony/zakon&MasterID=4919
- *Dôvodová správa* [online]. Vládny návrh zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, Parlamentná tlač 358, Národná rada SR [cit. 30.11.2015]. Dostupné z: https://www.nrsr.sk/web/Default.aspx?sid=zakony/cpt&ZakZborID=13&CisObdobia=6&ID=358
- Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. *European Treaty Series - No. 108* [online]. Council of Europe, 1981. [cit. 25.11.2015]. Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434
- Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. *European Treaty Series - No. 108* [online]. Council of Europe, 1981. [cit. 25.11.2015]. Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434
- *Návrh na začatie konania na preskúmanie súladu zákona č. 140/2014 Z.z.* [online]. Vyhľadávanie rozhodnutí, Ústavný súd SR [cit. 30.11.2015]. Dostupné z: http://portal.concourt.sk/SearchRozhodnutia/podanie.do?id_spisu=541607
- *Návrh zákona* [online]. Vládny návrh zákona o jednotnom informačnom systéme v cestnej doprave a o zmene a doplnení niektorých zákonov, Parlamentná tlač 1721, Národná rada SR [cit. 30.11.2015]. Dostupné z: http://www.nrsr.sk/web/Dynamic/Download.aspx?DocID=418206
- *Pozmeňujúce a doplňujúce návrhy* [online]. Vládny návrh zákona o jednotnom informačnom systéme v cestnej doprave a o zmene a doplnení niektorých zákonov, Parlamentná tlač 1721, Národná rada SR [cit. 30.11.2015]. Dostupné z: https://www.nrsr.sk/web/Dynamic/Download.aspx?DocID=421654
- *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market(COM/2012/0238)* [online] In: *EUR-lex* [on-line informačný systém]. 2012,European Union [cit. 25.11.2015]. Dostupné z: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52012PC0238
- *Report from the Commission to the European Parliament and the Council - Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures (COM/2006/0120)* [online] In: *EUR-lex* [on-line informačný systém]. 2006,European Union [cit. 25.11.2015]. Dostupné z: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52006DC0120
- Smernica Rady 2008/117/ES, zo 16. decembra 2008, ktorou sa mení a dopĺňa smernica 2006/112/ES o spoločnom systéme dane z pridanej hodnoty s cieľom bojovať proti daňovým podvodom spojeným s transakciami v rámci Spoločenstva. Dostupné z: http://eur-

lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:014:0007:0009:SK:PDF

- *Vyhodnotenie medzirezortného pripomienkového konania* [online]. Úrad vlády SR [cit. 30.11.2015]. Dostupné z: http://www.rokovania.sk/File.aspx/ViewDocumentHtml/Mater-Dokum-22181?prefixFile=m
- *Vzesené pripomienky v rámci medzirezortného pripomienkového konania - Návrh zákona o jednotnom informačnom systéme v cestnej doprave a o zmene a doplnení niektorých zákonov* [online] Úrad vlády SR [cit. 30.11.2015]. Dostupné z: http://www.rokovania.sk/File.aspx/Index/Mater-Dokum-190765
- *Zverejnenie rozhrania pre prenos údajov z identifikačného zariadenia do JISCD* [online]. JEDNOTNÝ INFORMAČNÝ SYSTÉM V CESTNEJ DOPRAVE, © MDVaRR SR [cit. 30.11.2015]. Dostupné z: http://www.e-doprava.sk/prenos-udajov.html

d) Ostatné dokumenty

- *„Jednotný informačný systém v cestnej doprave – Elektronické služby v doprave (JISCD-ESD)"*[online] JEDNOTNÝ INFORMAČNÝ SYSTÉM V CESTNEJ DOPRAVE, © MDVaRR SR [cit. 30.11.2015]. Dostupné z: http://www.e-doprava.sk/index.html
- *eDane – Používateľská príručka* [online]. Portál ďanovej správy SR (archivovaná stránka) [cit. 30.11.2015]. Dostupné z: https://web.archive.org/web/20120509075851/http://edane.drsr.sk/install/pouziv_prirucka_edane.pdf
- AKANDJI-KOMBE, Jean-François. *Positive obligations under the European Convention on Human Rights: A guide to the implementation of the European Convention on Human Rights*[online]. Human rights handbooks, No. 7, Council of Europe, 1st printing, 2007 [cit. 30.11.2015]. Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168007ff4d
- *Aplikácia eDane* [online]. Finančná správa SR (archivovaná stránka) [cit. 30.11.2015]. Dostupné z: https://web.archive.org/web/20140625051318/https://www.financnasprava.sk/sk/elektronicke-sluzby/elektronicka-komunikacia/elektronicka-komunikacia-dane/edane
- *Certifikácia produktov* [online]. Elektronický podpis, Národný bezpečnostný úrad [cit. 30.11.2015]. Dostupné z: http://www.nbusr.sk/sk/elektronicky-podpis/certifikacia-produktov.1.html.
- *Certifikované produkty pre používateľov* [online]. Elektronický podpis – Zoznam ceritifkovaných produktov, Národný bezpečnostný úrad [cit. 30.11.2015]. Dostupné z: *http://www.nbusr.sk/sk/elektronicky-podpis/certifikacia-produktov.1.html*
- *Čo je OPIS?* [online] Informatizácia.sk, Ministerstvo financií SR, aktualizované 30.04.2014 [cit. 30.11.2015]. Dostupné z: http://www.informatizacia.sk/co-je-opis-/1865s
- *Čo je to eTax* [online]. Portál ďanovej správy SR (archivovaná stránka) [cit. 30.11.2015]. Dostupné z:

https://web.archive.org/web/20041022095418/http://www.drsr.sk/wps/doc/sk/etax/about.html

- *Digital Signing Now Possible on Android Smartphones and Tablets* [online]. News, Mobiil-Id, ID.ee [cit. 01.12.2015]. Dostupné z: http://id.ee/?id=30607&read=33976
- DOWTY, Terri a Douwe KORFF. *Protecting The Virtual Child: The Law and Children's Consent to Sharing Personal Data*[online]. Action on Rights for Children, 2009 [cit. 30.11.2015]. Dostupné z: https://www.northumbria.ac.uk/static/5007/hces/virtual_child.pdf
- *E-government benefits study*. Canberra: NOIE, 2003. ISBN 1740820258. Dostupné z: http://www.finance.gov.au/agimo-archive/__data/assets/file/0012/16032/benefits.pdf
- *eID klient už aj pre Mac a Linux* [online]. Oznamy, Slovensko.sk – ústredný portál verejných služieb ľuďom, vydané 30.06.2015 [cit. 30.11.2015]. Dostupné z: https://www.slovensko.sk/sk/oznamy/detail/_eid-klient-uz-aj-pre-mac-a-lin
- *Elektronické podávanie dokumentov*[online]. Finančná správa SR (archivovaná stránka) [cit. 30.11.2015]. Dostupné z: https://web.archive.org/web/20121222105746/http://www.drsr.sk/wps/portal/vyplnenie_tlaciv
- *EZU/eTax* [online]. Finančná správa SR (archivovaná stránka) [cit. 30.11.2015]. Dostupné z:https://web.archive.org/web/20120509075757/https://esluzby.drsr.sk/
- GREENWALD, Glen, POITRAS, Laura, MACASKILL, Ewen. *Edward Snowden: the whistleblower behind the NSA surveillance revelations | US news.* [online]. The Guardian, 11.06.2013. [cit. 30.11.2015]. Dostupné z: http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance
- *Informačný systém kontrolných známok* [online]. Spotrebné dane,Finančná správa SR [cit. 30.11.2015]. Dostupné z: https://www.financnasprava.sk/sk/podnikatelia/dane/spotrebne-dane/iskz
- KERN, Miro. Štátna aplikácia na alkohol a cigarety sleduje ľudí, nechtiac môžete skončiť na súde. *Denník N* [online]. N press s.r.o., vydané 11.05.2015 [cit. 30.11.2015]. Dostupné z: https://dennikn.sk/101517/aplikacia-od-statu-ohrozuje-sukromie-ludi/
- KOLLÁROVÁ, Zuzana. 6 rád ako vybaviť e-občiansky a elektronický podpis. *Trend.sk* [online]. © 2015 News and Media Holding, vydané 23.07.2015 [cit. 1.12.2015]. Dostupné z: http://www.etrend.sk/financie/6-rad-ako-komunikovat-s-uradmi-online.html
- KRAJANOVÁ, Daniela. Tlačiareň v Kremnici môže tlačiť superkolky. *SME.sk* [online]. Petit Press, a.s., vydané 09.10.2014 [cit. 30.11.2015]. Dostupné z: http://ekonomika.sme.sk/c/7430410/tlaciaren-v-kremnici-moze-tlacit-superkolky.html
- KRÁĽ, Milan. Vodičské kurzy budú len pod dohľadom satelitu. *Pravda.sk*[online]. PEREX, a.s., vydané 29.07.2015 [cit. 30.11.2015]. Dostupné z: http://spravy.pravda.sk/domace/clanok/362857-vodicske-kurzy-len-pod-dohladom-satelitu/
- *Na stiahnutie* [online]. Slovensko.sk – ústredný portál verejných služieb ľuďom [cit. 30.11.2015]. Dostupné z: https://www.slovensko.sk/sk/na-stiahnutie
- *Náhradná strán*ka [online]. Portál ďanovej správy SR (archivovaná stránka) [cit. 30.11.2015].

Dostupné z: https://web.archive.org/web/20100629161805/http://www.drsr.sk/nahradnaStranka.html

- *Národný projekt: Jednotný informačný systém v cestnej doprave - Elektronické služby v doprave* [online] Informatizácia.sk, Ministerstvo financií SR [cit. 30.11.2015]. Dostupné z: http://www.informatizacia.sk/vdok_simple-np--jis-v-cd_esd/609s15519c
- *Návrh na začatie konania na preskúmanie súladu zákona č. 140/2014 Z.z.* [online]. Vyhľadávanie rozhodnutí, Ústavný súd SR [cit. 30.11.2015]. Dostupné z: http://portal.concourt.sk/SearchRozhodnutia/podanie.do?id_spisu=541607
- NBÚ nemá problém certifikovať elektronický podpis pre iné systémy. *IT NEWS*[online]. Digital Visions, spol. s.r.o., vydané 19.04.2010 [cit. 30.11.2015]. Dostupné z: http://www.itnews.sk/spravy/informatizacia/2010-04-19/c133141-nbu-nema-problem-certifikovat-elektronicky-podpis-pre-ine-systemy
- *Od decembra 2013 vydáva Slovenská republika elektronické občianske preukazy - eID karty* [online]. Tlačové správy, Ministerstvo vnútra SR [cit. 01.12.2015]. Dostupné z: http://www.minv.sk/?tlacove-spravy&sprava=od-decembra-2013-vydava-slovenska-republika-elektronicke-obcianske-preukazy-eid-karty
- *Odmietol Windows. Zažaloval štát, teraz čiastočne vyhral* [online]. Súdy a občianska spoločnosť, European Information Society Institute [cit. 30.11.2015]. Dostupné z: http://www.eisionline.org/index.php/sk/projekty-m-2/sudy-a-obcianska-spolocnost-m/63-eura-prvystupen
- *Odpoveď Daňového riaditeľstva na žiadosť o sprístupnenie informácií*. č. I/252/9847 68834/2010/Mal [online]. [cit. 30.11.2015]. Dostupné z: https://drive.google.com/file/d/0B8BvNOtIa2woakZMdXVTMGdndlk/view?usp=sharing
- *Odpoveď na predžalobnú výzvu o upustenie od protiprávneho konania.* č. 31761/2004 [online]. Vytvorené 08.12.2014 [cit. 01.12.2015]. Dostupné z: https://drive.google.com/file/d/0B8BvNOtIa2woVEV2bTNjb3JlUlU/view?usp=sharing
- *Overenie splnenia podmienok AES* [online]. Elektronické služby,Finančná správa SR [cit. 30.11.2015]. Dostupné z https://www.financnasprava.sk/sk/elektronicke-sluzby/verejne-sluzby/overenie-splnenia-podmienok-pr
- *Oznámenie k elektronickému doručovaniu*[online]. Finančná správa SR (archivovaná stránka) [cit. 30.11.2015]. Dostupné z: https://web.archive.org/web/20130120014231/http://drsr.sk/wps/portal
- *Podmienky využívania Autorizovaných elektronických služieb* [online]. Portál ďanovej správy SR (archivovaná stránka) [cit. 30.11.2015]. Dostupné z: https://web.archive.org/web/20100130190453/http://www.drsr.sk/wps/portal/podmienky_aes
- *Postup inštalácie offline aplikácie Súhrnný výkaz [*online]. Portál ďanovej správy SR (archivovaná stránka) [cit. 30.11.2015]. Dostupné z: https://web.archive.org/web/20100821060021/http://podajdp.drsr.sk/PostupInstalacieOfflineAplikSV.pdf
- *Superkolky* [online] Google Play, © 2015 Google [cit. 30.11.2015]. Dostupné z:

https://play.google.com/store/apps/details?id=sk.financnasprava.superkolky

- *Superkolky* [online]. Archív noviniek, Finančná správa SR, 24.03.2015[cit. 30.11.2015]. Dostupné z: https://www.financnasprava.sk/sk/pre-media/novinky/archiv-noviniek/detail-novinky/_superkolky-na
- *Štát zanedbal otvorené štandardy, podnikateľ ho teraz žaluje.* Súdy a občianska spoločnosť, European Information Society Institute [cit. 30.11.2015]. Dostupné z: http://www.eisionline.org/index.php/sk/projekty-m-2/sudy-a-obcianska-spolocnost-m/33-podnikatel-zaluje-stat
- Za povinný Windows môže podľa daňového riaditeľstva NBÚ. *IT NEWS* [online]. Digital Visions, spol. s.r.o., vydané 16.04.2010 [cit. 30.11.2015]. Dostupné z: http://www.itnews.sk/spravy/software/2010-04-16/c133109-za-povinny-windows-moze-podla-daneveho-riaditelstva-nbu?ref=rss
- *Zaslanie odborného stanoviska.* č. 3856/2010/KÚ/SOdOP-007[online]. Vytovrené 16.06.2010 [cit. 30.11.2015]. Dostupné z: https://drive.google.com/file/d/0B8BvNOtIa2wodjVFNzF3SDZaeVE/view

Právne predpisy

a) Slovenská republika

- Ústava SR, č. 460/1992 Zb.
- Zákona č. 222/2004 Z.z., o dani z pridanej hodnoty.
- Zákon č. 530/2011 Z.z., o spotrebnej dani z alkoholických nápojov.
- Zákon č. 106/2004 Z.z., o spotrebnej dani z tabakových výrobkov.
- Zákon č. 1/1993 Z.z. o Zbierke zákonov SR
- Zákon č. 250/2007 Z.z. o ochrane spotrebiteľa.
- Zákon č. 275/2006Z.z. o informačných systémoch verejnej správy.
- Zákon č. 122/2013 Z.z, o ochrane osobných údajov.
- Zákon č. 333/2011 Z.z., o orgánoch štátnej správy v oblasti daní, poplatkov a colníctva.
- Vyhláška č. 256/2014 Z.z. Ministerstva financií SR z 18. septembra 2014 o označovaní balení kontrolných známok určených na označovanie spotrebiteľského balenia liehu a o oznamovaní a zverejňovaní údajov o týchto kontrolných známkach.
- Vyhláška č. 252/2014 Z.z. Ministerstva financií SR z 10. septembra 2014, ktorou sa ustanovujú náležitosti, vyhotovenie a cena kontrolnej známky určenej na označovanie spotrebiteľského balenia liehu.
- Vyhláška č. 120/1976 Zb. ministra zahraničných vecí z 10. mája 1976 o Medzinárodnom pakte o občianskych a politických právach a Medzinárodnom pakte o hospodárskych, sociálnych a kultúrnych právach.
- Oznámenie č. 49/2001 Z. z. Ministerstva zahraničných vecí SR o ochrane jednotlivcov pri

automatizovanom spracovaní osobných údajov.

b) Európska únia

- Smernica Rady 2008/117/ES, zo 16. decembra 2008, ktorou sa mení a dopĺňa smernica 2006/112/ES o spoločnom systéme dane z pridanej hodnoty s cieľom bojovať proti daňovým podvodom spojeným s transakciami v rámci Spoločenstva.
- Smernica Európskeho Parlamentu a Rady 1999/93/ES z 13. decembra 1999 o rámci spoločenstva pre elektronické podpisy.
- Smernica Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov.
- Nariadenie Európskeho parlamentu a Rady 910/2014 zo dňa 23.6.2014 o elektronickej identifikácii a službách dôvery pre elektronické transakcie na vnútornom trhu.

c) Rada Európy

- Charta základných práv Európskej únie, 2010/C 83/02.

d) Ostatné

- Všeobecná deklarácia ľudských práv.

Rozhodnutia súdov

a) Európsky súd pre ľudské práva

- Rozsudok S a Marper proti Spojenému kráľovstvu (č. 30562/04 a 30566/04).
- Rozsudok Peck proti Spojenému kráľovstvu (č. 44647/98).
- Rozsudok P.G. a J.H proti Spojenému kráľovstvu(č. 44787/98).
- Friedl proti Rakúsku (Prípad č. 28/1994/475/556) - *Európska komisia pre ľudské práva.*
- Özgür Gündem v Turecko (č. 23144/93).
- Dink v. Turecko (č. 2668/07).
- Broniowski v Poľsko (č. 31443/96).
- Amann proti Švajčiarsku (č. 27798/95).
- Klass a ostatní proti Nemecku (č. 5029/71).
- Kopp proti Švajčiarsku (Prípad č. 13/1997/797/1000).
- Leander proti Švédsku (č. 9248/81).
- The Sunday Times proti Spojenému kráľovstvu (č. 6538/74).
- Weber a Saravia proti Nemecku (č. 54934/00).

- M.N. a ostatní proti San Marínu (č. 28005/12).

b) Súdny dvor Európskej únie

- Rozsudok Súdneho dvora EÚ, vo veci C-92/09 a C-93/09, Volker und Markus Schecke.
- Rozsudok Súdneho dvora EÚ, veci C-465/00, C-138/01 a C-139/01 (Österreichier Rundfunk).

c) Ústavný súd SR

- Nález Ústavného súdu SR, sp. zn. III. ÚS 100/02.
- Nález Ústavného súdu SR, sp. zn. III. ÚS 88/01.
- Nález Ústavného súdu SR,sp. zn. I. ÚS 33/95.
- Nález Ústavného súdu SR sp. zn. II. ÚS 8/97.
- Nález Ústavného súdu SR, sp. zn.PL. ÚS 29/05-161.
- Nález Ústavného súdu SR, sp.zn. PL. ÚS 19/98.
- Nález Ústavného súdu SR, sp.zn. PL. ÚS 29/05.
- Nález Ústavného súdu SR, sp. zn. II. ÚS 59/97.
- Nález Ústavného súdu SR, sp. zn. I. ÚS 4/02.
- Nález Ústavného súdu SR, sp. zn. PL. US 23/06.
- Nález Ústavného súdu SR, sp. zn. II. ÚS 19/97.
- Nález Ústavného súdu SR, sp. zn. PL. ÚS 10/2014.
- Nález Ústavného súdu SR, sp. zn. III. ÚS 204/02.
- Nález Ústavného súdu SR, sp. zn. I. ÚS 290/2015.
- Nález Ústavného súdu SR, sp. zn. II. ÚS 53/2010.
- Nález Ústavného súdu SR, sp. zn. I. ÚS 114/2012.
- Nález Ústavného súdu SR, sp. zn. PL. ÚS 140/2014.
- Nález Ústavného súdu SR, sp. zn. PL. US 3/09-378.

d) Najvyšší súd SR

- Rozhodnutie Najvyššieho súdu, sp. zn. 5Sžf/19/2009.

d) Ostatné

- Rozhodnutie Ústavného súdu Juhoafrickej republiky, Štát proti Bhulwana, 1996 (1) SA 388.

Vydal	European Information Society Institute, o.z.
Názov	Digitálna verejná správa a ľudské práva
Autori	Mgr. Matej Gera, LL.M. (Kapitola 1., 2., 3.2., 4.)
	Mgr. Martin Husovec (Kapitola 3.1.)
	Štefan Szilva (Kapitola 2.1., 2.2.)
	Mgr. Petra Zabuďková, LL.M. (Časť Exkurz)
Recenzoval	JUDr. Jakub Harašta

Prvé vydanie, náklad 200ks, strán 86.

European Information Society Institute o.z. (http://eisionline.org), december, 2015.

ISBN 978-80-971307-3-2 (tlač)

ISBN 978-80-971307-4-9 (pdf)