SLOVENSKÁ REPUBLIKA

NÁLEZ

Ústavného súdu Slovenskej republiky

V mene Slovenskej republiky

PL. ÚS 25/2019-117

Ústavný súd Slovenskej republiky v pléne zloženom z predsedu Ivana Fiačana a zo sudcov Jany Baricovej, Ladislava Duditša, Libora Duľu, Miroslava Duriša (sudca spravodajca), Rastislava Kaššáka, Jany Laššákovej, Miloša Maďara, Petra Molnára, Petra Straku, Roberta Šorla, Ľuboša Szigetiho a Martina Vernanského o návrhu **skupiny 33 poslancov Národnej rady Slovenskej republiky** na začatie konania podľa čl. 125 ods. 1 písm. a) Ústavy Slovenskej republiky o súlade ustanovení § 8 ods. 1 písm. b) a g) a § 8a ods. 1 v časti „daňové identifikačné číslo“ a v časti „unikátny identifikátor kupujúceho, ak je predložený kupujúcim pred zaevidovaním prijatej tržby“ zákona č. 289/2008 Z. z. o používaní elektronickej registračnej pokladnice a o zmene a doplnení zákona Slovenskej národnej rady č. 511/1992 Zb. o správe daní a poplatkov a o zmenách v sústave územných finančných orgánov v znení neskorších predpisov v znení neskorších predpisov s čl. 16 ods. 1, čl. 19 ods. 2 a 3 Ústavy Slovenskej republiky, čl. 8 Dohovoru o ochrane ľudských práv a základných slobôd a čl. 7, čl. 8 a čl. 52 ods. 1 Charty základných práv Európskej únie za účasti vlády Slovenskej republiky ako vedľajšieho účastníka konania takto

r o z h o d o l :

1. Ustanovenie § 8a ods. 1 zákona č. 289/2008 Z. z. o používaní elektronickej registračnej pokladnice a o zmene a doplnení zákona Slovenskej národnej rady č. 511/1992 Zb. o správe daní a poplatkov a o zmenách v sústave územných finančných orgánov v znení neskorších predpisov v časti *„unikátny identifikátor kupujúceho, ak je predložený kupujúcim pred zaevidovaním prijatej tržby“* **n i e j e v s ú l a d e** s čl. 16 ods. 1, čl. 19 ods. 2 a 3 Ústavy Slovenskej republiky.

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

O d ô v o d n e n i e :

I.
Návrh na začatie konania o súlade právnych predpisov

1. Ústavnému súdu bol 17. septembra 2019 doručený návrh navrhovateľov na začatie konania podľa čl. 125 ods. 1 písm. a) Ústavy Slovenskej republiky (ďalej len „ústava“) o súlade ustanovení

§ 8 ods. 1 písm. b) a g) a § 8a ods. 1 v časti „daňové identifikačné číslo“ (ďalej aj „DIČ“) a v časti „unikátny identifikátor kupujúceho (ďalej aj „UIK“), ak je predložený kupujúcim pred zaevidovaním prijatej tržby“ zákona č. 289/2008 Z. z. o používaní elektronickej registračnej pokladnice a o zmene a doplnení zákona Slovenskej národnej rady č. 511/1992 Zb. o správe daní a poplatkov a o zmenách v sústave územných finančných orgánov v znení neskorších predpisov v znení neskorších predpisov (ďalej aj „ZoERP“) s čl. 16 ods. 1, čl. 19 ods. 2 a 3 ústavy, čl. 8 Dohovoru o ochrane ľudských práv a základných slobôd (ďalej len „dohovor“) a čl. 7, čl. 8 a čl. 52 ods. 1 Charty základných práv Európskej únie (ďalej len „charta“) .

2. Ústavný súd uznesením č. k. PL. ÚS 25/2019-33 z 18. decembra 2019 prijal na ďalšie konanie návrh navrhovateľov v celom rozsahu.

3. Navrhovatelia vo svojom návrhu napádajú ustanovenia § 8 ods. 1 písm. b) a g) a § 8a ods. 1 v časti „daňové identifikačné číslo“ a v časti „unikátny identifikátor kupujúceho, ak je predložený kupujúcim pred zaevidovaním prijatej tržby“ zákona č. 289/2008 Z. z. o používaní elektronickej registračnej pokladnice a o zmene a doplnení zákona Slovenskej národnej rady č. 511/1992 Zb. o správe daní a poplatkov a o zmenách v sústave územných finančných orgánov v znení neskorších predpisov v znení neskorších predpisov (ďalej aj „napadnuté ustanovenia“) ako súčasť právnej úpravy tzv. systému *e-kasa* (ďalej len „e-kasa“).

4. Námietky navrhovateľov k sporným právnym predpisom možno rozdeliť do týchto oblastí:

I.1. Namietaný nesúlad s právom na nedotknuteľnosť súkromia a právom na ochranu pred neoprávneným zasahovaním do súkromného a rodinného života:

5. V tejto časti návrhu navrhovatelia napádajú nesúlad napadnutých ustanovení s čl. 16 ods. 1, čl. 19 ods. 2 ústavy, čl. 8 dohovoru, čl. 7 a čl. 52 ods. 1 charty.

6. Navrhovatelia o. i. argumentujú tým, že *«4 Ustanovenia § 8 ods. 1 a § 8a ods. 1 Zákona ustanovujú povinnosť podnikateľa pri evidovaní tržieb v pokladnici e-kasa klient zabezpečiť odovzdávanie orgánom verejnej moci veľkého rozsahu osobných údajov o kupujúcich širokého spektra produktov a služieb. Spracúvanie a poskytovanie niektorých z týchto údajov, či už jednotlivo alebo v spojení s inými údajmi, môže, a za istých okolností bude, predstavovať citeľný zásah do osobnej sféry dotknutých osôb.*
Navrhovatelia sú presvedčení, že takto Zákonom predpísaný zber údajov, ako aj ich odovzdávanie orgánom verejnej správy, je neproporcionálny a neodôvodnený, keďže uvedený Zákonom deklarovaný cieľ je možné dosiahnuť aj bez toho, aby z elektronických registračných pokladníc boli odovzdávané údaje v uvedenom neprimeranom rozsahu a uvedeným neprimeraným spôsobom...
7 V ustanovení § 8a ods. 1 Zákona je tak stanovená povinnosť podnikateľa do systému e- kasa zasielať nielen rozsiahle množstvo údajov týkajúcich sa podnikateľa, ale aj široký rozsah údajov týkajúcich sa osôb, ktoré s podnikateľom vstupujú do záväzkových vzťahov (v jazyku Zákona a nižšie tiež „kupujúcich“). Na povinnosť spracúvať a ďalej poskytovať takéto neprimerane rozsiahle množstvo osobných údajov však podľa navrhovateľov neexistuje žiadny legitímny dôvod. Ako je naznačené už vyššie v tomto návrhu, spracúvanie a poskytovanie niektorých z týchto údajov či už jednotlivo alebo v spojení s inými údajmi, môže predstavovať citeľný zásah do osobnej sféry dotknutých osôb...

19 Zavedenie povinnosti poskytovať údaje podľa napadnutých ustanovení predstavuje citeľný zásah do súkromného života dotknutých osôb. ZoERP nespĺňa požiadavky kladené na takýto druh zásahu, a to jednak z dôvodu, že poskytovanie uvedených údajov nie je odôvodnené a tiež z dôvodu, že v ZoERP absentuje vymedzenie dostatočných záruk proti zneužitiu informácií o súkromí jednotlivcov. Zo Zákona pritom nie je zrejmé ani to, či k takto získaným údajom, ktoré sa stanú súčasťou informačných systémov Finančnej správy SR, majú prístup len samotné zložky Finančnej správy SR, alebo aj iné osoby. Ide teda o získavanie a spracúvanie osobných údajov v miere, ktorá porušuje základné ľudské práva a slobody chránené medzinárodnými dokumentárni a Ústavou SR.».

7. Navrhovatelia preto uzavreli, že napadnuté ustanovenia sú v rozpore s čl. 16 ods. 1, čl. 19 ods. 2 ústavy, čl. 8 dohovoru, čl. 7 a čl. 52 ods. 1 charty. Na základe uvedeného navrhli, aby ústavný súd rozhodol, že napadnuté ustanovenia nie sú v súlade s príslušnými referenčnými normami.

I.2. Namietaný nesúlad s právom na ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe:

8. V tejto časti návrhu navrhovatelia napádajú nesúlad napadnutých ustanovení s čl. 19 ods. 3 ústavy, čl. 8 a čl. 52 ods. 1 charty.

9. Navrhovatelia o. i. argumentujú tým, že *„5 Navrhovatelia tiež majú za to, že nie sú stanovené dostatočné záruky proti možnosti zneužitia údajov, ktoré sa postupmi stanovenými Zákonom dostanú do dispozície podnikateľa v jeho elektronickej registračnej pokladnici, a tým aj do dispozície štátu...*
20 Z údajov identifikujúcich konkrétnych kupujúcich a z údajov o nimi nakúpených tovaroch a službách je možné vyčítať každodenné návyky konkrétnych kupujúcich, ich sociálne postavenie a finančné možnosti (podľa ceny tovaru alebo služby), údaje týkajúce sa ich zdravotného stavu (napríklad podľa údajov o nákupe liekov), náboženské zameranie (podľa nákupu tovarov s náboženskou témou) alebo údaje o intímnom živote týchto ľudí (podľa nákupu tovarov alebo služieb intímneho charakteru). Ak sú tieto údaje navyše kombinované s ďalšími údajmi, ktoré majú orgány verejnej moci k dispozícii (napr. údaje o podnikaní, uzavretí manželstva, evidencií motorových vozidiel), je možné vytvoriť prehnane presný profil jednotlivca...
23 Uvedené riziká sú najviac reálne pri technológiách, ktoré v rámci svojej činnosti zbierajú a uchovávajú veľké množstvo údajov. Takouto technológiou je aj systém e-kasa, ktorého esenciálnou súčasťou je prenos a spracúvanie obrovského množstva (osobných) údajov v reálnom čase. Algoritmické spracúvanie osobných údajov tiež môže generovať nové korelácie medzi informáciami týkajúcimi sa identifikovaných kupujúcich a informáciami, ktoré už orgány verejnej moci majú k dispozícii. Výsledkom takéhoto spracúvania osobných údajov môžu byť tiež skupinové profily jednotlivých vrstiev obyvateľstva.“.

10. Navrhovatelia preto uzavreli, že napadnuté ustanovenia sú v rozpore s čl. 19 ods. 3 ústavy, čl. 8 a čl. 52 ods. 1 charty. Na základe uvedeného navrhli, aby ústavný súd rozhodol, že napadnuté ustanovenia nie sú v súlade s príslušnými referenčnými normami.

II.
Stanoviská účastníkov konania a vedľajšieho účastníka a ďalší priebeh konania

II.1. Stanovisko Národnej rady Slovenskej republiky:

11. Národná rada Slovenskej republiky (ďalej len „národná rada“) vo svojom stanovisku č. PREDS-11/2020 z 12. júla 2020 uviedla, že súhlasí s upustením od ústneho pojednávania a nebude zaujímať stanovisko k predmetnej veci.

II.2. Stanovisko vlády Slovenskej republiky:

12. Vláda Slovenskej republiky zastúpená Ministerstvom spravodlivosti Slovenskej republiky (ďalej len „vláda“) vo svojom stanovisku č. 03206/2020/100 z 10. februára 2020 o. i. uviedla, že *«Zákon č. 289/2008 Z. z. upravuje povinnosti podnikateľov, t. j. predajcov tovaru a poskytovateľov služieb pri evidencii prijatých tržieb a výrobcov, distribútorov a predajcov pokladníc a neustanovuje žiadne povinnosti pre kupujúcich.*
Daňové identifikačné číslo DIČ je prideľované daňovému subjektu správcom dane na účely jeho jednoznačnej identifikácie a z dôvodu eliminovania potreby spracúvania iných osobných údajov, vrátane rodného čísla a dátumu narodenia v prípade fyzických osôb, teda účelom jeho existencie je aj ochrana osobných údajov, čo je jednoznačným dôvodom pre posúdenie takéhoto spracúvania osobných údajov ako primeraného a proporcionálneho, eliminujúceho väčší rozsah štátneho zásahu, avšak umožňujúci jednoznačnú identifikáciu podnikateľa pre finančnú správu, čo opodstatňuje záver o nevyhnutnosti spracúvania tohto údaja. I keď DIČ je osobným údajom podľa § 2 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „zákon č. 18/2018 Z. z.“), funkciu identifikovateľnosti osoby plní len vo vzťahu k finančnej správe, prípadne vo vzťahu k inému oprávnenému spracúvateľovi tohto údaja. Účel jeho existencie a spracúvania je vymedzený prioritne daňovými predpismi, pričom zákon č. 289/2008 Z. z. rozšíril jeho používanie aj na účely evidencie prijatej tržby, čím právna norma spĺňa požiadavky na zákonnosť právnej úpravy.
Nevyhnutnosť spracúvania údajov je daná aj z dôvodu, že doklady z elektronickej registračnej pokladnice (ďalej len „ERP“), ako aj z PEKK (pokladnica e-kasa klient, pozn.) *štandardne plnia aj funkciu faktúry podľa zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov (ďalej len „zákon č. 222/2004 Z. z.“) a zároveň aj funkciu podkladu k vyhotoveniu účtovného dokladu podľa zákona č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov (ďalej len „zákon o účtovníctve“), a teda aj dokladu posudzovaného na účely zákona č. 595/2003 Z. z. o dani z príjmov.*
Ustanovenia § 8 ods. 1 písm. b) a g) zákona č. 289/2008 Z. z. upravujú obsahové náležitosti pokladničného dokladu vyhotoveného ERP. Toto ustanovenie nenadväzuje na ustanovenie § 8a ods. 1 zákona č. 289/2008 Z. z., ktoré upravuje rozsah údajov zasielaných do systému e-kasa, pretože z ERP nie sú zasielané údaje do systému e-kasa, pretože ERP so systémom e-kasa nie je prepojená.
V ustanovení § 8a ods. 1 je použitá odvolávka len na ustanovenia § 8 ods. 1 písm. g) z dôvodu, aby nebol tento údaj uvádzaný v zákone duplicitne, ak sa dá priamo v zákone na konkrétne znenie odvolať.

Unikátny identifikátor kupujúceho (ďalej len „UIK“) nie je osobný údaj. UIK si kupujúci zvolí sám. Ak ide o kupujúceho, ktorý je registrovaný pre daň z príjmov, identifikátorom môže byť jeho daňové identifikačné číslo. UIK je nepovinný údaj, ktorý môže byť uvedený na pokladničnom doklade po dohode kupujúceho a podnikateľa.
Na základe vyššie uvedeného je vláda presvedčená, že ustanovenia § 8 ods. 1 písm. b) a g) a § 8a ods. 1 v slovách „daňové identifikačné číslo“ a v slovách „unikátny identifikátor kupujúceho, ak je predložený kupujúcim pred zaevidovaním prijatej tržby“ zákona č. 289/2008 Z. z. o používaní elektronickej registračnej pokladnice a o zmene a doplnení zákona Slovenskej národnej rady č. 511/1992 Zb. o správe daní a poplatkov a o zmenách v sústave územných finančných orgánov v znení neskorších predpisov v znení neskorších predpisov je v súlade s Ústavou a ustanoveniami medzinárodných zmlúv, ktorými je Slovenská republika viazaná, v dôsledku čoho návrh navrhovateľov považujeme za nedôvodný a navrhujeme aby Ústavný súd rozhodol tak, ako je uvedené v časti II. tohto stanoviska.».

13. Vláda vo svojom stanovisku č. 03206/2020/100 z 10. februára 2020 navrhuje, aby ústavný súd návrhu nevyhovel.

II.3. Stanovisko Generálnej prokuratúry Slovenskej republiky:

14. Generálna prokuratúra Slovenskej republiky vo svojom stanovisku č. k. 1 GÚp 4/20/1000-5 z 20. februára 2020 o. i. uviedla, že *«Daňové identifikačné číslo („DIČ“) prideľuje orgán daňovej správy daňovému subjektu na účely jeho identifikácie a z dôvodu eliminovania potreby vedenia iných údajov (napr. registračná povinnosť v zmysle § 49a zákona č. 595/2003 Z. z. o dani z príjmov).*
V minulosti v zmysle zákona č. 511/1992 Zb. o správe daní a poplatkov a o zmenách v sústave územných finančných orgánov bola fyzická osoba, ktorá nie je povinná sa podľa tohto alebo osobitného zákona registrovať pri styku so správcom dane povinná uvádzať rodné číslo. Takúto povinnosť už fyzická osoba v zmysle zákona č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov nemá. Takáto právna úprava by totiž mohla narážať na právnu úpravu ochrany osobných údajov.
Skupina poslancov vo svojom návrhu na podporu svojej argumentácie uviedla závery formulované v náleze Ústavného súdu Českej republiky Pl. ÚS 26/16, tento však nemožno aplikovať na právny stav na Slovensku, keďže DIČ na Slovensku nie je na rozdiel od Českej republiky tvorený na základe rodného čísla ani na základe žiadneho iného osobného údaju.
Unikátny identifikátor kupujúceho je nepovinný údaj, ktorý môže byť uvedený na pokladničnom doklade po dohode kupujúceho a podnikateľa. Ak tento údaj nebude uvedený na pokladničnom doklade, podnikateľ nebude môcť byť sankcionovaný, nakoľko ide o nepovinný údaj.
Keďže ide o nepovinný (dobrovoľný) údaj vo forme alfanumerického reťazca znakov, ktorý si môže zvoliť sám kupujúci a je len na vôli kupujúceho, či ho pri kúpe (pred zaevidovaním prijatej tržby) predloží (či sa ním preukáže), pričom finančná správa nemá prístup k dokumentácii podnikateľa (predávajúceho), ktorý si vedie evidenciu o unikátnych identifikátoroch kupujúcich (ďalej aj „UIA“), finančná správa nemá nástroje na stotožnenie kupujúceho.
Vzhľadom na vyššie uvedené zastávam názor, že ustanovenie § 8 ods. 1 písm. b) a g) a § 8a ods. 1 v slovách „daňové identifikačné číslo“ a v slovách „unikátny identifikátor kupujúceho, ak je predložený kupujúcim pred zaevidovaním prijatej tržby“ zákona č. 289/2008 Z. z. o používaní

elektronickej registračnej pokladnice a o zmene a doplnení zákona Slovenskej národnej rady č. 511/1992 Zb. o správe daní a poplatkov a o zmenách v sústave územných finančných orgánov v znení neskorších predpisov nie je v rozpore s čl. 16 ods. 1, čl. 19 ods. 2 a ods. 3 Ústavy Slovenskej republiky a čl. 8 Dohovoru o ochrane ľudských práv a základných slobôd a čl. 7, 8 a čl. 52 ods. 1 Charty základných práv Európskej únie.».

II.4. Stanovisko predsedu Najvyššieho súdu Slovenskej republiky:

15. Predseda Najvyššieho súdu Slovenskej republiky (ďalej len „najvyšší súd“) vo svojom stanovisku č. k. KP 3/2020-26 z 1. júna 2020 o. i. uviedol, že *«Právna úprava upravujúca obsah pokladničného dokladu uvedená v § 8 ods. 1 písm. b) a g) sama osebe nie je spôsobilá zasiahnuť do ústavou garantovaného práva (predávajúceho ani kupujúceho) na ochranu osobných údajov.*
Pri akceptovaní výkladu, že slovné spojenie „daňové identifikačné číslo“ v ustanovení § 8a ods. 1 sa týka len predávajúceho rovnako nie je dôvod návrhu vyhovieť.
Slovné spojenie „unikátny identifikátor kupujúceho, ak je predložený kupujúcim pred zaevidovaním prijatej tržby“ sa z doterajšieho znenia zákona sa javí ako nejasné, podmienky a spôsob použitia tohto inštitútu sú nedostatočne upravené. V tomto stave poznania veci sa k ústavnosti tejto časti petitu návrhu skupiny poslancov nevyjadrujem.».

II.5. Stanovisko Úradu na ochranu osobných údajov Slovenskej republiky:

16. Úrad na ochranu osobných údajov Slovenskej republiky (ďalej len „úrad na ochranu osobných údajov“) vo svojom stanovisku č. 00264/2020-Op-2 z 30. júla 2020 o. i. uviedol, že *„Z uvedeného vyplýva, že kupujúci si toho času môže sám zvoliť UIK a tiež to, či ho poskytne, avšak, ak je kupujúcim osoba registrovaná pre daň z príjmov, môže byť jej UIK aj daňové identifikačné číslo, ktoré jej bolo pridelené.*
V prípade, ak si však kupujúci UIK zvolí a predloží ho podnikateľovi pred zaevidovaním tržby, tak tovary alebo služby budú v zmysle uvedenej novely online (prípadne následne offline) zaslané finančnej správe spolu s UIK, teda finančná správa bude disponovať aj týmito údajmi od obchodníka o kupujúcom, nakoľko ak si kupujúci s predávajúcim zadanie UIK dohodne obchodník je povinný aj tento údaj zaslať v zmysle mu vyplývajúcej zákonnej povinnosti podľa § 8a ods. 1 zákona č. 289/2008 Z. z.
Taktiež z vyššie citovanej dôvodovej správy, ktorá sa týka UIK nie je zrejmý účel spracúvania UIK spolu s nakúpenými položkami tovaru a služieb a úrad nevidí súvislosť medzi účelom novely ako celku a zavedením a spracúvaním UIK; z dostupných materiálov takáto súvislosť nevyplýva a inštitút UIK v teraz nastavenom režime spracúvania podľa úradu nijako neprispieva k tomu, aby štát dosiahol sledovaný cieľ, ktorým je eliminácia krátenia prijatých tržieb.
Štátny orgán môže aj v zmysle ústavy konať len to, čo má zákonom dovolené, ustanovené a vzhľadom na to, ako sme uviedli vyššie, že účel spracúvania pre údaje týkajúce sa UIK v spojení s konkrétnym tovarom a službou nie je novelou vôbec, alebo riadne ustanovený je len veľmi ťažké určiť, akým spôsobom sú získané údaje štátnou správou (finančnou správou) spracúvané avšak nie je možné vylúčiť, že uvedené údaje vzhľadom na ich netransparentné spracúvanie môžu byť predmetom ich využitia aj na profilovanie konkrétnej fyzickej osoby.
Pokiaľ ide o profilovanie zo strany predávajúceho a možnosti jeho vykonávania na základe spracúvania UIK a konkrétneho tovaru a služby aj vzhľadom na obmedzené možnosti podnikateľa

by bolo veľmi špekulatívne sa vyjadrovať k tomu do akej miery je podnikateľ svojimi prostriedkami schopný identifikovať osobu kupujúceho a vytvárať jej profily. Považujeme však za potrebné dodať, že podnikatelia už teraz majú legálnu možnosť, ako získať nákupné preferencie kupujúceho tak, aby o tom bol informovaný a prípadne z odovzdávania takýchto údajov aj profitoval; ide v súčasnosti o používaný model vernostných kariet, kedy kupujúci na základe súhlasu alebo oprávneného záujmu predávajúceho vie, že tento o ňom zbiera osobné údaje.
V kontexte spracúvania osobných údajov podľa osobitných predpisov sa javí, že ide o vzťah dvoch samostatných prevádzkovateľov; nakoľko povinnosť odovzdať údaje UIK a tovar a službu je povinnosťou podnikateľa – predávajúceho, akonáhle si kupujúci UIK zvolí, javí sa, že údaje sú predmetom záujmu skôr finančnej správy, ako podnikateľa. Aj vzhľadom na absenciu stanovenia účelu spracúvania UIK spolu s tovarom a službami je preto veľmi ťažké zaujať jednoznačný postoj v tom, aké postavenie majú pri spracúvaní uvedených údajov jednotlivé subjekty. Uvedené je dôsledkom nesprávneho a nekonzistentného ustanovenia jasných a presných pravidiel spracúvania od počiatku, kedy v zákone absentujú základné nastavenia spracúvania pre UIK v spojení s tovarom a službou.“.

II.6. Stanovisko Finančného riaditeľstva Slovenskej republiky:

17. Finančné riaditeľstvo Slovenskej republiky (ďalej len „finančné riaditeľstvo“) vo svojom stanovisko č. 356624/2020 z 30. júla 2020 o. i. uviedlo, že *«Návrhom napadnuté ustanovenia § 8 ods. 1 písm. b) a g) zákona č. 289/2008 Z. z. upravujú obsahové náležitosti pokladničného dokladu vyhotoveného elektronickou registračnou pokladnicou (ďalej len „ERP“), používanie ktorých bolo ukončené k 31.12.2019. Na uvedené ustanovenia však nenadväzuje ustanovenie § 8a ods. 1 zákona č. 289/2008 Z. z., ktoré upravuje rozsah údajov zasielaných do systému e-kasa, pretože z ERP nie sú zasielané údaje do systému e-kasa (ERP so systémom e-kasa nie je prepojená). V ustanovení § 8a ods. 1 je použitý odkaz na ustanovenia § 8 ods. 1 písm. g) len z legislatívno-technických dôvodov.*
Daňové identifikačné číslo (ďalej len „DIČ“) je prideľované daňovému subjektu správcom dane na účely jeho jednoznačnej identifikácie a z dôvodu eliminovania potreby spracúvania iných osobných údajov, vrátane rodného čísla a dátumu narodenia v prípade fyzických osôb, teda účelom jeho existencie je aj ochrana osobných údajov, čo je jednoznačným dôvodom pre posúdenie takéhoto spracúvania osobných údajov ako primeraného a proporcionálneho, eliminujúceho väčší rozsah štátneho zásahu, avšak umožňujúci jednoznačnú identifikáciu podnikateľa pre finančnú správu, čo opodstatňuje záver o nevyhnutnosti spracúvania tohto údaja.
DIČ plní funkciu identifikovateľnosti osoby len vo vzťahu k finančnej správe, prípadne vo vzťahu k inému oprávnenému spracúvateľovi tohto údaja. Účel jeho existencie a spracúvania je vymedzený prioritne daňovými predpismi, pričom zákon č. 289/2008 Z. z. rozšíril jeho používanie aj na účely evidencie prijatej tržby, čím právna norma spĺňa požiadavky na zákonnosť právnej úpravy.
Nevyhnutnosť takéhoto spracúvania údajov je daná aj z dôvodu, že doklady z ERP ako aj z PEKK štandardne plnia aj funkciu faktúry podľa zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov (ďalej len „zákon č. 222/2004 Z. z.“) a zároveň aj funkciu účtovného dokladu podľa zákona č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov (ďalej len „zákon o účtovníctve“), a teda aj dokladu posudzovaného na účely zákona č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov.

Aby bolo možné pokladničný doklad vyhotovený ERP alebo PEKK považovať za zjednodušenú faktúru, musí obsahovať zákonom č. 222/2004 Z. z. predpísané náležitosti. Z uvedeného dôvodu pokladničný doklad vyhotovený ERP, ako aj PEKK obsahuje okrem iného také povinné údaje, ktoré korešpondujú s náležitosťami zjednodušenej faktúry upravenými zákonom č. 222/2004 Z. z...

Unikátny identifikátor kupujúceho (ďalej len „UIK“) nie je osobný údaj. UIK si kupujúci zvolí sám. Ak ide o kupujúceho, ktorý je registrovaný pre daň z príjmov, identifikátorom môže byť jeho DIČ. UIK je nepovinný údaj, ktorý môže byť uvedený na pokladničnom doklade výlučne po dohode kupujúceho a podnikateľa.

V odseku 8 návrhu navrhovatelia uvádzajú, že: „Unikátnym identifikátorom kupujúceho je v zmysle Zákona taktiež údaj, ktorý je pridelený kupujúcemu v prípade, že používa tzv. vernostné alebo zľavové karty.“ V tejto súvislosti zastávame názor, že v zákone č. 289/2008 Z. z. nie je zrejmý, dokonca ani naznačený, vzťah medzi UIK a vernostnou kartou zákazníka, a preto uvedené nie je možné konštatovať. Ak by sme pripustili, že číslo vernostnej karty možno považovať za osobný údaj, predávajúci ho v žiadnom prípade nesmie bez súhlasu kupujúceho zaslať do systému e-kasa. UIK slúži na to, aby sa kupujúci identifikoval voči systému e-kasa v pripravovanej zóne kupujúceho (zatiaľ táto zóna ešte neexistuje), ktorá kupujúcemu poskytne prehľad realizovaných výdavkov, bude slúžiť ako podklad pre účtovníctvo kupujúceho-podnikateľa, na evidenciu dokladov pre potreby reklamácií, resp. na archiváciu prijatých pokladničných dokladov.

Ani zaslaním ID zákazníckej karty finančná správa nezískava žiadne iné údaje, ktoré sa k danej karte viažu (napr. trvalý pobyt, meno a priezvisko, telefón a podobne). Tieto údaje (ak vôbec) má len podnikateľ, ktorý vydal zákaznícku kartu a nikdy ich v zmysle zákona č. 289/2008 Z. z. neposkytuje finančnej správe pri evidencii tržieb (mohol by tak postupovať len v prípade, že by o to kupujúci požiadal, t. j. dobrovoľne).

UIK je dobrovoľný údaj, ktorý je na pokladničnom doklade uvedený iba na základe dohody s kupujúcim, pričom pri každom nákupe, resp. u každého podnikateľa môže kupujúci použiť iný identifikátor (napr. NBÚ1234567, potom NBÚ2345678). Rôzni kupujúci môžu uviesť identické identifikátory. Finančná správa preto nedokáže UIK priradiť ku konkrétnemu kupujúcemu. Nakoľko UIK je nepovinný údaj, nemožno hovoriť o neprimeranom zásahu do práv a slobôd kupujúcich.

DIČ je jedinečný identifikátor vygenerovaný systémom finančnej správy, ktorý neobsahuje údaj o rodnom čísle. Uvedený princíp bol zavedený ešte v čase platnosti zákona č. 511/1992 Zb. o správe daní a poplatkov a o zmenách v sústave územných finančných orgánov v znení účinnom od 01.01.2005, a to na základe jeho novely zákonom č. 679/2004 Z. z., ktorým bola zmenená dikcia § 31 ods. 11. Tento údaj používa podnikateľ, resp. daňový subjekt vždy pri komunikácii s finančnou správou. Z uvedeného dôvodu bolo stanovené, že DIČ slúži na identifikáciu podnikateľa pri komunikácii PEKK so systémom e-kasa. Na základe tohto identifikátora je možné jednoznačne určiť, ktorý podnikateľ zaslal z PEKK údaje do systému e-kasa. Uvedením DIČ podnikateľa (predajcu, poskytovateľa služby) na pokladničnom doklade vyhotovenom PEKK podnikateľa podľa nášho názoru nedochádza k porušeniu práv upravených Ústavou Slovenskej republiky. Štandardne podnikateľ používa a zverejňuje svoje DIČ.

Ustanovenie § 8a ods. 1 zákona č. 289/2008 Z. z. upravuje, že podnikateľ je povinný zabezpečiť, aby PEKK zasielala do systému e-kasa aj údaj podľa § 8 ods. 1 písm. g) zákona č. 289/2008 Z. z., t. j. údaj o označení tovaru alebo služby a množstve tovaru alebo rozsahu služby. Tento údaj obsahuje aj pokladničný doklad vyhotovený PEKK, ktorý je odovzdaný kupujúcemu.

Podľa § 8 ods. 3 zákona č. 289/2008 Z. z. označenie tovaru alebo označenie služby musí byť vyjadrené tak, aby bolo možné predávaný tovar alebo poskytovanú službu jednoznačne určiť alebo pomenovať a odlíšiť od iného tovaru alebo od inej služby, pričom sa môže uvádzať aj skrátený názov tovaru alebo služby. Tovar alebo službu nemožno označiť len číselným znakom alebo alfanumerickým kódom.
Zákon č. 289/2008 Z. z. ustanovuje, akým spôsobom má podnikateľ povinnosť označiť tovar alebo poskytovanú službu, avšak pri označovaní tovaru alebo poskytovanej služby nie je podnikateľ ničím viazaný – môže uvádzať aj skrátený názov tovaru alebo služby. Neexistuje ustanovenie, ktoré by určovalo konkrétny číselník tovarov alebo služieb resp. ich presné označenie, je to len v kompetencii samotného podnikateľa (predávajúceho). Pre spracovanie údajov v systéme e-kasa týkajúcich sa označenia tovaru alebo poskytovanej služby by bolo potrebné, aby bola zabezpečená konzistentnosť spracúvaných dát. Vzhľadom na to, že každý podnikateľ označuje tovar alebo poskytovanú službu podľa vlastného uváženia, nie je reálne, aby systém e-kasa vyhodnocoval nákupy podľa druhu tovaru alebo poskytovanej služby, napr. počet predaných chlebov v daný deň všetkými podnikateľmi na území Slovenskej republiky.
Systém e-kasa nemá za cieľ sledovať dennodenné správanie kupujúcich a vytvárať profil kupujúcich, pretože ako už bolo v tomto stanovisku uvedené, UIK môže byť na pokladničnom doklade uvedený ako dobrovoľný údaj, ktorý nie je s výnimkou použitia DIČ kupujúcim (podnikateľom), rozpoznateľný finančnou správou na konkrétnu fyzickú osobu. Do systému e-kasa nie je podnikateľ (predávajúci) povinný zasielať a plošne poskytnúť údaje vzťahujúce sa k vernostnému programu uzatvorenému medzi predávajúcim a kupujúcim. Na základe UIK, ktorý nie je vo forme DIČ, nie je možné získať a spracúvať osobné údaje kupujúcich, nakoľko finančná správa nemá prístup k informáciám podnikateľa (predávajúceho), ktorý eviduje osobné údaje kupujúceho vo vzťahu k UIK.
Na základe vyjadrení k problematike DIČ, UIK, názvu tovaru alebo služby, ktoré sú uvedené v predchádzajúcich častiach tohto stanoviska zastáva Finančné riaditeľstvo Slovenskej republiky názor, že § 8 ods. 1 písm. b) a g) a § 8a ods. 1 v slovách „daňové identifikačné číslo“ a v slovách „unikátny identifikátor kupujúceho, ak je predložený kupujúcim pred zaevidovaním prijatej tržby“ nie sú protiústavné (čl. 16 ods. 1, čl. 19 ods. 2 a 3), nie sú v rozpore s čl. 8 Dohovoru o ochrane ľudských práv a základných slobôd a čl. 7, 8 a ani s čl. 52 ods. 1 Charty základných práv Európskej únie. Finančné riaditeľstvo Slovenskej republiky preto odporúča, aby Ústavný súd Slovenskej republiky návrhu nevyhovel.».

18. Na žiadosť ústavného súdu finančné riaditeľstvo listom č. 50912/2021 z 3. februára 2021 doplnilo a spresnilo už uvedené stanovisko a predložilo okrem odpovedí na zaslané otázky aj interný riadiaci akt č. 136/2018 – smernicu o ochrane osobných údajov, interný riadiaci akt č. 17/2020 – smernicu riadenia prístupu externého subjektu k informačno-komunikačným technológiám finančnej správy a externých prístupov interných zamestnancov finančnej správy a materiál *„Koncepcia registrácie maloobchodných transakcií pre Slovenskú republiku“*.

II.7. Replika navrhovateľov:

19. Poslanec národnej rady Alojz Baránik za navrhovateľov vo svojej replike zo 7. septembra 2020 uviedol, že *„k vyššie uvedeným stanoviskám nepovažujem za potrebné sa vyjadriť a zároveň podľa § 58 ods. 3 zákona č. 314/2018 Z. z. o Ústavnom súde Slovenskej republiky a o zmene a doplnení*

niektorých zákonov v znení neskorších predpisov súhlasím s upustením od ústneho pojednávania o prijatom návrhu.“.

II.8. Ústne pojednávanie:

20. Vo veci sa ústne pojednávanie nekonalo, pretože účastníci navrhli od neho upustiť a ústavný súd ho nepovažoval za nevyhnutné.

III.
Posúdenie dôvodnosti návrhu

21. Ústavný súd po oboznámení sa s návrhom navrhovateľov, so stanoviskami národnej rady a vedľajšieho účastníka a predsedu najvyššieho súdu, finančného riaditeľstva a úradu na ochranu osobných údajov dospel k týmto záverom:

III.1. K napadnutým ustanoveniam ako súčasti daňovej legislatívy:

22. Ustanovenie § 8a ods. 1 zákona č. 289/2008 Z. z. o používaní elektronickej registračnej pokladnice a o zmene a doplnení zákona Slovenskej národnej rady č. 511/1992 Zb. o správe daní a poplatkov a o zmenách v sústave územných finančných orgánov v znení neskorších predpisov bolo do tohto zákona doplnené jeho novelou zákonom č. 368/2018 Z. z. ako súčasť právnej úpravy systému e-kasa

22.1. Dôvodová správa k tomuto zákonu o systéme e-kasa o. i. uvádza, že „Systém e-kasa predstavuje bezpečný, vysokopriepustný systém evidencie tržieb a pokladničných dokladov v reálnom čase, ktorý umožní integráciu on-line pokladníc, ako aj virtuálnych registračných pokladníc na centrálnu databázu finančnej správy, zasielanie údajov v reálnom čase, ako aj v off-line režime. Systém e-kasa bude pre podnikateľov znamenať zníženie administratívnej záťaže pri obstarávaní hardvéru, zníženie nákladov pri prevádzke, kontinuálny prechod medzi účtovnými dňami, export dát na zjednodušenie podávania kontrolného výkazu na účely DPH, dostupnosť dát počas archivácie. Zákazníkom systém umožní overenie pravosti pokladničných dokladov v reálnom čase. Systém e-kasa okrem toho umožní finančnej správe vykonávať prehľad a triedenie získaných dát a ich využitie na účely kontroly dodržiavania ustanovení tohto zákona, ako aj na účely daňovej kontroly.“.

23. Systém e-kasa predstavuje reformu finančnej správy, ktorá sleduje zníženie daňovej medzery na dani z pridanej hodnoty. Systém e-kasa to zabezpečuje evidenciou tržieb a pokladničných dokladov v reálnom čase, integráciou on-line pokladníc, ako aj virtuálnych registračných pokladníc na centrálnu databázu finančnej správy a zasielaním údajov v reálnom čase.

24. Je potrebné podotknúť, že napadnuté ustanovenia síce nepredstavujú hmotnoprávnu úpravu daní v zmysle určenia predmetu, výšky či poplatníka dane, ale predstavujú súčasť rozpočtovej a daňovej politiky štátu tým, že sú súčasťou nástrojov na kontrolu plnenia daňových povinností daňovými subjektmi.

25. Stanovenie daňových povinností, ale aj vytvorenie efektívneho systému ich kontroly a vynucovania je dôležité z hľadiska plnenia funkcií štátu, pre ktoré je nevyhnutné, aby mal zabezpečené daňové príjmy. Efektívna kontrola a vynucovanie plnenia daňových povinností

predstavujú legitímny cieľ, ktorým je možné odôvodniť proporcionálny zásah do základných práv a slobôd.

26. Ustanovenie § 8 ods. 1 písm. b) a g) zákona č. 289/2008 Z. z. o používaní elektronickej registračnej pokladnice a o zmene a doplnení zákona Slovenskej národnej rady č. 511/1992 Zb. o správe daní a poplatkov a o zmenách v sústave územných finančných orgánov v znení neskorších predpisov nie je súčasťou právnej úpravy systému e-kasa. Odkaz na § 8 ods. 1 písm. b) a g) použitý v § 8a ods. 1 má len legislatívno-technický charakter v tom, že odkazuje na slová už v zákone raz použité, čím nedochádza k ich opakovanému neúčelnému používaniu v texte zákona. Tento odkaz nemá funkčný charakter v tom, že by funkčne a vecne prepojoval tieto ustanovenia, práve naopak. V § 8 ods. 1 písm. b) a g) uvedené údaje sú súčasťou pokladničného dokladu vyhotoveného elektronickou registračnou pokladňou, ktorá nie je prepojená so systémom e-kasa a údaje z nej nie sú do systému e-kasa zasielané. Údaje, ktoré obsahuje pokladničný doklad vyhotovený pokladnicou e-kasa klient, upravuje § 8 ods. 7, ktorý ale napadnutý nie je.

III.2. K namietanému nesúladu s právom na ochranu súkromia a osobných údajov:

27. Napadnuté ustanovenia zákona č. 289/2008 Z. z. o používaní elektronickej registračnej pokladnice a o zmene a doplnení zákona Slovenskej národnej rady č. 511/1992 Zb. o správe daní a poplatkov a o zmenách v sústave územných finančných orgánov v znení neskorších predpisov obsahujú tri *štádiá* zásahov do práva na ochranu súkromia a osobných údajov: (a) zber a lokálne uchovanie údajov na zariadení pri kúpe v obchode vrátane vydania pokladničného dokladu, (b) automatizované odoslanie a uchovávanie údajov v reálnom čase v centrálnej databáze finančnej správy a (c) následne spracúvanie týchto údajov finančnou správou vrátane ich používania na automatizované posudzovanie a poskytovania ďalším štátnym orgánom na iné účely. Tieto štádiá zásahu sa líšia svojou intenzitou, cieľom a zárukami, a preto ich ústavný súd analyzuje osobitne. Zároveň ústavný súd pri svojej analýze odlišoval zásah do práv predávajúcich a kupujúcich v tomto systéme.

28. Navrhovatelia tvrdia, že predmetné ustanovenia predstavujú neprimeraný zásah do ochrany súkromia a osobných údajov. Ustanovenia napadli podľa čl. 16 ods. 1 a čl. 19 ods. 2 a 3 ústavy, čl. 8 dohovoru a čl. 7, 8 a 52 charty.

29. Pri abstraktnej kontrole podľa čl. 125 ústavy vykonáva ústavný súd prieskum podľa viacerých referenčných rámcov, najčastejšie podľa ústavy a ústavných zákonov, dohovoru a charty. Ich voľba je v dispozícii navrhovateľa [§ 45 a § 75 písm. c) zákona č. 314/2018 Z. z. o Ústavnom súde Slovenskej republiky a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o ústavnom súde“)]. Právo Európskej únie (ďalej aj „EÚ“) môže mať dopad na *predmet* abstraktného prieskumu, ako aj *referenčný rámec*. Princíp prednosti práva EÚ (čl. 7 ods. 2 ústavy) sa uplatní na obe stránky. Uplatní sa na zistenie toho, aké pravidlá tvoria právny poriadok, ktorý sa preskúmava, ale aj na určenie obsahu referenčného rámca, s ktorým sa súladnosť skúma.

30. Postupnosť prieskumu závisí od toho, či je skúmaná právna otázka:

1. neharmonizovaná,
2. neúplne harmonizovaná alebo
3. plne harmonizovaná právom EÚ.

30.1. Ak je preskúmaná právna norma neharmonizovaná, ústavný súd v prípade mnohosti referenčných rámcov a zhodnosti označených práv ťažiskovo skúma súlad s ústavou a prípadne aj súlad s dohovorom alebo inou referenčnou normou. Charta sa v týchto prípadoch v zásade neaplikuje (čl. 51 ods. 1). Aj pri prieskume podľa ústavy v kontexte neharmonizovanej úpravy je však judikatúra k ostatným referenčným normám, najmä dohovoru a charte stále prítomná ako možný zdroj obohatenia výkladu jej ustanovení.

30.2. Ak je preskúmaná právna norma neúplne harmonizovaná právom EÚ, ústavný súd v prípade mnohosti referenčných rámcov skúma najprv ich súladnosť s ústavou. Judikatúra k ostatným referenčným normám, najmä dohovoru a charte ostáva stále prítomná ako zdroj obohatenia výkladu a určenia rozsahu možnosti uváženia slovenského zákonodarcu. Základné situácie, ktoré môžu nastať sú tieto:

(i) Výklad vnútroštátnych noriem vo svetle práva EÚ pripúšťa ich súlad s ústavou; ústavný súd v takom prípade vykoná ústavno-konformný výklad z interpretačných možností poskytovaných právom EÚ. Ak to navrhovateľ žiada, explicitne sa v ďalšom kroku preskúma aj ich súlad s chartou, pričom sa osobitne musí skúmať rozsah jej aplikovateľnosti, prípadne tiež aj dopad na princípy práva Európskej únie, ak o ich dodržaní existuje pochybnosť [čl. 51 ods. 1 charty a jeho výklad v judikatúre Súdneho dvora Európskej únie (ďalej len „SDEÚ“), napr. Åkerberg Fransson, C-617/10, ako aj iné princípy podľa Stefano Melloni C-399/11, bod 60].

(ii) Výklad vnútroštátnych noriem, ktorými sa nesprávne (z pohľadu európskeho a ústavného) implementuje právo EÚ, nepripúšťa ich súlad s ústavou; ústavný súd v takom prípade konštatuje porušenie a zákonodarca musí vykonať nápravu v súlade s ústavou a právom EÚ. Aj výklad vo svetle práva EÚ je obmedzený všeobecne akceptovanými metódami výkladu práva, a teda nemôže ísť *„contra legem“* (SDEÚ, Konstantinos Adeneler C-212/04, bod 110, Pupino C-105/03, body 44, 47). Ak vznikne pochybnosť o výklade práva EÚ, ústavný súd sa obráti na SDEÚ podľa čl. 267 Zmluvy o fungovaní Európskej únie [ďalej len „ZFEÚ“ (pozri bližšie II. ÚS 381/2018)]. Súladnosť s chartou ako explicitnou referenčnou normou v tomto prípade už osobitne skúmať netreba (PL. ÚS 3/09, PL. ÚS 10/2014).

(iii) Výklad vnútroštátnych noriem vo svetle práva EÚ nepripúšťa ich súlad s ústavou, pričom existuje pochybnosť o platnosti práva EÚ. Ústavný súd sa v takom prípade obráti na SDEÚ na účely preskúmania platnosti podľa čl. 267 ZFEÚ. Svoje pochybnosti vyjadrí vzhľadom na referenčný rámec charty (porov. Foto-frost, C-314/85, bod 15 a nasl., porov. explicitnejšie body 44 – 46 stanoviska AG Stix-Hackl vo veci Intermodal Transports, C-495/03, napr. rakúsky ústavný súd, VfGH, Vorratsdatenspeicherung, sp. zn. G 47/12 ua, vo veci, ktorá viedla k Digital Rights Ireland, C-293/12 a C-594/12, a neskôr ovplyvnila rozhodnutie PL. ÚS 10/2014).

30.3. Ak je preskúmaná právna norma plne harmonizovaná právom EÚ, ústavný súd v prípade mnohosti referenčných rámcov preskúma najprv ich súladnosť s chartou. Vyplýva to z toho, že spoločná legislatíva tvorená v rámci preneseného výkonu práv musí byť meraná v prvom rade podľa spoločného katalógu ľudských práv. Plná harmonizácia v určitej oblasti znamená, že právo EÚ v danej otázke neposkytuje priestor pre uváženie slovenského zákonodarcu (napr. SDEÚ vo veciach: Funke Medien, C-469/17, bod 35 a nasl.; Pelham and Others, C-476/17, bod 58 a nasl.; Breyer, C-582/14, bod 57; Fashion ID, C-40/17, body 54 a 55; Huber, C-524/06, bod 52; naopak, príkladom uváženia: čl. 85 GDPR, pozri obšírne aj rozhodnutie BVerfG, napr.

sp. zn. 1 BvR 276/17, bod 42 a nasl.). Ak ústavný súd dospeje k záveru, že právna norma nie je v súlade s chartou alebo existuje pochybnosť o výklade predmetu skúmania alebo použitého referenčného rámca, ústavný súd sa obráti na SDEÚ podľa čl. 267 ZFEÚ. V prípade zistenia súladu s chartou, ak to navrhovateľ žiadal, sa explicitne následne preskúma aj súlad s ústavou. Súlad sa pritom posúdi aj podľa zásad ekvivalentnosti ochrany a lojálnej spolupráce pri ochrane práv (čl. 4 ods. 3 Zmluvy o Európskej únii, pozri aj II. ÚS 501/2010, bod 20). Delegáciou právomocí sa totiž štát nezbavuje svojej zodpovednosti voči jednotlivcovi a aj ako člen spoločenstva štátov musí zabezpečiť, aby vzniknutá organizácia poskytovala porovnateľný stupeň ochrany základných práv a slobôd [obdobne Európsky súd pre ľudské práva (ďalej len „ESĽP“) vo veciach Bosphorus v. Írsko, č. 45036/98, La société Etablissement Biret et CIE S.A. v. 15 členských štátov EÚ, č. 13762/04].

31. V posudzovanej veci ide o situáciu, keď povinnosť zberu údajov síce nie je harmonizovaná právom EÚ, avšak otázka ochrany osobných údajov štátnymi orgánmi a podnikateľmi je predmetom nariadenia č. 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov – GDPR). Ide teda všeobecne o situáciu (bod 30.2), a to otázku neúplne harmonizovanú právom EÚ, keď má členský štát možnosť uváženia [pozri aj stanovisko generálneho advokáta Bobeka k postaveniu daňových orgánov podľa čl. 2 ods. 2 písm. d) GDPR (Valsts ieņēmumu dienests, C-175/20, bod 40)]. Ústavný súd preto zohľadnil mantinely poskytnuté právom EÚ v tejto oblasti, avšak zvýraznil aj priestor, kde slovenský zákonodarca môže (z pohľadu práva EÚ) a musí (z pohľadu ústavy) konať zodpovednejšie vzhľadom na ochranu práv jednotlivca (najmä body 117 až 141). Ako bude ďalej vysvetlené, časti napádaného zákona dokonca existencia priamo aplikovateľného práva EÚ o ochrane osobných údajov „zachránila“ pred konštatovaním nesúladu s ústavou tým, že poskytla inak chýbajúce záruky proti zneužitiu práv jednotlivca.

32. Ústavný súd sa v minulosti už viackrát vyjadril k otázke cieľa ochrany súkromia a osobných údajov (pozri najmä nosné rozhodnutia PL. ÚS 10/2014, PL. ÚS 13/2020). Účelom ústavou priznaného práva na súkromie je zabrániť verejnej moci, aby zasahovala do správania jednotlivca nad nevyhnutnú mieru a príliš neprimerane riadila jeho súkromný život (PL. ÚS 43/95, s. 26, PL. ÚS 12/01, PL. ÚS 13/2020, bod 69). Podstatou je teda možnosť jednotlivca žiť podľa svojich predstáv bez zbytočných obmedzení, príkazov a zákazov ustanovených orgánmi verejnej moci (II. ÚS 19/97, II. ÚS 7/99, II. ÚS 19/99, PL. ÚS 12/01). V najširšom význame ide teda o ochranu proti neprimeranému štátnemu dirigizmu (PL. ÚS 13/2020, bod 69). V tomto ohľade je právo na súkromie úzko spojené s právom na ľudskú dôstojnosť (čl. 19 ods. 1 ústavy) a princípom slobody konať (čl. 2 ods. 3 ústavy). Podľa judikatúry ústavného súdu právo na ochranu pred neoprávneným zasahovaním do súkromnej sféry jednotlivca zahŕňa nielen negatívnu povinnosť štátu zdržať sa mocenského zásahu, ale aj jeho pozitívny záväzok prijať účinné opatrenia na zabezpečenie jeho efektívnej ochrany (III. ÚS 331/09, II. ÚS 424/2012, PL. ÚS 10/2014). Tam, kde však k zásahu do práv dochádza zo strany súkromnej moci, ale na základe delegácie od verejnej moci, zodpovedá štát za zásah priamo ako za svoje konanie (*Copland proti Spojenému Kráľovstvu*, č. 62617/00, bod 39; *Vukota-Bojic proti Švajčiarsku*, č. 61838/10, bod 47, podobne aj generálny advokát Henrik Saugmandsgaard Øe vo veci C-401/19, *Poľská republika proti Európskemu parlamentu a Rade EÚ*, body 115 a 151).

33. Právo na súkromný život v sebe zahŕňa i právo na ochranu pred sledovaním, striehnutím a prenasledovaním zo strany verejnej moci, a to i vo verejnom priestore či na verejne prístupných miestach. Navyše, žiadny zásadný dôvod neumožňuje vylúčiť z pojmu súkromný život profesijné, obchodné či sociálne aktivity (rozhodnutie ESĽP vo veci *Niemietz proti Nemecku*, č. 13710/88 zo 16. 12. 1992).

34. Z judikatúry vyplýva, že zatiaľ čo ústavná ochrana súkromia sa podľa čl. 16 ods. 1 ústavy spája s nedotknuteľnosťou osoby, jej telesnou integritou a súvisiacimi materiálnymi hodnotami, ochrana nemateriálnych hodnôt súkromnej povahy sa zaručuje podľa čl. 19 ods. 2 ústavy (napr. III. ÚS 88/01, s. 17). Článok 22 ústavy poskytuje osobitnú ochranu pre tajomstvo dopravovaných správ. Návrh namieta porušenie čl. 16 a 19 ústavy, avšak z jeho znenia je na prvý pohľad zrejmé, že sa netýka telesnej integrity jednotlivca, ale skôr nemateriálnej stránky jeho súkromia, ktorá je chránená skôr podľa čl. 19 a 22 ústavy.

35. Ochrana súkromia (čl. 16 ods. 1, čl. 19 ods. 2 ústavy) a osobných údajov (čl. 19 ods. 3 a čl. 22 ods. 1 ústavy) sa síce zásadne prekrývajú, avšak sledujú aj osobitné ciele. Súkromie chráni jednak osobnú a intímnu sféru jednotlivca, jeho tajomstvá a dôvernú komunikáciu, ale aj zachytenie jeho správania na verejných miestach a všeobecnú slobodu rozhodovania, ako viesť svoj život. Ochrana osobných údajov je síce previazaná len so spracovávaním údajov, no zároveň je koncipovaná širšie. Je chápaná najmä ako ochrana pred automatizovaným zbieraním a spracúvaním informácií o jednotlivcovi, ktoré môžu ohroziť *akékoľvek* jeho slobody vo všetkých sférach života, a teda nielen v oblasti ochrany súkromia. Cieľom je preto chrániť najmä právo jednotlivca na sebaurčenie, ale aj autonómnosť jeho rozhodovacieho procesu, a to predchádzaním jeho manipulácii, diskriminácii alebo ohrozením jeho bezpečnosti (pozri aj čl. 1 Dohovoru Rady Európy č. 108 o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov publikovaného v Zbierke zákonov Slovenskej republiky ako oznámenie Ministerstva zahraničných vecí Slovenskej republiky č. 49/2001 Z. z.).

36. Proti zberu a zneužitiu osobných údajov chráni ústava v čl. 19 ods. 3 a čl. 22 ods. 1, ktoré takto zakotvujú právo jednotlivca na informačné sebaurčenie (PL. ÚS 10/2014, bod 133). Cieľom práva na informačné sebaurčenie je zabezpečiť slobodný rozvoj osobnosti v kontexte modernej spoločnosti, ktorá je definovaná jednoduchým zhromažďovaním a automatizovaným spracúvaním informácií o jednotlivcovi (PL. ÚS 13/2020, bod 69). Nekontrolované spracúvanie osobných údajov by ohrozovalo nielen slobodu konania jednotlivca, pretože by sa nikdy necítil úplne voľný, ale v konečnom dôsledku aj samotné demokratické zriadenie, keďže jeho garantmi môžu byť len skutočne slobodní jednotlivci [PL. ÚS 13/2020, bod 69, podobne Spolkový ústavný súd Nemecka (BVerfG), *Volkszählungsurteil*, sp. zn. 1 BvR 209, 269, 362, 420, 440, 484/83].

37. Podnikatelia, či už v pozícii fyzických osôb, alebo právnických osôb, musia v súvislosti s výkonom svojej podnikateľskej činnosti strpieť viac zásahov zo strany štátu ako bežný jednotlivec. Štát má oprávnenie vyberať dane z hospodárskej činnosti a na tento účel zbierať potrebné informácie. Rovnako môže podnikateľov zaťažovať zberom rôznych údajov s cieľom ochrany verejného záujmu alebo základných práv a slobôd jednotlivcov (napr. PL. ÚS 23/06). A môže aj ukladať rôzne povinnosti na účely ochrany jednotlivca pred zneužitím ekonomickej sily podnikateľov samotných. Vystavenie podnikateľov primeraným povinnostiam zberu údajov je

bežnou súčasťou napĺňania pozitívnej povinnosti štátu vytvoriť podmienky sociálne a ekologicky orientovanej trhovej ekonomiky (čl. 55 ods. 1 ústavy).

38. V tomto smere je preto nutné zdôrazniť, že v prejedávanej veci nejde o situáciu, kde by dochádzalo „len“ k zásahu do práv právnických osôb podnikateľov. Ochrana právnických osôb podnikateľov by síce bola predmetom odlišného prieskumu z dôvodu intenzity zásahu, no aj pri nich ústava poskytuje ochranu.

39. Súkromie a ochrana osobných údajov kupujúcich a predávajúcich v prejedávanom prípade sa týka fyzických osôb aj právnických osôb. Zatiaľ čo na strane predávajúcich môžu figurovať len fyzické osoby alebo právnické osoby, ktoré sú podnikateľmi, na strane kupujúcich to môžu byť jednak podnikatelia v oboch formách, ale aj fyzické osoby nepodnikatelia. Z dôvodu tohto zmiešaného charakteru adresátov noriem je nutné na strane predávajúcich vychádzať z toho, že je medzi nimi aj silné zastúpenie fyzických osôb, preto sa uplatní vyšší štandard ochrany uplatniteľný na fyzické osoby podnikateľov. Na strane kupujúcich je zas nutné vychádzať zo štandardu ochrany fyzických osôb nepodnikateľov, keďže právna úprava na nich dopadá rovnako ako na podnikateľov. Ak sú adresáti „zmiešaní“ a právna úprava ich neoddeľuje, vždy sa uplatní vyšší štandard ochrany.

40. Je pravdou, že právo na súkromie v prvom rade chráni fyzické osoby. Týka sa práva „na zachovanie ľudskej dôstojnosti“, „osobnej cti“, zachovania „rodinného života“, a teda hodnôt, ktoré si môže nárokovať chrániť len človek. Nárok právnických osôb na práva zaručené ústavou treba ale hodnotiť podľa podstaty označeného práva (PL. ÚS 15/1998). Podobne ako pri slobode prejavu (PL. ÚS 15/1998) čl. 19 a 22 chránia aj také hodnoty, ktoré si môžu uplatniť aj právnické osoby. Aj preto ústava v čl. 19 pracuje s pojmom „každý“ a v čl. 22 adresáta zamlčuje. Z judikatúry ESĽP v kontexte čl. 8 rovnako vyplýva, že právnické osoby si môžu uplatňovať niektoré čiastkové práva na ochranu súkromia aj podľa dohovoru [pozri *Niemietz proti Nemecku*, A No 251-B. (1992), ods. 29 až 31, *Colas Est a ďalší proti Francúzku*, č. 37971/97, ods. 41, *Peck proti Spojenému Kráľovstvu*, č. 44647/98, ods. 57, *Bernh Larsen Holding AS a ďalší proti Nórsku*, č. 24117/08, bod 106 (čo sa týka údajov firmy), *Liberty a ďalší proti Spojenému Kráľovstvu*, č. 58243/00, body 56 – 57 (čo sa týka neziskovej organizácie)].

41. Dôraz na človeka je ešte zreteľnejší pri práve na ochranu osobných údajov v súčasnej úprave v slovenskom, európskom a medzinárodnom právnom poriadku. Historicky je Dohovor Rady Európy č. 108 o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov obmedzený na fyzické osoby, pričom členské štáty môžu jeho pôsobnosť rozšíriť aj na právnické osoby [čl. 3 ods. 2 písm. b) Dohovoru č. 108]. Rovnako v európskom kontexte je podľa judikatúry SDEÚ ochrana primárnym a sekundárnym právom obmedzená na údaje fyzických osôb (pozri rozhodnutie *Volker und Markus Shecke and Eifert*, C-92/09 a C-93/09, ods. 53). Právnické osoby sa „môžu dovolávať ochrany podľa článkov 7 a 8 charty v súvislosti s týmto uvedením len v rozsahu, v akom názov právnickej osoby identifikuje jednu alebo viaceré fyzické osoby“ (pozri rozhodnutie *Volker und Markus Shecke and Eifert*, C-92/09 a C-93/09, ods. 53). Slovenská republika však prijala svoj ústavný text skôr, než pristúpila k Dohovoru č. 108 alebo charte. Ochrana predovšetkým fyzických osôb je dôsledkom únijného práva, keďže historicky viacero členských štátov chránilo rôznymi spôsobmi legislatívne aj právnické osoby [pozri ERDOS, D. *Dead Ringers? Legal Persons and the Deceased in European Data Protection Law* (May 13, 2020). University of Cambridge, Faculty of Law Research Paper No. 21/2020, s. 3; ale aj KORFF, D. *Study on the Protection of the*

Rights and Interests of Legal Persons with Regard to the Processing of Personal Data Relating to Such Persons (2008). Dostupné na: <https://ssrn.com/abstract=1288583>].

42. V januári 1991 Federálne zhromaždenie Českej a Slovenskej Federatívnej Republiky prijalo ústavný zákon č. 23/1991 Zb., ktorým sa uvádza Listina základných práv a slobôd. Súčasný čl. 19 ods. 3 ústavy bol prijatý ako čl. 10 ods. 3 Listiny základných práv a slobôd, avšak predloha súčasného čl. 22 ods. 1 ústavy v čl. 13 Listiny základných práv a slobôd neobsahovala odkaz na osobné údaje. V apríli 1992 Federálne zhromaždenie Českej a Slovenskej Federatívnej Republiky prijalo zákon č. 256/1992 Zb. o ochrane osobných údajov v informačných systémoch. Ten v § 10 definoval ako dotknutú len fyzickú osobu. Na medzinárodnej úrovni už v tom čase existoval Dohovor č. 108, avšak Česká a Slovenská Federatívna Republika nebola jeho signatárom. Oznámenie v Zbierke zákonov Slovenskej republiky z roku 2001 týkajúce sa Dohovoru č. 108 (oznámenie Ministerstva zahraničných vecí Slovenskej republiky č. 49/2001 Z. z.) nevykonalo notifikáciu podľa čl. 3 ods. 2 písm. b) o jeho rozšírení na právnické osoby a Rada Európy takúto notifikáciu dosiaľ neeviduje.

43. Zároveň však jazykový výklad čl. 19 a čl. 22 ústavy existenciu ochrany u právnických osôb neobmedzuje, a preto ani u nich nemožno túto ochranu úplne vylúčiť (m. m. PL. ÚS 10/08, podobne v nemeckej doktríne BVerfG, sp. zn. 1 BvR 1550/03, body 151 až 154). Popri ochrane prostredníctvom ochrany súkromia sa môžu v ústavnom kontexte aj právnické osoby dovolávať ochrany pred systematickým neoprávneným zhromažďovaním údajov (čl. 22 ods. 1 a čl. 19 ods. 3) alebo pred narušením listového tajomstva (čl. 21 ods. 1). Táto parciálna ochrana však plne nezodpovedá ochrane fyzických osôb, najmä tam, kde sa právo dotýka ľudskej dôstojnosti. Činnosť právnických osôb je viac účelová, a preto je aj ústavnoprávna ochrana užšie koncipovaná.

44. Zároveň ochranu súkromia a osobných údajov je nutné odlíšiť od ochrany majetkových pozícií podľa čl. 20 ústavy, a to či už hmotného (napr. obchodných priestorov), alebo nehmotného charakteru (napr. typicky obchodného tajomstva), alebo práva na výkon povolania podľa čl. 35 ústavy. V porovnaní s čl. 35 ústavy sa parciálna ochrana súkromia právnických osôb poskytuje bez potreby zákonnej úpravy v zmysle čl. 51 ods. 1 ústavy. Na rozdiel od ochrany majetkových pozícií nie je uplatnenie závislé od existencie vlastníckeho alebo iného práva, ako napríklad práva na obchodné tajomstvo [pozri II. ÚS 647/2014, bod 45 a k jeho ústavnej ochrane pozri tiež APLIN, T. *Right to Property and Trade Secrets in Christpophe Geiger (ed) Research Handbook on Human Rights and Intellectual Property* (Edward Elgar, 2015), kapitola 22, s. 421 – 437].

45. Práva na ochranu súkromia a osobných údajov nie sú absolútne práva, a preto môžu byť primerane okolnostiam obmedzené (PL. ÚS 12/01, PL. ÚS 10/2014, bod 95, PL. ÚS 13/2020, ods. 70). Akékoľvek obmedzenie však musí byť dostatočne určité, primerané okolnostiam zásahu a poskytovať silné záruky proti zneužitiu (PL. ÚS 10/2014, body 95, 102 a 133). Ústavný súd pri prieskume uplatňuje svoj klasický test troch základných kritérií: legality, legitimity a proporcionality (PL. ÚS 23/06, PL. ÚS 3/09, PL. ÚS 3/00, PL. ÚS 67/07). Odlišuje pritom rôzne stupne intenzity zásahu do súkromia a osobných údajov (PL. ÚS 10/2014, bod 81) od minimálneho cez mierny až po závažný alebo obzvlášť závažný zásah.

46. V kontexte zberu a sprístupňovania osobných údajov vzhľadom na trvácny charakter zásahu do práv navyše ústavný súd vo svojej judikatúre zdôrazňuje, že okrem povinnosti zákonodarcu

formulovať zásah adekvátne vzhľadom na sledovaný cieľ musí byť zákon aj dostatočne ošetrený formou kontinuálnych efektívnych zákonných záruk proti zneužitiu údajov.

47. Na základe týchto východísk teda ústavný súd pristúpil k prieskumu napádaného zákona.

1. K zberu a lokálnemu uchovávaniu údajov pri kúpe v obchode vrátane vydania pokladničného bloku:

48. Zo zákona vyplýva predajcovi ako podnikateľovi povinnosť zadokumentovať každú tržbu a ZoERP v § 8 ods. 1 ustanovuje rozsah údajov, ktoré je predajca povinný zbierať, ako napríklad cenu tovaru alebo služby, typ tovaru, miesto a čas predaja, rozpis odvedenej dane a pod. Tieto údaje sú fyzicky vytlačené na pokladničnom bloku, ktorý je ponúknutý kupujúcemu, a uložené v pamäti pokladne na dobu potrebnú pre zákon č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov (ďalej len „zákon o účtovníctve“), a teda 10 rokov (§ 35 zákona o účtovníctve). Navrhovatelia napádajú aj tento zber údajov podľa § 8 ods. 1 písm. b) a g) ZoERP. Podľa dotknutých ustanovení musí každý pokladničný doklad vyhotovený elektronickou registračnou pokladnicou obsahovať „b) daňové identifikačné číslo, ak podnikateľ nie je platiteľom dane z pridanej hodnoty... g) označenie tovaru alebo označenie služby, množstvo tovaru alebo rozsah služby a priradenie sadzby dane z pridanej hodnoty okrem prípadu, ak platiteľ dane z pridanej hodnoty uplatňuje osobitnú úpravu uplatňovania dane podľa osobitného predpisu“.

49. Z podania nie je zrejmé, prečo navrhovatelia napadli uvádzanie týchto údajov na pokladničnom doklade a ich lokálne ukladanie na zariadení pokladnice v § 8 ZoERP, pretože argumenty navrhovateľov smerujú skôr k ich následnému odovzdávaniu do centrálnej databázy, ktoré je upravené v § 8a ZoERP. Zaznamenanie identifikácie predávajúceho spolu so zoznamom tovarov a služieb, ich množstvom a použitou sadzbou dane je desaťročia medzinárodne uznávaným spôsobom dokladovania kúpy v obchode. Slúži jednak na ochranu podnikateľa pred nečestnými zamestnancami, ale aj spotrebiteľa pred nečestnými podnikateľmi. Táto povinnosť napomáha pri vedení účtovníctva podnikateľov a asistuje štátu pri výbere daní, resp. kontrole iných zákonných povinností a spotrebiteľom pri reklamácii tovarov alebo služieb.

50. Intenzita zásahu do oboch práv zákazníkov a predajcov je v kontexte lokálneho zberu týchto údajov pomerne nízka a poľahky ospravedlniteľná (pozri ďalej).

51. V prípade kupujúcich nie sú pokladničné bloky, resp. ich lokálne kópie na zariadeniach podľa tohto ustanovenia ešte nijak centralizované a vzájomne prepojené, a preto poskytujú len minimálne vzhliadnutie do ich súkromia. Kupujúci totiž síce prostredníctvom každého nákupu zanechá po sebe určitú údajovú stopu (zoznam nakúpených výrobkov v čase a mieste), no z desiatok jednotlivých záznamov u rôznych predajcov je náročné a nákladné spätne agregovať dáta a identifikovať konkrétnu osobu a jej nákupné správanie. V každom prípade pokiaľ štát alebo jeho orgány tieto údajové stopy žiadnym spôsobom nezbierajú a neanalyzujú, zásah do súkromia kupujúceho je minimálny.

52. V prípade súkromia a osobných údajov predávajúcich síce ide o systematické monitorovanie ich činnosti, avšak cieľom tejto záznamovej povinnosti je riadny výber daní, ochrana spotrebiteľa a zdravej konkurencie, a preto § 8 ods. 1 písm. b) a g) ZoERP v tomto prípade bezpochyby sleduje legitímny záujem.

53. Z pohľadu proporcionality predmetné ustanovenie vyžaduje zahrnutie len takých informácií, ktoré sa striktne týkajú ťažiska podnikateľskej činnosti. Ich zber je nevyhnutný z hľadiska splnenia účtovných a daňových povinností. Opakované evidovanie toho, že určitý podnikateľ predal určité tovary za určitú cenu v určitý deň na určitom mieste, no neurčitým osobám, len ťažko možno považovať za nadmerný štátny dirigizmus pri súčasných technologických možnostiach. Údaje o predaných tovaroch a službách nejdú nijak nad rozsah nevyhnutného, keďže sa obmedzujú len na „označenie tovaru alebo označenie služby“, a teda nie ich podrobnú špecifikáciu. Naopak, základné informácie o ich predanom množstve a uplatňovanej sadzbe sú všetky dôležité z pohľadu ochrany spotrebiteľa a výberu daní. Bez označenia tovaru a jeho množstva si spotrebiteľ nedokáže skontrolovať riadne naúčtovanie nákupu a finančná správa autenticitu zaúčtovania transakcie. Na rozdiel od navrhovateľmi spomenutej českej úpravy slovenská nikdy nenúti predajcu, aby na pokladničnom doklade uvádzal svoje rodné číslo (porovnaj nález Ústavného súdu Českej republiky sp. zn. Pl. ÚS 26/16, ods. 100 a 101). Informácie uložené v elektronických registračných pokladniach, ako aj na tlačených pokladničných blokoch sú navyše chránené proti zneužitiu [§ 9, § 11, § 16a písm. p) ZoERP].

54. Z týchto dôvodov ústavný súd dospel k záveru, že § 8 ods. 1 písm. b) a g) ZoERP bezpochyby sleduje legitímny záujem. Zásah do súkromia zákazníkov je zároveň minimálny. Zásah do súkromia predajcov, ktorí sú podnikateľmi, je pri lokálnom zbere a uchovávaní dát minimálny až mierny. Zákonná povinnosť vydávať a uchovávať si vydané pokladničné bloky o transakciách je proporcionálna, pretože rozsah zbieraných údajov je adekvátny vzhľadom na cieľ ochrany spotrebiteľa a výberu daní. Navrhovatelia ani v tomto smere nepoukázali na menej invazívne riešenia, ako tento legitímny cieľ dosiahnuť. Ústavný súd vzal do úvahy aj väzbu § 8 ods. 1 písm. g) ZoERP na ustanovenie § 16 ods. 1 písm. d) zákona č. 250/2007 Z. z. o ochrane spotrebiteľa a o zmene zákona Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov vyžadujúce vydanie dokladu o kúpe výrobku alebo o poskytnutí služby predávajúcim spotrebiteľovi, v ktorom sú uvedené o. i. aj názov a množstvo výrobku alebo druh služby. Nie je preto zrejmé, aké šetrnejšie spôsoby zadokumentovania nákupu sú možné, pričom už aj tie existujúce nemožno bez ďalšieho považovať za neprimerane invazívne do súkromia predajcov.

55. Obdobná situácia je zreteľná aj z pohľadu čl. 7 a 8 charty, ktoré sa aplikujú vzhľadom na únijné pravidlá o ochrane osobných údajov (GDPR), do ktorých pôsobnosti spadá zber a prístup, správanie finančnej správy (pozri ďalej). V kumulácii s inými údajmi môže ísť o osobné údaje predávajúceho (pozri najmä bod 76 odôvodnenia tohto nálezu), ktoré sú spracúvané automatizovaným spôsobom (pozri čl. 2 ods. 1 a čl. 4 ods. 1 a 2 GDPR), pričom na relevantných podnikateľov sa neaplikuje žiadna výluka z pôsobnosti (čl. 2 GDPR). Je pritom nepodstatné, že sa informácie týkajú profesijnej činnosti podnikateľov (*Volker*, C-92/09 a C-93/09, body 57 až 59). Keďže navrhovatelia v tomto smere nijak nenačrtli svoju argumentáciu, pretože sa primárne sústredili na následné spracúvanie údajov v systéme e-kasa, ústavný súd nehľadal ďalšie dôvody na prípadnú nesúladnosť dotknutých ustanovení v štádiu ich lokálneho zberu a uchovávania. Z pohľadu charty a súvisiacej judikatúry k čl. 7 a 8 sú rovnako dôležité už uvedené zistenia, že na zber údajov existuje riadny právny základ, ktorý sleduje legitímny záujem (čl. 52 ods. 1 charty, napr. *Volker*, C-92/09 a C-93/09, body 65 až 77). Keďže údaje sa v tomto kroku nijak nezverejňujú a slúžia len vnútorným záznamom firmy, pričom sú predmetom aj rôznych záruk, zákonodarca riadne zohľadnil aj test proporcionality (porovnaj, *Volker*, C-92/09 a C-93/09, bod 78 a nasl.). Napokon z hľadiska dohovoru taktiež

situácia nie je odlišná, čo je zrejmé už z toho, že v oblasti daňových predpisov sa všeobecne v kontexte ochrany súkromia uplatňuje širšia možnosť uváženia členského štátu (*G.S.B. proti Švajčiarsku*, č. 28601/11, bod 93, hoci to neplatí vždy, pozri *M.N. a ďalší proti San Marinu*, č. 28005/12, body 52 – 53).

2. K automatizovanému odosielaniu a uchovávaniu údajov v centrálnej databáze finančnej správy v reálnom čase:

56. Navrhovatelia svojím podaním ďalej žiadajú o preskúmanie tých častí § 8a ods. 1 ZoERP, ktoré vedú k zasielaniu určitého typu údajov do centralizovaného systému e-kasa. V kontexte odosielaných údajov napádajú len *„daňové identifikačné číslo“* predávajúceho a *„unikátny identifikátor kupujúceho“*. Nenamietajú preto zber a odosielanie údajov o zozname a množstve tovarov a služieb alebo o mieste a čase nákupu. Vzhľadom na to, že prípadný zásah do súkromia predávajúceho a kupujúceho je možné posúdiť len v kontexte všetkých zbieraných údajov, ústavný súd vo svojom prieskume berie do úvahy aj zber týchto údajov, aj keď nebude osobitne posudzovať ich súladnosť, len existenciu spoločných záruk.

2.1. Zber osobných údajov predávajúceho:

57. Podľa navrhovateľov je zber daňového identifikačného čísla predávajúceho v rámci systému e-kasa neprimeraným zásahom do súkromia a ochrany osobných údajov.

58. Daňové identifikačné číslo prideľuje správca dane každému daňovému subjektu pri registrácii a slúži na jeho identifikáciu pri styku s finančnou správou. Predstavuje jedinečný identifikátor vytvorený pre každý daňový subjekt bez toho, aby obsahoval rodné číslo alebo dátum narodenia. Daňové identifikačné číslo slúži na jednoznačnú identifikáciu daňového subjektu finančnou správou, preto bol tento identifikátor zvolený aj pre identifikáciu podnikateľa, ktorý zasiela údaje do systému e-kasa. Nedošlo k vytvoreniu nového alebo iného identifikátora a ani k použitiu identifikátora postaveného na rodnom čísle alebo dátume narodenia. V napadnutých ustanoveniach ide o daňové identifikačné číslo predávajúceho, resp. poskytovateľa služby, a nie kupujúceho (aj keby bol podnikateľom).

59. Ak by ústavný súd považoval tento údaj sám osebe za neprípustný, znamenalo by to, že systém e-kasa nemôže priamo poznať identitu podnikateľa. Bez identifikácie predávajúceho má ale centralizovanie pokladničných dokladov finančnou správou len veľmi obmedzený zmysel. Cieľom systému e-kasa je zlepšiť výber daní tým, že sa podnikateľom zúži priestor na neregistrované platby, a tým daňové úniky. Takýto systém môže plniť tento cieľ len vtedy, ak dokáže identifikovať predávajúceho. Následná fyzická kontrola totiž umožňuje finančnej správe porovnať centrálne uložené záznamy s tými, ktoré sú predložené zo strany podnikateľa [pozri aj prípadové štúdie z iných krajín v OECD (2019), Implementing Online Cash Registers: Benefits, Considerations and Guidance, OECD, Paris]. Nad rozsah DIČ predávajúceho má navyše finančná správa k dispozícii veľké množstvo nepriamych identifikátorov, ktoré navrhovateľmi neboli napadnuté.

60. Na druhej strane, týmto zákonným opatrením dochádza k permanentnému monitorovaniu podnikateľov týkajúcemu sa toho, čo a za koľko, kedy a kde predávajú. Na rozdiel od jednoduchého ukladania pokladničných blokov u podnikateľa pre prípad kontroly cez systém e-kasa informácie štát získava v agregovanej podobe pre celý trh a v reálnom čase, t. j. v čase, keď sa realizujú

transakcie v obchode. Údaje takto uchováva po dobu 10 rokov (pozri ďalej). Štát tak disponuje náhľadom do všetkých dotknutých transakcií predávajúcich bez toho, aby musel permanentne realizovať daňovú kontrolu. Zber údajov sa týka všetkých podnikateľov bez ohľadu na ich predchádzajúce správanie alebo minulosť. Údaje v systéme e-kasa majú potenciálne veľkú výpovednú hodnotu o podnikaní. Tieto podrobne mapujú, kedy je ktorá prevádzka podnikateľa otvorená, koľko rôznych pokladníc tam prevádzkuje, v akej intenzite, koľko zákazníkov a v akom čase počas dňa má, koľko zvyknú pri nákupoch zaplatiť, ktoré výrobky sú najviac predávané, ako sa ich ceny líšia v priebehu roka, prípadne podľa druhu prevádzok aj počas dňa. Ide preto skutočne o citeľný plošný zásah do práva na súkromie a osobných údajov predávajúcich.

61. Vo všeobecnej rovine je ale takýto zber údajov odôvodniteľný záujmom na riadnom výbere daní, preto úprava § 8a ods. 1 ZoERP, ktorá je zároveň aj dostatočne určitá, nepochybne sleduje legitímny cieľ. Otáznou tak zostáva predovšetkým proporcionalita zásahu.

62. Pri posudzovaní proporcionality tohto systematického centralizovaného zberu dát je však zrejmé, že výsledok závisí od toho, aké ďalšie údaje sú zbierané, na aký účel a ako sú následne používané zo strany štátnych orgánov. Samotný zber daňového identifikačného čísla môže byť len ťažko neproporcionálny. Ostatne, štát sám udeľuje toto číslo podnikateľovi práve na účely identifikácie v kontexte daňových povinností. Zber DIČ však môže byť problematický v kontexte, ak by spolu s ním zbierané údaje boli neprimerané vzhľadom na deklarovaný účel boja proti kráteniu daní. Takýto prieskum by však vyžadoval, aby navrhovatelia napadli aj iné údaje, ktoré sú spolu s DIČ takto zbierané, ako napríklad zoznam tovarov a služieb alebo miesto a čas predaja. Pretože sú to tieto údaje, ktoré by spolu s DIČ mohli byť prípadne neproporcionálne vzhľadom na deklarovaný cieľ, DIČ samo osebe len tieto ostatné údaje individualizuje. Navrhovatelia však napadli v §8a ods. 1 ZoERP len odovzdávanie DIČ. Ústavný súd je obmedzený petitom navrhovateľov, a teda na to, aby posúdil proporcionalitu celkového penza údajov, ktoré sú vstupom do systému e-kasa, ako aj ich vzťah k iným údajom, niet návrhu. Z tohto dôvodu ústavný súd preskúmal len otázku spoločných podmienok spracúvania týchto údajov, a teda to, či DIČ spoločne s ostatnými údajmi je dostatočne zákonne ošetrené proti prípadnému zneužitiu (pozri odsek 76 a nasl.).

2.2. Zber osobných údajov kupujúceho:

63. Kritickým bodom právnej úpravy je prípadný zásah do súkromia a práva na ochranu osobných údajov kupujúceho. Podľa §8a ods. 1 ZoERP je podnikateľ „povinný pri evidovaní tržby v pokladnici e-kasa klient zabezpečiť, aby pokladnica e-kasa klient zasielala do systému e-kasa... unikátny identifikátor kupujúceho, ak je predložený kupujúcim pred zaevidovaním prijatej tržby“. Podľa § 2 písm. q) ZoERP je unikátny identifikátor kupujúceho „číselný znak alebo alfanumerický reťazec, ktorý slúži na identifikáciu kupujúceho; unikátnym identifikátorom kupujúceho môže byť daňové identifikačné číslo“. V praxi teda ide o rôzne typy identifikátorov. Môže tak ísť o DIČ podnikateľa, číslo klubovej karty fyzickej osoby alebo akýkoľvek iný ľubovoľný identifikátor. Zákon, ako aj dôvodová správa predpokladajú, že kupujúcim je aj nepodnikateľ.

64. Z dikcie zákona je zrejmé, že unikátny identifikátor kupujúceho zákon nevyžaduje zbierať vždy. Ak zákazník odovzdá údaj pri kúpe, je povinnosťou predávajúceho tento údaj odovzdať do e-kasy. Na tomto výklade sa zhodlo aj finančné riaditeľstvo a predseda najvyššieho súdu. Zákon

nepredpokladá, že by kupujúci údaj použil (napr. klubovú kartu), ale predávajúci nemal povinnosť ho do systému odoslať. Neodovzdanie údaja v takom prípade vedie k spáchaniu správneho deliktu predávajúcim podľa § 16a písm. c) ZoERP, pričom dôsledkom je nielen uloženie pokuty, ale potenciálne aj zákaz predaja v prípade neuhradenia pokuty (§ 16b ods. 8 ZoERP). Hoci finančná správa trvá na dobrovoľnosti zberu tohto údaja, zákon dobrovoľnosť negarantuje. Zákon totiž nestanovuje žiadne požiadavky, za akých okolností môže predajca získať tento údaj od zákazníka. Ak údaj kupujúci použije, musí sa odoslať finančnej správe bez ohľadu na skutočnú vôľu zákazníka. Finančná správa podľa svojich slov dobrovoľnosť alebo súhlas na odovzdanie a spracúvanie tohto údaja nijako neoveruje. V takom prípade teda nemožno hovoriť o dobrovoľnosti.

65. Finančná správa a Generálna prokuratúra Slovenskej republiky namietajú, že unikátny identifikátor kupujúceho nie je osobný údaj, pretože s výnimkou použitia DIČ pre fyzickú osobu podnikateľa štátny orgán nevie, aký identifikátor bol komu pridelený. Ústavný súd v tomto smere pripomína, že čl. 19 ods. 3 a čl. 22 ods. 1 ústavy chránia pred zhromažďovaním a spracúvaním osobných údajov bez ohľadu na to, či ide o údaje, ktoré priamo identifikujú dotknutú osobu. Ako je aj z podústavnej ochrany osobných údajov zrejmé, kvalifikácia toho, čo je osobný údaj, závisí od toho, akými údajmi už štátny orgán disponuje a aké má právne možnosti získania ďalších informácií. Pokiaľ orgán verejnej moci spracúvajúci údaje vzhľadom na svoje právomoci a iné informácie, ktoré má k dispozícii, dokáže po vynaložení primeraného úsilia identifikovať konkrétneho jednotlivca, stále ide o osobné údaje. Je preto nepodstatné, že ide o údaje, ktoré jednotlivca neidentifikujú priamo [pozri SDEÚ, Breyer, C582/14, ods. 49; čl. 4(1) GDPR, ale aj *Benedik proti Slovinsku*, č. 62357/14, body 107 – 108 a 113, *Amann proti Švajčiarsku*, č. 27798/95, bod 65; *Haralambie proti Rumunsku*, č. 21737/03, bod 77]. Z rovnakých východísk vychádza aj zahraničná ústavnoprávna judikatúra, keď napríklad evidenčné čísla áut považuje za nepriamo identifikujúce jednotlivca (BVerfG, sp. zn. 1 BvR 142/15, bod 97). Ak preto údaje po vložení do mozaiky právomocí a ďalších existujúcich údajov u daného orgánu verejnej moci môžu pri zapojení primeraného úsilia viesť k identifikácii jednotlivca, uplatní sa ochrana podľa čl. 19 ods. 3 a čl. 22 ods. 1 ústavy. V ďalšom prieskume preto treba zohľadniť aj rozsiahle kontrolné právomoci finančnej správy [pozri napr. § 17a ods. 1 a 4 ZoERP, § 14, § 20, § 29 ods. 2 zákona č. 35/2019 Z. z. o finančnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „ZoFS“)].

66. V tomto prípade finančná správa síce nevie priamo z čísla klubovej karty vyčítať, o koho ide, dokáže to ale zistiť nepriamo, napríklad pri kontrole platieb, dopytom u predávajúceho alebo inak. Podľa jej vlastného vyjadrenia pri nákupoch prekračujúcich určitý limit *„platí povinnosť pre predávajúceho vedieť identifikovať odberateľa (podnikateľ, nepodnikateľ) pri nákupe v hotovosti alebo pri platbe kartou“*. Navyše, identifikácia z UIK je možná aj bez realizácie kontrolných oprávnení zo strany finančnej správy, kedykoľvek sa kupujúci prostredníctvom stránky finančnej správy snaží overiť autenticitu svojho pokladničného bloku. Unikátny identifikátor kupujúceho je preto z pohľadu finančnej správy nepochybne nutné kvalifikovať ako osobný údaj so všetkými dôsledkami.

67. Vzhľadom na už uvedené je zrejmé, že prípadné odovzdávanie unikátneho identifikátora kupujúceho podľa § 8a ods. 1 ZoERP predstavuje zásadný zásah do práva na súkromie a ochranu osobných údajov kupujúceho. Hoci dnes štát v zásade nedokáže priamo priradiť, kto, čo, kde a kedy

kúpil ku konkrétnym osobám, takto centrálne zbierané údaje to môžu umožniť, ak by sa akýkoľvek štátny orgán s prístupom rozhodol realizovať svoje zákonné právomoci. Toto konštatovanie platí bez ohľadu na to, že tento zber je dnes vzhľadom na technickú realizáciu zanedbateľný. Ako ústavný súd už v minulosti (PL. ÚS 13/2020, bod 78) zdôraznil, pri abstraktnej kontrole ústavnosti je nutné zohľadniť nielen existujúce zásahy vyplývajúce z aktuálnej aplikácie zákonného znenia, ale aj riziká vyplývajúce z jeho budúceho možného uplatnenia. Právny predpis preto nemožno v tomto konaní obhájiť tým, že jeho konkrétna implementácia v danom čase nevyužíva v plnom rozsahu vytvorený zákonný rámec. Ústavný súd posudzuje nielen existujúci, ale aj potenciálny zásah do práv, ktorý vyplýva z výkladu abstraktného znenia právnej úpravy.

68. Ústavný súd sa teda zameral na posúdenie legitimity, legality a proporcionality zásahu formou zberu a ďalšieho spracúvania unikátneho identifikátora kupujúceho. Dospel pritom k záveru, že ustanovenie nespĺňa základnú ústavnú požiadavku konkrétnosti legitímneho účelu (nedostatok legitimity). Keďže napadnuté ustanovenie neprešlo testom legitimity, je potom už ďalšie pokračovanie testu proporcionality bezpredmetné.

69. Zákonodarca a finančná správa nedokázali ani po mesiacoch dostatočne artikulovať dôvod na zber týchto údajov. Jediné, čo komunikovali ústavnému súdu, sú abstraktné plány, ktoré zatiaľ nie sú realizované alebo ani dopracované. Vo vzťahu ku kupujúcim, ktorí sú podnikateľmi, vyjadrenia zdôrazňujú budúcu klientsku zónu. Podľa ich vyjadrení ak by sa v budúcnosti ako údaj použilo DIČ, mohol by tak mať každý podnikateľ určité výhody pri preukazovaní svojich výdavkov v daňovom systéme. Lenže v súčasnosti údaj nie je obmedzený len na DIČ podnikateľa, nie je povinný alebo jasne zvýhodňovaný a takáto klientska zóna navyše neexistuje.

70. Nedostatok konkrétneho legitímneho účelu je ešte zrejmejší pri kupujúcich nepodnikateľoch. Finančná správa ani tu dostatočne nedokázala artikulovať žiadny konkrétny účel v kontexte zberu údajov, ktorý by tento zber odôvodňoval. Jeden z dokumentov, ktorý interne predstavuje e-kasu, krátko spomína blokovú lotériu alebo reklamačné konanie ako spôsoby použitia údajov. Lotéria sa však dnes realizuje inak, keďže overovanie pokladničných blokov vyžaduje iniciatívu zákazníka. Je preto zrejmé, že akékoľvek údaje o kupujúcom nepodnikateľovi sú v systéme zavedené úplne zbytočne.

71. V súčasnosti neexistuje žiadny konkrétny legitímny cieľ, pre ktorý by štát v kontexte e-kasy zbieral unikátny identifikátor kupujúceho. Jediné, čo ústavný súd vo vyjadreniach postrehol, sú už spomínané plány do budúcna. Ústavný súd vo svojej predchádzajúcej judikatúre už jasne povedal, že nie je možné, aby štát zber údajov odôvodňoval len budúcimi plánmi (PL. ÚS 13/2020, rovnako BVerfG, sp. zn. 1 BvR 1550/03, bod 97).

72. Ako z rozhodnutia vo veci sp. zn. PL. ÚS 13/2020 vyplýva, zákonodarca musí v kontexte systematického zberu dát jasne a určito upraviť, aké údaje a na aký účel zbiera. Nemôže sa pritom skrývať len za vágne ustanovenia (napr. PL. ÚS 19/09, bod 57, PL. 13/2020, bod 84).

73. Neurčitosť právnej úpravy však môže byť aj vo formulácii jej konkrétneho legitímneho účelu. Právna úprava môže byť určitá, pokiaľ ide o to, čo a ako sa má zbierať, avšak zároveň môže zahmlievať dôvody toho, prečo sa tak robí. Je to tak práve v prípade unikátneho identifikátora kupujúceho, pretože takéto ustanovenie nerealizuje konkrétny cieľ. Konkrétny cieľ, pre ktorý sa zbierajú predmetné údaje, musí byť zrejmý už z legislatívneho procesu. Bez toho, aby už

v legislatívnom procese existoval jasný plán, na aký sa majú údaje použiť, nemožno hovoriť o konkrétnom legitímnom cieli ich spracúvania. Zákonodarca tak môže už dnes urobiť vo svojej dôvodovej správe alebo aj priamo v normatívnom texte. Ak by ústavný súd akceptoval takéto „zahmlené“ ustanovenia v právom poriadku, akýkoľvek zber a používanie údajov by bolo možné ľahko odôvodniť, ak existuje aspoň nejaký mysliteľný budúci cieľ, ktorý si možno dotvoriť *ex post* podľa ľubovôle. Ak štát potrebuje konkrétne údaje od svojich občanov, musí v prvom rade vedieť vysvetliť, na aký konkrétny účel ich potrebuje. Nestačí uviesť to, že ich možno raz bude potrebovať.

74. Z už uvedeného vyplýva, že § 8a ods. 1 ZoERP nie je v súlade s čl. 19 ods. 2 a 3 ústavy v časti umožňujúcej zber a odosielanie údajov o unikátnom identifikátore kupujúceho a tiež aj s čl. 16 ods. 1 ústavy, pretože tento zásah do súkromia a ochrany osobných údajov kupujúcich nesleduje žiadny existujúci konkrétny cieľ a údaje sú dnes zbierané pre teoretický budúci účel. Z dôvodov uvedených v bodoch 29 a 30 tohto odôvodnenia je osobitný prieskum podľa ustanovení charty nadbytočný.

3. K spracúvaniu údajov finančnou správou vrátane ich poskytovania ďalším štátnym orgánom na iné účely:

75. Keďže ústavný súd považuje § 8a ods. 1 ZoERP v časti týkajúcej sa unikátneho identifikátora kupujúceho za protiústavný, ostáva len posúdiť spracúvanie a prístup k údajom predávajúceho odosielaným do e-kasy. Ústavný súd skúmal, akým spôsobom v súčasnosti dochádza k používaniu týchto údajov v rámci a mimo finančnej správy, na akom podklade a aké záruky proti zneužitiu predpokladá zákon. Ako bude ďalej vysvetlené, ústavný súd dospel k záveru, že nakladanie s údajmi podľa § 8a ods. 1 ZoERP je možné vykladať ústavnokonformne, avšak tento výklad zároveň vylučuje niektoré spôsoby použitia údajov, ktoré v súčasnosti vykonáva finančná správa. Vzhľadom na to, že niektoré tieto použitia musí upraviť zákonodarca, ústavný súd zhrnul základné ústavné parametre potrebnej úpravy, aby tak poskytol užitočnú odpoveď. Len pre pripomenutie, ako bolo už v odseku 63 uvedené, ústavný súd v rámci konania nemohol skúmať, či je celý zákonný rozsah údajov, ktorý je odosielaný do systému e-kasa, v súlade s právom na ochranu súkromia a osobných údajov. Navrhovatelia totiž napadli len odosielanie DIČ, a nie iných položiek.

76. Ako už bolo uvedené, systém e-kasa vytvára permanentné systematické monitorovanie podnikateľov týkajúce sa toho, čo a za koľko, kedy a kde predávajú. Ak by jej súčasťou bol aj unikátny identifikátor kupujúceho, dokonca by štát sledoval, komu tieto tovary alebo služby predávajú. Prostredníctvom DIČ je vždy zrejmé, o ktorého predávajúceho presne ide. Zásah je o to silnejší, že štát zbiera tieto údaje v agregovanej podobe pre celý trh a v reálnom čase. Navyše, tieto údaje uchováva po veľmi dlhé obdobie a využíva na posudzovanie rizikovosti jednotlivých podnikateľov (pozri ods. 117 a nasl.), a preto k údajom, ktoré kedysi vyžadovali fyzickú kontrolu a aktiváciu súvisiacich ochranných mechanizmov, dnes možno pristúpiť bez vedomia predajcu. Je pritom nepodstatné, že istá časť týchto informácií môže byť súčasne dostupná verejnosti inak (podobne ESĽP k daňovým údajom vo veci *Satakunnan Markkinapörssi Oy and Satamedia Oy proti Fínsku*, č. 931/13, bod 138).

77. Zároveň však pri predávajúcich ide o podnikateľov, ktorí vo vzťahu k výkonu svojej podnikateľskej činnosti musia strpieť širšiu mieru zásahov. Údaje o transakciách v obchode sú bez

ich priradenia ku konkrétnym osobám menej výpovedné. Bez údajov o kupujúcich preto nejde o „zvlášť závažný zásah“ ako pri prevádzkových a lokalizačných údajoch telekomunikačných operátorov alebo odpočúvaní (pozri PL. ÚS 10/2014, bod 113; III. ÚS 97/2012, body 4.3.4, 4.3.6). Na rozdiel od údajov z telekomunikačnej prevádzky sa údaje menej sústreďujú na aktivitu konkrétnych ľudí o ich osobnom živote, stále však ide o plošný, a teda necielený zber množstva údajov s veľkou výpovednou hodnotou. Ústavný súd preto zber a spracúvanie údajov podľa § 8a ods. 1 ZoERP (bez údajov o kupujúcom) považuje za závažný zásah do práva na súkromie a osobných údajov predávajúcich podnikateľov.

78. Závažnosť zásahu musí byť preto zo strany právnej úpravy ošetrená prostredníctvom záruk proti zneužitiu týchto údajov. Čím hlbšie zákonodarca obmedzuje práva jednotlivca, o to silnejšie záruky musí poskytnúť pri ochrane práv pred ich možným zneužitím (PL. ÚS 13/2020, bod 88). Táto požiadavka sa vzťahuje jednak na obsah záruk, ale aj ich legislatívnu určitosť (PL. ÚS 13/2020, bod 84). Ústavný súd vo svojej judikatúre pri závažných až obzvlášť závažných zásahoch vyžaduje, aby sa zákonodarca vysporiadal aj s okruhom záruk proti zneužitiu (pozri PL. ÚS 13/2020, bod 86).

79. Najprv je však nutné zosumarizovať súčasné spracúvanie údajov tak, ako ho ústavnému súdu vysvetlila finančná správa. Z vyjadrení je zrejmé, že používanie údajov je zatiaľ len v počiatkoch. Údaje z centrálnej databázy e-kasa sú dnes využívané takto:
(A) *Overovanie bločkov*: verejnosť môže overiť pravosť vydaných pokladničných blokov.
(B) *Podnikateľská zóna*: predajca vidí svoje pokladničné bloky v osobitnej sekcii.
(C) *Centrálny register pokladníc*: vybraní zamestnanci finančného riaditeľstva môžu vidieť jednotlivé pokladničné bloky a ich sumarizáciu.
(D) *Analytický prístup*: zamestnanci oddelenia evidencie tržieb majú hromadný prístup k všetkým údajom, aby mohli realizovať daňové kontroly. Tu sa údaje spájajú s inými na účely vyhodnocovania rizikovosti daňových subjektov. Kontrolóri majú aj osobitné prenosné zariadenia, kde vidia prísun dát v reálnom čase v teréne.

80. Samotný ZoERP nejasne formuluje spôsob použitia údajov. Konkrétne, § 17 ods. 9 ZoERP predpokladá používanie údajov z e-kasy „na účely tohto zákona“. Ustanovenie § 17 ods. 1 ZoERP predpokladá použitie týchto údajov pri kontrole dodržiavania ZoERP ako dôkaz. Napokon podľa § 17 ods. 1 ZoERP „Finančné riaditeľstvo umožní verejnosti overiť, či boli údaje z pokladničných dokladov vyhotovených pokladnicou e-kasa klient zaslané do systému e-kasa“.

81. Z vyjadrení finančnej správy vyplýva, že podľa jej výkladu sú údaje minimálne teoreticky dostupné širokému okruhu ďalších štátnych inštitúcií na plnenie ich úloh podľa § 20, § 22 ods. 1 ZoFS. To by znamenalo, že hoci § 17 ods. 9 ZoERP explicitne vyžaduje použitie len na účely kontroly dodržiavania „tohto zákona“, údaje v rámci štátnej správy možno použiť aj na iné účely, ako sú tie, pre ktoré boli zbierané. Takýto výklad je však nutné s poukazom na potrebu ústavnokonformného výkladu odmietnuť.

3.1. K existencii záruk:

82. Finančná správa vo svojich vyjadreniach uviedla, že neprijala žiadne osobitné opatrenia na ochranu osobných údajov vo vzťahu k e-kase. Poukazuje na trestné právo a všeobecnú úpravu ochrany osobných údajov. Na konkrétnu otázku, či vykonala osobitné posúdenie vplyvu na ochranu osobných údajov podľa čl. 35 nariadenia Európskeho parlamentu a Rady EÚ č. 2016/679

z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov „GDPR“), odpovedala negatívne.

83. ZoERP neposkytuje priamo žiadne záruky proti zneužitiu prístupu k údajom zo systému e-kasa. Finančná správa poukazuje na ZoFS, ktorý sa aplikuje ako všeobecný predpis. Podľa § 20 ZoFS existujú tieto záruky:
- ak údaje už nie sú potrebné, majú sa zničiť (§ 20 ods. 6 ZoFS);
- každé tri roky sa má skontrolovať relevantnosť údajov (§ 20 ods. 7 ZoFS);
- prísnejšie požiadavky na zlučovanie údajov pri prechádzaní trestným činom (§ 21 ZoFS);
- protokolovanie prístupu zamestnancami na päť rokov (§ 29 ods. 6 ZoFS).

84. Ústavný súd vo svojej judikatúre pri závažných až obzvlášť závažných zásahoch vyžaduje, aby sa zákonodarca vysporiadal s týmto okruhom záruk proti zneužitiu (pozri PL. ÚS 13/2020, bod 86):
(i) subsidiarita používania získaných údajov,
(ii) jasné vymedzenie účelu použitia daných údajov,
(iii) kvalitný dohľad zo strany súdu alebo iných nezávislých inštitúcií,
(iv) zabezpečenie (mimoriadne) vysokej úrovne ochrany a bezpečnosti,
(v) časovo podmienené zničenie údajov a zároveň
(vi) vyrozumenie dotknutých osôb.

3.1.1. Subsidiarita používania údajov:

85. Subsidiarita používania získaných údajov znamená, že údaje sa majú získať z citlivejších zdrojov len vtedy, ak ich nemožno získať z menej citlivých zdrojov. Ak údaje možno vzhľadom na povahu opatrenia získať priamo od dotknutej osoby, ich spracovanie na základe jej súhlasu by malo byť pravidlom (PL ÚS 13/2020, bod 90). To nevylučuje, že v odôvodnených prípadoch súhlas nebude nutné žiadať (napr. ak to vylučuje povaha úkonu). Získanie súhlasu posilňuje legitimitu a primeranosť akéhokoľvek spracúvania osobných údajov, keďže sa odvíja od dôvery jednotlivca v pohnútky a správanie orgánu verejnej moci. Predovšetkým vo vertikálnych vzťahoch však treba upozorniť, že ak by bol súhlas získaný pod hrozbou negatívneho dôsledku, nemožno hovoriť o jeho dobrovoľnosti.

86. Finančná správa opísala vo svojich vyjadreniach obmedzenú funkcionalitu vyhľadávania v údajoch e-kasy. ZoERP umožňuje, aby na kontrolu dodržiavania zákona boli „využité aj všetky informácie uložené v systéme e-kasa“ (§ 17 ods. 1). Je pochopiteľné, že údaje odosielané do e-kasy nie sú získané na základe dobrovoľnosti. Ak štát chce bojovať proti daňovým podvodom formou kontroly, môže postupovať cielene alebo plošne, ale v každom prípade najmä nútene.

87. V súčasnosti nie je zrejmé, že by existoval menej invazívny spôsob, ako získať prístup k plošným dátam, ktoré by dokázali dokumentovať transakcie ako systém e-kasa, ktorý sa snaží donútiť podnikateľov evidovať a odviesť dane z každého realizovaného predaja, resp. poskytnutia služby. Evidovanie transakcií jasne súvisí s cieľom tohto systému, ktorý sa snaží predísť kráteniu daní. Pre ilustráciu, ak by štát takýto zber chcel využiť na kontrolovanie nesúvisiacich zákonných zákazov, napr. zákaz predaja počas sviatkov, išlo by zjavne o porušenie princípu subsidiarity, keďže tie možno kontrolovať na základe oveľa menej invazívnych prostriedkov.

3.1.2. Účel použitia údajov:

88. Jasné vymedzenie účelu použitia údajov znamená, že údaje musia byť použité na vopred stanovený účel, ktorý musí byť vymedzený v zákone. Účel je v tomto význame užším pojmom ako pojem „cieľ“ uvádzaný v čl. 13 ods. 4 ústavy (PL ÚS 13/2020, bod 91). Ako bolo už uvedené (bod 79), finančné riaditeľstvo pomenovalo štyri okruhy použitia údajov v rámci finančnej správy na „účely tohto zákona“.

89. Koncepcia e-kasy zdôrazňuje jej snahu o „vytvorenie predpokladov pre automatizovanú analýzu a správu údajov zhromaždených na serveri daňovej autority“. Podľa slovenskej prípadovej štúdie OECD finančná správa plánovala alebo stále plánuje informácie porovnávať dokonca aj s daňovými priznaniami jednotlivcov [OECD (2019), Implementing Online Cash Registers: Benefits, Considerations and Guidance, OECD, Paris, s. 27].

90. Účel použitia údajov je nutné rozlíšiť na použitie finančnou správou a použitie ďalšími štátnymi orgánmi. Podľa výkladu finančnej správy totiž ďalšie štátne orgány majú možnosť prístupu k údajom zo systému e-kasa. Finančná správa svoj výklad pritom opiera len o to, že ustanovenia ZoFS sa uplatňujú subsidiárne k ustanoveniam ZoERP ako *lex generalis*. Prístup iných orgánov podľa § 17 ods. 9 poslednej vety ZoERP sa vzťahuje len na tam špecifikované údaje, ktorými sú „meno, priezvisko, adresa trvalého pobytu, rodné číslo, telefónne číslo, adresa elektronickej pošty a IP adresa“.

91. Keďže celý zber údajov v systéme e-kasa je odôvodnený kontrolou dodržiavania tohto osobitného zákona, ústavný súd zastáva názor, že inou všeobecnou úpravou bez explicitného ustanovenia nemožno rozširovať rozsah prístupu k údajom na ďalšie účely pre iné štátne orgány.

92. Takáto legislatívna technika nespĺňa ústavnoprávne požiadavky na určitosť jej účelu pre tieto ďalšie spôsoby použitia údajov. Popiera totiž myšlienku, že akékoľvek údaje štát zbiera, musí tak robiť pre konkrétny účel, ktorý dokáže obhájiť v rámci legitímnosti a proporcionality. Akceptovanie takéhoto výkladu by znamenalo, že údaje zozbierané pre jeden účel možno následne voľne používať na akékoľvek ďalšie účely bez toho, aby tieto bolo treba osobitne posúdiť (podobne aj *Prokuratuur*, C-746/18, bod 50, alebo BVerfG, sp. zn. 1 BvR 142/15, bod 165). Umožnilo by sa tak, že verejnosť akceptuje zásadnú úpravu v legislatívnom procese pod rúškom istých účelov prístupu k dátam, zatiaľ čo po prijatí úpravy sa na základe kreatívnych výkladov tie isté údaje začnú poskytovať aj iným štátnym orgánom na iný ako pôvodný účel. Ústavný súd už vyslovil, že legitímny prístup k údajom o osobe nezíska orgán verejnej moci na základe všeobecného „prístupu k informáciám“, ale získa ho až vtedy, keď mu zákon prizná právo oboznámiť sa s údajmi zhromažďovanými na účel, ktorý je legitímny z hľadiska činnosti daného orgánu verejnej moci (III. ÚS 400/2016).

93. Zákonodarca musí preto explicitne v rámci prístupu k údajom, ktoré predstavujú závažný zásah do práv, upraviť, ktoré orgány a na aké konkrétne účely môžu mať prístup k akým údajom.

94. Z tohto dôvodu údaje podľa § 8a ods. 1 ZoERP v kontexte čl. 19 ústavy dnes možno použiť len vo vnútri orgánov finančnej správy a len na účely dodržiavania ZoERP. Keďže ZoERP je pomerne úzko koncipovaný zákon, z § 1 a § 16a ZoERP je možné pomerne jasne identifikovať, porušenie akých povinností takto možno kontrolovať. Tento ústavnokonformný výklad je potvrdený aj pri prieskume ďalšej podmienky, a to existencie kvalitného dohľadu.

95. Ak majú byť údaje zbierané podľa § 8a ods. 1 ZoERP do budúcna dostupné širšie medzi ostatnými štátnymi orgánmi, musí tak zákonodarca explicitne uviesť v kontexte týchto údajov. Nestačí pritom jednoduchá legislatívna poznámka s demonštratívnym výpočtom možných predpisov, ako to je v prípade poznámky k § 17 ods. 9 ZoERP. Poznámky pod čiarou nie sú súčasťou právneho predpisu a majú iba informatívnu hodnotu, a preto nesmú obsahovať údaje, ktoré majú normatívnu povahu. Každý ďalší prístup k údajom podľa § 8a ods. 1 ZoERP predstavuje osobitný zásah do práv, ktorý musí byť spôsobilý prieskumu ústavným súdom. To je možné len pri explicitnej zákonnej právnej úprave normatívneho charakteru.

3.1.3. Kvalitný nezávislý dohľad:

96. Kvalitný nezávislý dohľad znamená, že musí existovať nezávislá inštitúcia, ktorá dokáže vopred odfiltrovať alebo následne korigovať prípadné nedodržiavanie rozsahu a účelu právnej normy (PL. ÚS 13/2020, bod 92). Kvalitný nezávislý dohľad nemožno vykonávať bez dostatočného udelenia oprávnení a nástrojov kontroly. S nezávislým dohľadom súvisí aj potreba transparentnosti, ktorá umožňuje verejnú kontrolu nakladania s osobnými údajmi. Bez toho, aby bolo nutné ohroziť ochranu osobných údajov jednotlivcov alebo bezpečnosť systémov, sa má verejnosť možnosť oboznámiť s rozsahom používania prístupu k spracovávaným údajom (napr. štatistické ukazovatele, typy použitia, rozsah zabezpečenia a pod.).

97. Nad používaním údajov z e-kasy neexistuje žiadny osobitný dohľad. Úrad na ochranu osobných údajov má však všeobecnú pôsobnosť. Podľa § 29 ods. 6 ZoFS musí byť každý prístup k údajom protokolovaný, čím sa umožňuje spätná kontrola toho, kto a kedy mal prístup k akým dátam. Keďže úrad na ochranu osobných údajov má možnosť v rámci svojej kontroly skúmať aj tieto protokoly, existujú podmienky na efektívny dohľad používania údajov. Tento mechanizmus je ale efektívny len pri použitiach vo vnútri organizácie, keďže po odovzdaní údajov iným organizáciám už nedochádza k protokolovaniu z ich strany.

98. Z čl. 35 GDPR vyplýva podľa ústavného súdu jednoznačná povinnosť vykonať posúdenie vplyvu na ochranu údajov [pozri aj Christopher Kuner, Lee A. Bygrave, Christopher Docksey and Laura Drechsler: EU General Data Protection Regulation (GDPR): A Commentary (OUP, 2019), s. 531, 665]. Ako už bolo skôr vysvetlené, je nepochybné, že v prípade systému e-kasa ide o typ spracúvania s využitím nových technológií, ktorý s ohľadom na povahu, rozsah, kontext a účely spracúvania pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb. Toto konštatovanie platí o to viac, ak ho finančná správa využíva na automatizované posudzovanie rizikovosti podnikateľov, a preto čl. 35 GDPR poskytuje jednu zo záruk, ktorá vyplýva zo všeobecne aplikovateľnej úpravy.

99. Hoci čl. 35 GDPR nepredpisuje zverejnenie takéhoto posúdenia, dotknutí jednotlivci sa môžu domáhať jeho sprístupnenia podľa zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov (ďalej len „zákon o slobode informácií“). Len tak totiž môže jednotlivec uplatniť svoje práva prostredníctvom úradu na ochranu osobných údajov, ktorý môže vidieť aj nevyčiernené časti a reálne používanie údajov na základe protokolovania podľa § 29 ods. 6 ZoFS. Sprístupnenie takéhoto posúdenia podľa čl. 35 nemožno v celku odmietnuť podľa § 9 až 11 zákona o slobode informácií s poukazom na autorské práva, ochranu dotknutých osôb alebo obchodného tajomstva.

Keďže v praxi je táto otázka zjavne vysoko problematická a bráni jednotlivcom pri uplatnení ich práv [pozri situáciu opísanú v článku Šimona Chvojku: Ochrana soukromí v česko-slovenských chytrých karanténách (2021) 23. In: *Revue pro právo a technologie*, s. 18, poznámka pod čiarou č. 66 odkazujúca na rozhodnutie Úradu verejného zdravotníctva Slovenskej republiky č. OK/10825/2020], ústavný súd uvádza niekoľko základných východiskových bodov.

100. Pokiaľ ide o autorské práva, ako už ústavný súd judikoval, zákon č. 185/2015 Z. z. Autorský zákon v znení neskorších predpisov (ďalej aj „autorský zákon" alebo „AutZ") priznáva autorom rôzne vylúčené práva k určitým spôsobom použitia ich diel tretími osobami na vopred stanovený čas. Keďže autor takto získava možnosť zakázať šíriť svoje dielo inými, na jemu zverené práva je nutné nahliadať ako na spôsob obmedzenia všeobecnej slobody prejavu (II. ÚS 647/2014, ods. 30, *Funke Medien*, C-469/17, body 73 a 74; *Spiegel Online*, C-516/17, body 57, 58, 81, 82; *Pelham*, C-476/17, bod 34; ESĽP: *Ashby Donald a ďalší v. Francúzsko*, 36769/08; *Neij a Sunde Kolmisoppi v. Švédsko*, 40397/12). V prvom rade právno-technické posúdenie podľa kritérií, ktoré uvádza čl. 35 GDPR, poskytuje len extrémne minimálny priestor na tvorivý vklad (pozri II. ÚS 647/2014, ods. 34, pozri SDEÚ, *Brompton Bicycle*, C-833/18, body 24 až 27). Je preto ťažko predstaviteľné, že autorskoprávna ochrana k určitým častiam dokumentu podľa čl. 35 GDPR vôbec existuje. Autorské právo nechráni všetko, čo napíše človek, hoci aj na základe erudovanosti a rokov poctivého štúdia. Chráni len výtvory, ktoré umožňujú tvorcovi preniesť do diela odtlačok svojej osobnosti (SDEÚ, *Painer*, C-145/10, ale aj II. ÚS 647/2014, bod 34 a III. ÚS 651/2016, bod 23 a nasl.). Takýto scenár je pri mechanickom právno-technickom posúdení vplyvu na ochranu osobných údajov prakticky nepredstaviteľný. Úsilie nemožno dať na úroveň autorskoprávnej tvorivosti.

101. Navyše, akékoľvek hypotetické autorské práva externých firiem, ktoré sa prácne podieľali na príprave dokumentu, nie sú dotknuté vzhliadnutím informácie. Autorský zákon fyzické vzhliadnutie informácie nepovažuje za právne relevantné použitie diela (pozri § 18, § 19 AutZ). Autorský zákon, ak sa vôbec aplikuje, prakticky môže obmedzovať vyhotovenie kópie alebo umiestnenie diela na internete. Fyzické vzhliadnutie je možné vždy. Napokon aj keby tento dokument (resp. jeho časť) bol z osobitne tvorivých dôvodov chránený (napr. je napísaný vo veršoch), autorský zákon vylučuje mnohé predmety zo svojej ochrany pre verejný záujem [napr. právny predpis a technickú normu ako úradné dielo, ale aj posudky znalcov podľa § 5 písm. b) a h) AutZ] alebo ich podrobuje osobitným obmedzeniam práve z dôvodu verejného záujmu vrátane ochrany slobodného prístupu k informáciám (II. ÚS 647/2014, bod 35). Autorským právom sa nikdy nechráni myšlienka, „spôsob, systém, metóda, koncept, princíp, objav alebo informácia, ktorá bola vyjadrená, opísaná, vysvetlená, znázornená alebo zahrnutá do diela" [§ 5 písm. a) AutZ], a preto aj vyhotovenie kópie autorského diela tretej osoby, hoci je autorskoprávne relevantným použitým diela, nemožno obmedziť len preto, lebo s ním držiteľ práv nesúhlasí. Práve na tieto účely autorský zákon vytvára tzv. zákonné licencie, ktoré majú umožniť vyhotovenie kópií na osobnú potrebu, účel výskumu, úradné účely, citáciu alebo informačné účely aj bez súhlasu autora (pozri napr. § 37, § 39, § 44, § 53 AutZ, pričom dielo poskytnuté orgánom verejnej moci na plnenie ich povinností je vždy zverejnené podľa § 6 AutZ). Autorské právo nestojí vzhliadnutiu alebo kopírovaniu dokumentu podľa čl. 35 GDPR v ceste. Je pritom nepodstatné, čo stanovuje zmluva medzi orgánom verejnej moci a dodávateľom posúdenia, pretože ide o kogentné zákonné ustanovenia, t. j. autorské právo nemožno zmluvne rozšíriť alebo výnimky chrániace slobodu prejavu vylúčiť.

102. Osobitnú situáciu bude predstavovať prípad, ak je dokument podľa čl. 35 vytvorený interne zamestnancami orgánu verejnej moci. Ak nejde o diela vylúčené z ochrany podľa § 5 písm. b) AutZ, vykonávateľom autorských práv bude zamestnávateľ, t. j. orgán verejnej moci (§ 90 AutZ). Ak by však orgán verejnej moci mohol sám sebe odmietnuť udeliť súhlas na použitie diela, napr. pre účely skopírovania dokumentu, išlo by zjavne o obchádzanie zákona a povýšenie drobného ekonomického záujmu štátu nad právo na prístup k informáciám na účely jeho kontroly. Keďže odovzdanie hoci aj kópie dokumentov neznamená možnosť ich bezbrehého použitia zo strany žiadateľa, obmedzovanie prístupu k informáciám, ak je vykonávateľom autorských práv orgán verejnej moci, by bolo zjavne neproporcionálne.

103. Pokiaľ ide o obchodné tajomstvo, z jeho zákonnej definície rovnako vyplýva, že obsah posúdenia toho, či orgán verejnej moci spĺňa zákonné požiadavky ochrany svojich občanov, nemôže predstavovať obchodné tajomstvo. Je pochopiteľné, že externé firmy si chránia svoje know-how, za to však nemožno vydávať štruktúru, koncept a kroky posúdenia ochrany osobných údajov podľa čl. 35 GDPR. Obchodné tajomstvo nemôže chrániť bežnú aplikáciu právneho predpisu. Skutočnosti obchodnej povahy sú skôr „informácie o zákazníkoch a dodávateľoch, obchodných plánoch a výskume a stratégiách týkajúcich sa trhu“ [odôvodnenie č. 2 smernice č. 2016/943 z 8. júna 2016 o ochrane nesprístupneného know-how a obchodných informácií (obchodného tajomstva)], nie štruktúra alebo spôsob aplikovania ustanovení právneho predpisu, ktoré sú aj tak bežne prístupné osobám v kruhoch, ktoré sa dotknutým druhom informácií zaoberajú [čl. 2 ods. 1 písm. a) smernice č. 2016/943]. Aj keby dokument vytvorený na účely posúdenia toho, ako orgán verejnej moci chráni osobné údaje, mal obsahovať v nejakej časti takéto informácie, ochrana nie je absolútna. Aj bez súhlasu držiteľa práv totiž možno obchodné tajomstvo sprístupniť na účely ochrany slobody prejavu vrátane prístupu k informáciám, odhalenia pochybenia či protiprávneho konania alebo na účely ochrany oprávneného záujmu, ktorým je aj uplatnenie práv dotknutej osoby (pozri čl. 5 smernice č. 2016/943 a jeho transpozíciu v § 51 ods. 6 až 8 Obchodného zákonníka). Z toho vyplýva, že obchodné tajomstvo nemôže byť dôvodom na odmietnutie celého dokumentu podľa čl. 35 GDPR, keďže z povahy veci nejde o obchodné tajomstvo a tam, kde je aj obsiahnuté v časti dokumentu, je jeho sprístupnenie často ospravedlnené priamo zákonom aj bez súhlasu jeho držiteľa (pozri aj analogicky II. ÚS 647/2014, body 31 až 40). Napokon ostatné práva duševného vlastníctva, ako napríklad ochrana patentov alebo databáz, neprichádzajú z povahy dokumentu podľa čl. 35 GDPR do úvahy.

104. Z už uvedeného vyplýva, že čl. 35 GDPR spolu so zákonom o slobode informácií vytvárajú dostatočné podmienky kvalitného dohľadu nad použitím údajov v rámci finančnej správy.

105. Finančná správa sa však na existenciu záruk zo všeobecnej úpravy na ochranu osobných údajov nemôže odvolať vo vzťahu k poskytovaniu údajov externým subjektom, a teda najmä štátnym orgánom. Ako už ústavný súd (PL. ÚS. 13/2020, PL ÚS 10/2014) judikoval, ak sú údaje, ktoré predstavujú závažný alebo obzvlášť závažný zásah do práv, odovzdávané mimo organizácie vykonávajúcej zber, je nevyhnutné, aby nad týmto prístupom existoval kvalitný nezávislý dohľad. Ten musí byť upravený v zákone, ktorý tento zásah predpisuje. Nestačí preto odkaz na všeobecnú úpravu ochrany osobných údajov a všeobecnú pôsobnosť úradu na ochranu osobných údajov. Takáto právna úprava dnes chýba. Aj preto nemožno na základe ústavnokonformného výkladu údaje zo systému e-kasa poskytnúť iným štátnym orgánom.

3.1.4. Zabezpečenie vysokej úrovne ochrany a bezpečnosti:

106. Zabezpečenie vysokej úrovne ochrany a bezpečnosti pomocou technologických a organizačných opatrení znamená, že čím sú údaje citlivejšie, tým je potrebnejšie trvať na kvalitnejších spôsoboch ochrany údajov proti zneužitiu (napr. formou asymetrického šifrovania, implementovaním certifikácie v oblasti bezpečnosti, obmedzením prístupu k údajom alebo vyškolením zodpovedných osôb). Tieto musia byť v prípade obzvlášť závažných zásahov upravené osobitne a zodpovedať najnovším vysokým štandardom používaným v odborných kruhoch (PL. ÚS 13/2020, bod 93). Na rozdiel od obzvlášť závažných zásahov do súkromia a osobných údajov, pri ktorých je nutné zabezpečiť „mimoriadne" vysokú úroveň ochrany (PL ÚS 13/2020, bod 93), v kontexte závažných zásahov postačí zabezpečenie vysokej úrovne ochrany a bezpečnosti.

107. V § 29 ods. 6 ZoFS existuje povinnosť finančnej správy „zabezpečiť ochranu informácií a osobných údajov pred ich neoprávneným zverejnením, poskytovaním alebo sprístupnením". Finančná správa uviedla jednu konkrétnejšiu normu interného charakteru, ktorá ma zabezpečovať ochranu osobných údajov zo systému e-kasa. Tá je však z júla 2018, t. j. pred zavedením e-kasy (zákon č. 368/2018 Z. z. bol platný k 20. decembru 2018 a účinný k 1. októbru 2019). Navyše, podľa vyjadrení *„neboli zo strany finančnej správy prijaté špeciálne opatrenia na ochranu osobných údajov"* týkajúce sa systému e-kasa.

108. Ústavný súd v tomto smere poukazuje na to, že na finančnú správu sa vzťahujú predpisy jednak v oblasti ochrany osobných údajov, ako aj v oblasti kybernetickej bezpečnosti. V oblasti ochrany osobných údajov musí finančná správa zhodnotiť riziká vyplývajúce zo spracúvania osobných údajov. Súčasťou týchto opatrení sú aj už spomínané opatrenia zabezpečiť bezpečnosť spracúvania svojich údajov podľa čl. 32 GDPR, notifikovať úrad na ochranu osobných údajov a dotknutú osobu v prípade incidentov podľa čl. 33 a 34 GDPR a vykonať posúdenie podľa čl. 35 GDPR. V oblasti kybernetickej bezpečnosti zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „ZoKB"), ako aj zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „ZoITVS") stanovujú finančnej správe ďalšie konkrétne povinnosti v oblasti bezpečnosti.

109. Systém e-kasa prevádzkovaný finančnou správou zjavne musí spadať pod pojem „základnej služby" podľa jednej alebo viacerých alternatív v rámci § 3 písm. k) ZoKB. Z čl. 3 smernice č. 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii, ktorých je ZoKB implementáciou, je zrejmé, že vyňatie z tohto režimu je možné len pri zabezpečení vyššej osobitnej ochrany, ktorej v tomto prípade niet. Vzhľadom na zákonnú povinnosť podľa § 17 ods. 1 ZoKB existuje povinnosť finančnej správy posúdiť a následne notifikovať Národný bezpečnostný úrad (ďalej len „NBÚ") o prekročení dopadových kritérií podľa § 18 ZoKB. Keďže e-kasa je plošný systém, na ktorý sú naviazané obchodné transakcie v celej krajine v reálnom čase, je pomerne ťažké si predstaviť záver, že tieto kritériá nie sú splnené. Akýkoľvek útok na e-kasu alebo únik dát z nej môžu mať nedozerné dôsledky pre dotknutých podnikateľov, ich podnikateľskú činnosť a obyvateľstvo. Ako dôsledok má finančná správa niekoľko zásadných bezpečnostných povinností vrátane povinnosti prijať bezpečnostné opatrenia v personálnej a technologickej oblasti, povinnosti detegovať, evidovať, oznamovať NBÚ a aktívne riešiť bezpečnostné incidenty (§ 19, § 20 ZoKB), ako aj povinnosti

podrobovať sa dohľadu NBÚ a nezávislým auditom (§ 28, § 29 ZoKB). Podobné povinnosti pritom prevádzkovateľovi e-kasy vyplývajú aj zo ZoITVS, pričom tie sa uplatnia, ak sú prísnejšie [§ 2 ods. 2 písm. e) ZoKB], ako napríklad § 23 ods. 3 ZoITVS pri notifikácii bezpečnostných incidentov.

110. NBÚ, ako aj iné štátne orgány v tomto smere disponujú aj širokou možnosťou vykonávať kontrolu na poli bezpečnosti. Podľa § 29 ods. 5 ZoKB môže NBÚ kedykoľvek vykonať audit kybernetickej bezpečnosti s cieľom potvrdiť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených týmto zákonom. Po vykonaní kontroly alebo ak audit ukáže nedostatky, môže NBÚ vydať rozhodnutie o uložení opatrení na nápravu a uložiť pokutu za priestupok alebo iný správny delikt [§ 5 ods. 1 písm. u), § 28, § 29 ods. 4 ZoKB].

111. Tieto povinnosti sú realizáciou ústavnej povinnosti štátu aktívne chrániť dôvernosť a integritu informačných systémov, ktoré obsahujú osobné údaje jednotlivca. Právo na ochranu dôvernosti a integrity informačných systémov predstavuje súčasť ochrany podľa čl. 19 ods. 3 a čl. 22 ústavy (podobne BVerfG, 1 BvR 370/07, 1 BvR 595/07, BVerfG 120). Zároveň sú tieto opatrenia predpokladom akceptovateľného závažného zásahu do práva na ochranu osobných údajov (SDEÚ, *Digital Rights Ireland*, C-293/12 and C-594/12, ods. 66 – 67). V kontexte prevádzkovania e-kasy je preto aj povinnosťou finančnej správy riadne uplatňovať na svoje fungovanie ustanovenia ZoKB.

112. Z právnej úpravy, ktorá reguluje finančnú správu, jej preto vyplývajú konkrétne a obšírne požiadavky na bezpečnosť. Tie možno považovať za dostatočné.

3.1.5. Časová podmienenosť zničenia a vyrozumenie dotknutých osôb:

113. Časová podmienenosť zničenia znamená, že ak pominuli dôvody na spracúvanie údajov, musia byť zneškodnené (vymazané). Táto podmienka je vyjadrením toho, že tak, ako sa subsidiarita vzťahuje na vyžiadanie údajov, uplatňuje sa aj na ich následné spracúvanie. Ak teda odpadne dôvod na ich spracúvanie v danej kvalite, štátna moc musí riziko zneužitia minimalizovať tým, že nepotrebné údaje čím skôr znehodnotí alebo úplne zničí (PL. ÚS 13/2020, bod 94). Zničenie údajov zo systému finančnej správy nie je súčasťou právnej úpravy a vyplýva podľa finančnej správy z legislatívy len nepriamo, a to z právnych predpisov o účtovníctve (§ 35 zákona o účtovníctve) v spojení s § 20 ZoFS.

114. Finančná správa konkrétne na otázku doby uchovávania odpovedala, že táto je *„plánovaná na obdobie 10 rokov“* pre potreby správcu dane, ale pre potreby finančnej správy budú *„zobrazované údaje do doby uplynutia práva vyrubiť daň – 5-7 rokov“*.

115. Z § 20 ods. 6 a 7 ZoFS subsidiárne vyplýva, že finančná správa musí bezodkladne zničiť údaje, ak budú irelevantné pre výkon jej povinností, pre ktoré sú údaje zbierané, čo musí aj periodicky kontrolovať. Ústavný súd konštatuje, že vzhľadom na účel § 8a ods. 1 ZoERP musí finančná správa podľa § 20 ods. 6 a 7 ZoFS údaje zo systému e-kasa odstrániť automaticky hneď, ako uplynie doba uchovávania nevyhnutná pre kontrolu ZoERP. Štátny orgán totiž dopredu vie, kedy uplynie táto doba, pretože jej ukončenie nezávisí od iných okolností ako plynutia času. Zákonodarca by mal takúto dobu vždy jasne upraviť, ale ak to nie je možné, ale doba aspoň jasne zo súvisiacich predpisov vyplýva, záruku zničenia dát možno považovať za splnenú.

116. Požiadavka vyrozumenia dotknutých osôb znamená, že pokiaľ je to možné, je nutné o rozsahu a spôsobe použitia údajov upovedomiť dotknutú osobu, a to hoci aj dodatočne. Je vyjadrením požiadavky na prístup k súdu a efektívnej súdnej ochrane (PL. ÚS 13/2020, bod 95). Keďže ústavný súd posudzuje v tomto kroku len údaje predajcov ako dotknutých osôb, je zrejmé, že k nim títo majú prístup. Podnikateľ má právo vidieť svoje údaje v klientskej zóne.

117. Údaje zbierané podľa § 8a ZoERP sú dnes predmetom dostatočných záruk, avšak len na ich používanie v kontexte tohto zákona. Zákon neustanovuje dostatočné záruky na to, aby tieto údaje boli poskytnuté mimo finančnej správy alebo používané na iné účely. Je na zákonodarcovi, či chce takýto prístup upraviť, avšak musí sa vysporiadať s potrebou už načrtnutých záruk. Musí tak urobiť explicitne, rešpektujúc riadnu legislatívnu techniku, ktorá umožňuje prieskum ústavným súdom.

3.1.6. Posudzovanie rizikovosti podnikateľov v rámci finančnej správy:

118. Z vyjadrení finančnej správy vyplýva, že údaje z e-kasy sú dnes využívané aj *„pre účel analytického vyhodnocovania... rizikovosti daňových subjektov z pohľadu evidencie tržieb“*. Údaje sú potom prepojené s ďalšími databázami. Údaje z e-kasy teda slúžia na hodnotenie podnikateľov podľa ich rizikovosti. Takáto analytická činnosť predstavuje tzv. profilovanie, ktoré sa v literatúre a podústavných normách chápe ako „akákoľvek forma automatizovaného spracúvania osobných údajov, ktoré pozostáva z použitia týchto osobných údajov na vyhodnotenie určitých osobných aspektov týkajúcich sa fyzickej osoby, predovšetkým analýzy alebo predvídania aspektov dotknutej fyzickej osoby súvisiacich s výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom“ [pozri čl. 4 ods. 4 GDPR (vlastné zvýraznenie) a širšie: HILDEBRANDT, M. (2008) Defining Profiling: A New Type of Knowledge? In: HILDEBRANDT, M., GUTWIRTH, S. (eds) *Profiling the European Citizen*. Springer, Dordrecht. Dostupné na: <https://doi.org/10.1007/978-1-4020-6914-7_2>].

119. Hodnotenia rizikovosti sú potom využívané v kontexte vykonávania kontrolnej činnosti štátnymi zamestnancami finančnej správy. Automatizované posudzovanie rizikovosti však nemá dostatočnú oporu v zákone. Je síce možné, že v konkrétnom prípade takáto operácia spadá pod konkrétny legitímny cieľ a účel zberu dát podľa ZoERP, no jej realizácia na podklade súčasného zákona, a to ani v rámci finančnej správy, nespĺňa požiadavky zákonnosti a existencie záruk týkajúcich sa kvality dohľadu.

120. Automatizované posudzovanie jednotlivca na základe plošného zberu dát predstavuje zásah do práva na informačné sebaurčenie bez ohľadu na to, či pre neho má určitý následok. Aj preto napríklad Spolkový ústavný súd Nemecka považoval automatizované posudzovanie evidenčných čísiel áut za zásah aj pri osobách, u ktorých kontrola neviedla k žiadnemu negatívnemu výsledku (BVerfG, sp. zn. 1 BvR 142/15, body 45 a 51). Rovnako SDEÚ vo svojom stanovisku č. 1/15 zastáva názor, že automatizované posudzovanie osôb v leteckej preprave prestavuje osobitný zásah do práva na ochranu súkromia a osobných údajov (stanovisko SDEÚ č. 1/15, ods. 168 a nasl.). Každé takéto posudzovanie štátom bez ohľadu na to, či spôsobuje nepríjemnosť alebo negatívny dôsledok u jednotlivca, totiž obmedzuje jeho slobodu. Štát ním uplatňuje svoju moc nad jednotlivcom tým, že ho sleduje, hodnotí alebo kontroluje. Tým sa u jednotlivca vytvára pocit sledovania zo strany štátu (BVerfG, sp. zn. 1 BvR 142/15, bod 98).

121. Ako aj sudcovia ESĽP Lemmens, Vehabovic a Bošnjak vo svojom nedávnom súhlasnom stanovisku k rozhodnutiu vo veci *Big Brother Watch a ďalší proti Spojenému kráľovstvu* zdôraznili, „[S]amotný pocit, že jednotlivec je konštantne sledovaný a posudzovaný inými, môže mať vážny dopad na jeho psychické a fyzické zdravie. Núti totiž jednotlivcov príliš internalizovať ich spoločenské správanie, čím sa cítia vinní alebo zahanbení za svoje pocity, myšlienky, túžby alebo konania, ktoré by nechceli vyjadriť verejne“ (pozri súhlasné stanovisko sudcu Lemmensa, Vehabovica a Bošnjaka v *Big Brother Watch a ďalší proti Spojenému kráľovstvu*, č. 58170/13, 62322/14, 24960/15, bod 4).

122. Každé automatizované posúdenie vyžaduje minimálne spojenie údajov s určitými kritériami, modelmi alebo inými databázami (napr. evidenčné číslo auta sa porovná s existujúcimi zoznamami alebo činnosť podnikateľa so zvyčajným správaním porovnateľného podnikateľa). Vo väčšine prípadov sa využíva algoritmus s cieľom, niečo z údajov odvodiť, navrhnúť určité usporiadanie alebo poskytnúť odporúčanie pre zamestnanca orgánu verejnej moci či dokonca predpripraviť mu rozhodnutie alebo jeho časť. Keďže automatizované posúdenie jednotlivca predstavuje zásah do jeho práva na informačné sebaurčenie, musí byť podľa čl. 13 ods. 2 ústavy stanovené zákonom. Základom tejto požiadavky je, aby adresáti právnych noriem vedeli posúdiť, ako sú obmedzené ich práva a aké to má pre nich následky (pozri *Leander proti Švédsku* [1987] č. 9248/81, bod 50; *Margareta and Roger Andersson proti Švédsku* [1992] č. 12963/87, bod 75). Zákon obmedzujúci základné práva musí byť dostatočne konkrétny, aby jeho aplikácia bola predvídateľná. Problematické obmedzenie práv sa nemôže skrývať pod lepšie znejúce alebo nič nehovoriace abstraktné znenie (PL. ÚS 13/2020, bod 84). Táto požiadavka sama osebe nevylučuje možnosť prijatia všeobecnej právnej úpravy v oblasti verejnej správy. Legislatíva však musí dostatočne jasne poskytovať občanovi náležitú indikáciu okolností a podmienok, za akých je verejná moc zmocnená na takéto zásahy do jeho práva. Pripustenie vysokej neurčitosti právnej normy by obmedzilo aj reálnu kontrolu súladu ustanovenia zákona s ústavou, a tým znemožnilo ústavnému súdu vykonávať svoju kontrolnú funkciu.

123. „Mlčiaci zákon“ nemôže slúžiť ako podklad pre automatizované posudzovanie jednotlivca, či už je jeho výsledkom rozhodnutie, alebo nečinnosť. Automatizované posudzovanie rizikovosti nemôže byť len dôsledkom manažérskeho rozhodnutia orgánu verejnej správy, ale má byť predmetom verejnej debaty premietnutej v legislatívnom procese. Nedostatok explicitného odobrenia zákonodarcom sa prejavuje aj nedostatkom úpravy infraštruktúry dohľadu nad takýmto posudzovaním. Už z kontextu mocenského vzťahu medzi štátom a jednotlivcom je zrejmé, že dopad automatizovaného posúdenia jednotlivca a jeho okolností je spravidla zásadný pre jeho adresáta. Často bude dôležitým vstupom pre následné správanie zamestnanca orgánu verejnej moci, ktorý výsledok tohto automatizovaného posúdenia nebude dostatočne kriticky alebo vôbec korigovať.

124. V preskúmavanej právnej úprave akákoľvek osobitná alebo všeobecná právna norma tohto typu chýba.

125. Po splnení zákonnosti (legality) takéhoto obmedzenia musí zákonodarca zabezpečiť aj legitimitu a proporcionalitu svojho riešenia. Ak je automatizované posudzovanie plošné, a teda nevzťahuje sa na obmedzený okruh „podozrivých“ osôb, je nutné osobitne zvážiť, či záujmy chránené takýmto posudzovaním dostatočne prevážia nad všeobecným pocitom sledovania, ktorý sa tak umocňuje. Nemožno uplatniť automatizáciu všade, kde je technicky možná a užitočná, len

preto, lebo verejnej moci, a teda aj daňovým poplatníkom šetrí prostriedky. Spolkový ústavný súd Nemecka dospel napríklad k záveru, že neobmedzené automatizované kontrolovanie evidenčných čísiel áut na cestách na účely ochrany pred akýmkoľvek nebezpečím by bolo neproporcionálne (BVerfG, sp. zn. 1 BvR 142/15, bod 104). Aj v slovenskom kontexte preto nasadenie automatizovaného posudzovania na základe osobných údajov bude nutné skúmať *ad hoc* pre konkrétne použitie. Samotný fakt, že existuje dostatočný verejný záujem na zbere určitých údajov, totiž ešte neznamená, že rovnaký záujem existuje aj na ich ďalšom použití (analogicky *Satakunnan Markkinapörssi Oy and Satamedia Oy proti Fínsku*, č. 931/13, body 172 – 178 a 198).

126. Ako ESĽP pripomína, každý štát, ktorý na seba prevezme rolu vývoja a použitia nových technológií, nesie osobitnú zodpovednosť, aby zabezpečil správny balans so základnými právami (*S. a Marper proti Spojenému Kráľovstvu*, č. 30562/04, 30566/04, bod 112). Predovšetkým nemožno podceniť fakt, že vývoj technológií zákonite povedie k novým nepredvídateľným spôsobom, ako zbierané informácie a ich použitie môžu dopadnúť na jednotlivca (*S. a Marper proti Spojenému Kráľovstvu*, č. 30562/04, 30566/04, bod 71). Nasadenie technológií si preto vyžaduje komplexné posúdenie vo svetle stále nových možností ich použitia (napr. *Gaurghran proti Spojenému Kráľovstvu*, č. 45245/15, body 67 až 70 vo vzťahu k používaniu rozpoznávania tváre na staršie data-sety).

127. Dôsledkom uplatnenia technologického pokroku vo verejnej správe nemôže byť neosobný štát, ktorého rozhodnutia sú nevysvetliteľné, nepreskúmateľné a zároveň za nich nie je nik zodpovedný.

128. Osobitosť automatizovaného posudzovania spočíva v tom, že sa často týka veľkej skupiny osôb a používané kritéria, vzory alebo prepojené databázy nie sú ľahko pochopiteľné pre adresáta, hoci môžu obsahovať chyby alebo viesť k chybným záverom o jednotlivcovi. Takéto nedostatky systému preto vytvárajú systémové riziko pre spoločnosť a jednotlivca (prof. Pasquale v tomto smere hovorí o riziku tzv. čiernych skriniek v spoločnosti, pozri PASQUALE, F. *The Black Box Society: The Secret Algorithms that Control Money and Information.* Harvard University Press, 2015.). V zahraničí už dnes možno badať prípady, keď sa jasne prejavujú takéto zásadné riziká používania automatizovaného posudzovania bez dostatočného dohľadu, na čo nedávno reagovala aj Rada Európy [pozri odporúčanie CM/Rec(2020)1 Rady ministrov členským štátom týkajúce sa ľudskoprávnych aspektov algoritmických systémov z 8. apríla 2020, ako aj deklaráciu Decl(17/03/2021)2 Rady ministrov týkajúcu sa rizík rozhodnutí v oblasti sociálneho zabezpečenia, ktoré sú asistované výpočtovou technikou alebo umelou inteligenciou, zo 17. marca 2021; pre konkrétne kauzy pozri algoritmické upravovanie maturitných známok vo Veľkej Británii z roku 2020 – HUSOVEC, M., MESARČÍK, M. a ANDRAŠKO, J. *Právo informačných a komunikačných technológií 1* (TINCT 2020). s. 108, a kauzu odhaľovania zneužívania sociálneho systému v Holandsku známu ako tzv. Systeem Risico Indicatie (SyRI) – dostupné na: <https://www.hrw.org/news/2019/11/08/welfare-surveillance-trial-netherlands>].

129. Aj po zvolení proporcionálneho uplatnenia technológie je preto nutné zabezpečiť existenciu záruk dohľadu ich ďalšieho používania. SDEÚ v kontexte automatizovaného posudzovania leteckých cestujúcich zdôraznil, že „vopred stanovené vzory a kritériá mali byť na jednej strane konkrétne a spoľahlivé“ a „na druhej strane nediskriminačné“, pričom databázy, s ktorými sa údaje porovnávajú, musia byť „spoľahlivé a aktuálne“ (stanovisko SDEÚ č. 1/15, ods. 172), a preto aj „každý pozitívny výsledok získaný v nadväznosti na automatizované spracovanie uvedených

údajov“ má byť „podrobený individuálnemu preskúmaniu prostredníctvom neautomatizovaných prostriedkov pred prijatím individuálneho opatrenia“, ktoré by malo na osoby „negatívny dopad“ (stanovisko SDEÚ č. 1/15, ods. 173). Ako dôsledok sa výsledok automatizovaného posúdenia „nemôže rozhodujúcim spôsobom zakladať iba na výsledku automatizovaného spracúvania údajov“ (stanovisko SDEÚ č. 1/15, ods. 173).

130. Automatizované posúdenie založené na osobných údajoch v systéme e-kasa spolu s ďalšími kritériami, vzormi alebo databázami vedie k vyhodnoteniu určitých podnikateľov ako rizikovejších, a teda vhodných na podrobnejšiu kontrolu. Ústavný súd nedisponuje konkrétnosťami týkajúcimi sa fungovania tohto systému. Vzhľadom na nedostatok legality tohto systému však ani nie sú potrebné pre posúdenie veci. Z opisu finančnou správou je zrejmé, že minimálne v medzikroku používa analytický systém, ktorý automatizovane pripisuje konkrétnemu podnikateľovi určité riziko. To, že systém sám nerobí aj rozhodnutie o tom, či sa vykoná daňová alebo iná kontrola, nie je z pohľadu práva na informačné sebaurčenie podstatné. Z jeho pohľadu je podstatné, že sa automatizácia vzťahuje na hodnotenie osoby na základe jej osobných údajov.

131. Ak by osobné údaje netvorili podklad konania štátu, situácia by spadala mimo rozsahu čl. 19 ods. 3 a čl. 22 ods. 1 ústavy (podobne BVerfG, sp. zn. 1 BvR 142/15, bod 48), hoci stále bude spadať pod iné ustanovenia ústavy. Relevantné v tomto ohľade sú najmä právo na spravodlivý proces, zákaz nerovného zaobchádzania, ako aj sloboda prejavu či sloboda zhromažďovania. Je totiž zrejmé, že najmä algoritmické posudzovanie môže mať dopad na jednotlivca a jeho základné práva aj vtedy, ak jeho podkladom nie je osobný údaj [pozri odporúčanie CM/Rec(2020)1, časť A, bod 4]. Zároveň treba pripomenúť, ako bolo obšírne v bodoch odsekov 38 až 46 tohto nálezu vysvetlené, že ústavnoprávna ochrana práva podľa čl. 19 ods. 3 a čl. 22 ods. 1 ústavy nie je vždy obmedzená na osobné údaje fyzických osôb, ako to je bežné v podústavnom práve.

132. Zákonodarca má ako jediný možnosť prostredníctvom konkrétnych zákonných ustanovení vo všeobecnom alebo v osobitnom predpise zabezpečiť, aby používané kritéria, modely alebo prepojené databázy v kontexte automatizovaného posudzovania boli aktuálne, spoľahlivé a nediskriminačné. Nad rozsah všeobecných záruk, ktoré sú nevyhnutné pri spracovaní osobných údajov, tak robí prostredníctvom osobitných záruk: (i) transparentnosti, (ii) individuálnej ochrany a (iii) kolektívneho dozoru [podobne BVerfG, sp. zn. 1 BvR 142/15, bod 101, stanovisko SDEÚ č. 1/15, ods. 168 a nasl., ako aj odporúčanie CM/Rec(2020)1, časť B, body 4 a 5]. Tieto záruky musia zohľadňovať osobitnosť obstarávania a nasadzovania automatizovaných systémov, ktorých činnosť bude mať dopad na jednotlivca a jeho základné práva a slobody.

133. V prvom rade dotknutý jednotlivec preto musí mať informácie o tom, že správanie orgánu verejnej moci, napríklad jeho rozhodnutie, je ovplyvnené použitím takéhoto automatizovaného systému [odporúčanie CM/Rec(2020)1, časť B, bod 4]. Jednotlivec musí mať možnosť vedieť o existencii, rozsahu a dopadoch posúdenia jeho osoby automatizovanými prostriedkami, či už prostredníctvom verejných registrov, špecifických poučení, alebo inak. Len ak je adresátovi zrejmé, že je predmetom automatizovaného posúdenia v určitom rozsahu, dokáže sa efektívne brániť proti prípadným chybám. Je na zákonodarcovi, ako zhmotní túto požiadavku.

134. Povinnosť transparentnosti môže vyplývať orgánu verejnej moci čiastočne aj zo všeobecnej podústavnej úpravy práva na ochranu osobných údajov (čl. 12 až 15 GDPR). V kontexte automatizovaného posúdenia bude spravidla vznikať orgánu verejnej moci povinnosť vykonať

posúdenie vplyvu ochrany údajov podľa čl. 35 GDPR. Na rozdiel od iných spracovateľských operácií sa však posúdenie vplyvu musí sústrediť na celkový ľudskoprávny dopad automatizovaných systémov na jednotlivca [odporúčanie CM/Rec(2020)1, časť B, bod 5.2]. V rámci neho je potom nutné aj identifikovať konkrétne riziká, ako aj dokumentovať rozsah ľudského a automatizovaného posúdenia v jednotlivých krokoch procesu spracúvania údajov, spôsob testovania „data-set" a použitých modelov, ako aj alternatívne šetrnejšie riešenia [pozri Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (2018), s. 29 a odporúčanie CM/Rec(2020)1, časť B, body 3 a 5]. Dostatočnosť tejto všeobecnej úpravy bude závisieť od okolností a závažnosti zásahu do práva na informačné sebaurčenie.

135. V prípade, ak je technické riešenie poskytované štátu treťou stranou, štát musí splniť rovnaké podmienky transparentnosti. Práva duševného vlastníctva, obchodné tajomstvo alebo bezpečnosť systému nemôžu byť dôvodom na odopretie efektívneho prístupu k potrebným informáciám [rovnako odporúčanie CM/Rec(2020)1, časť B, bod 5.2]. V opačnom prípade by jednoduché rozhodnutie o zapojení externých dodávateľov ukrátilo práva jednotlivca, a preto ak štátny orgán používa riešenia od externých dodávateľov, musí zabezpečiť efektívny prístup k potrebným informáciám. Ako už bolo v odsekoch 97 až 104 tohto nálezu uvedené, podzákonná úprava týchto práv poskytuje široký priestor na realizáciu práva na prístup k informáciám. To však neznižuje povinnosť orgánov verejnej moci konať zodpovedne už v štádiu verejného obstarávania týchto systémov [rovnako odporúčanie CM/Rec(2020)1, časť A, bod 12].

136. V druhom rade nad používaním takéhoto systému musí existovať nezávislá kolektívna kontrola, ktorá funguje ako *ex-ante* (pre zavedením), tak aj *ex-post* (po zavedení). V tomto smere sa nemožno spoliehať len na infraštruktúru z oblasti práva na ochranu osobných údajov, keďže tá funguje na princípe ochrany práv jednotlivca. Jednotlivcovi však nemožno klásť za úlohu, aby prostredníctvom svojej situácie pravidelne korigoval systematické problémy verejnej správy. Kolektívna kontrola, či už prostredníctvom nezávislých štátnych inštitúcií, certifikácie, zapojenia občianskej spoločnosti, alebo akadémie, preto dopĺňa individuálnu ochranu pred ujmami kolektívneho charakteru (pozri EDWARDS, L., VEALE, M. Slave to the Algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for (2017). In: *Duke Law & Technology Review* 18, s. 22.).

137. To znamená, že kontrola musí umožňovať posúdenie kvality systému, jeho komponentov, chybovosti a nedokonalostí pred tým, ako je uvedený do prevádzky, ako aj po tom, keď sa začne používať (napríklad prostredníctvom auditov, skúmaním kvality vzorky rozhodnutí, podávaním správ a štatistík a pod.). Čím komplexnejší systém, tým hlbšia musí byť jeho kolektívna kontrola. Ak má systém slabé alebo slepé miesta, musia štátni zamestnanci, ktorí s ním budú pracovať, tieto miesta preukázateľne poznať, keďže ich neznalosť môže byť práve zdrojom chýb. Používanie systému musí byť predmetom dokumentácie a protokolovania, aby sa jednak umožnil kolektívny dozor, ale aj zjednodušilo vymáhanie práv jednotlivca [BVerfG, sp. zn. 1 BvR 142/15, body 156 a 157, rovnako aj odporúčanie CM/Rec(2020)1, časť A, body 3 a 4].

138. Napokon dohľad nad automatizovaným posúdením musí umožňovať jednotlivcovi efektívne sa brániť proti nedokonalostiam a chybám systému. Je na zákonodarcovi, aké presne prostriedky zvolí. Musia byť však efektívne a dostupné a zároveň zverené nezávislým orgánom dohľadu

[rovnako aj odporúčanie CM/Rec(2020)1, časť A, body 4.5]. Vzhľadom na rôzne spôsoby posudzovania neexistuje jeden spôsob, ako ochrániť jednotlivca pred chybami systému. Efektívnosť prostriedkov, či už vo forme práva odvolať sa, korigovať vstupy alebo kritéria posúdenia, alebo dostať prístup k logike dotknutého rozhodnutia alebo individuálneho posúdenia človekom, bude závisieť od toho, či automatizované posúdenie používa vzory, modely alebo ďalšie databázy a či vedie k rozhodnutiu alebo nečinnosti orgánu verejnej moci. Taktiež bude závisieť od rizikovosti daného systému.

139. Použitie týchto už uvedených záruk dohľadu musí byť však schopné dosiahnuť zmenu správania orgánu verejnej moci. Ako ústavný súd už v minulosti zdôraznil, kvalitný nezávislý dohľad nemožno vykonávať bez dostatočného udelenia oprávnení, finančných zdrojov a nástrojov kontroly. Ak preto orgán verejnej moci nedokáže rýchlo korigovať chyby alebo vysvetliť diskriminačné účinky posudzovania, musí existovať možnosť štátneho orgánu alebo súdu prikázať verejnému orgánu tieto chyby alebo nedokonalosti napraviť. V krajnom prípade musí existovať aj možnosť systém v jeho problematickej podobe prikázať prestať používať.

140. Vo všeobecnej rovine právo EÚ už dnes v čl. 22 a iných ustanoveniach GDPR čiastočne poskytuje určité záruky proti automatizovanému posudzovaniu vo forme profilovania alebo automatizovaného rozhodovania [pozri podrobnejšie Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (2018)]. Článok 22 GDPR vyžaduje explicitnú autorizáciu výlučne automatizovaných rozhodnutí právom členského štátu, resp. právom EÚ [pozri čl. 22 ods. 2 písm. b) GDPR]. V takýchto situáciách, a to vrátane kontextu „monitorovania podvodov a daňových únikov a ich predchádzania“, núti aj sekundárne právo EÚ slovenského zákonodarcu, aby vytvoril osobitný právny základ, ktorý bude garantovať právo na ľudský zásah zo strany orgánu verejnej moci, právo jednotlivca vyjadriť svoje stanovisko a právo napadnúť rozhodnutie (pozri čl. 22 ods. 3 a odôvodnenie č. 71 GDPR). To isté platí aj v kontexte odhaľovania trestnej činnosti podľa čl. 11 smernice č. 2016/680 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov. Toto ustanovenie taktiež vyžaduje osobitný právny základ a existenciu osobitných záruk v špecializovaných vertikálnych vzťahoch.

141. Priestor pre slovenského zákonodarcu sa nevyčerpáva týmito dvomi uvedenými ustanoveniami. Napriek tomu, že pre mnoho otázok predstavuje GDPR plnú harmonizáciu (pozri bod 30 tohto nálezu), nie je to tak v tejto právnej otázke. GDPR predstavuje len neúplnú harmonizáciu v otázke spracúvania osobných údajov orgánmi verejnej moci na účely výkonu verejnej moci. To vyplýva z čl. 6 ods. 2 v spojení s čl. 6 ods. 1 písm. e) GDPR, ktorý výslovne predpokladá, že členské štáty môžu zachovať alebo zaviesť špecifickejšie ustanovenia s cieľom prispôsobiť uplatňovanie pravidiel tohto nariadenia v kontexte, ak spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi. Slovenský zákonodarca je preto oprávnený presnejšie stanoviť osobitné požiadavky na spracúvanie, ako aj prijať ďalšie opatrenia, ktorými sa „zaistí zákonné a spravodlivé spracúvanie“, a to prípadne aj prevzatím častí nariadenia do slovenskej legislatívy (čl. 6 ods. 2 a odôvodnenie č. 8 GDPR). Už uvedené ústavné požiadavky sú preto úplne kompatibilné s implementačným priestorom slovenského zákonodarcu a riadne zohľadňujú jeho mantinely stanovené čl. 6 ods. 2, pričom rozvíjajú aj požiadavky čl. 6 ods. 3 GDPR. Na rozdiel od prípadu

vedeného pred SDEÚ a týkajúceho sa automatizovaného posudzovania bonity jednotlivca neštátnymi aktérmi v kontexte ich podnikateľskej činnosti je preto otázka implementačného priestoru slovenského zákonodarcu pomerne jasná (pozri SCHUFA Holding, C-634/21, prejudiciálna otázka Správneho súdu Wiesbaden z 1. októbra 2021, sp. zn. 6 K 788/20.WI dostupná na: <https://www.jurpc.de/jurpc/show?id=20210144>).

IV.
Závery ústavného súdu

142. Ústavný súd konštatuje, že zákonodarca musí posúdiť, ako čo najlepšie zužitkovať benefity automatizácie bez toho, aby tým zároveň ohrozil základné hodnoty právneho štátu a miesto jednotlivca v ňom. Aktuálne neexistuje zákon, ktorý by umožňoval finančnej správe osobné údaje zo systému e-kasa používať na automatizované posudzovanie jednotlivcov. Ak chce zákonodarca umožniť takéto automatizované posudzovanie na základe osobných údajov, musí zabezpečiť splnenie ústavnoprávnych záruk, ktoré už ústavný súd podrobne uviedol.

143. Ústavný súd považuje lokálny zber daňového identifikačného čísla a zoznamu tovarov a služieb na pokladničných blokoch [§ 8 ods. 1 písm. b) a g) ZoERP] za súladné s ústavnou ochranou súkromia a osobných údajov. Zbieranie a odosielanie pokladničných blokov predajcov spolu s ich DIČ v rámci systému e-kasa vytvára permanetné systematické monitorovanie podnikateľov týkajúce sa toho, čo a za koľko, kedy a kde predávajú. Sleduje však legitímny cieľ boja proti daňovým únikom. Zber samotného DIČ nie je neproporcionálny vzhľadom na tento účel. Proporcionalita zberu iných údajov nebola navrhovateľmi zahrnutá do prieskumu. Z uvedených dôvodov ústavný súd v tejto časti návrhu navrhovateľov nevyhovel (bod 2 výroku)

144. Zbieranie a odosielanie unikátneho identifikátora kupujúceho do centrálnej databázy finančnej správy podľa § 8a ods. 1 ZoERP považuje ústavný súd za protiústavné z dôvodu absencie legitímnosti zásahu. Ústavný súd pritom upozorňuje, že prípadné rozšírenie na tieto údaje by znamenalo zásadné zintenzívnenie zásahu do práva na ochranu súkromia a osobných údajov, pokiaľ by nebolo realizované na základe preukázateľnej dobrovoľnosti, a preto ústavný súd rozhodol, že uvedené ustanovenie § 8a ods. 1 ZoERP v časti „unikátny identifikátor kupujúceho, ak je predložený kupujúcim pred zaevidovaním prijatej tržby“ nie je v súlade s čl. 16 ods. 1, čl. 19 ods. 2 a 3 ústavy (bod 1 výroku)

145. Na základe vykonania detailného ústavnokonformného výkladu ústavným súdom je súčasné legislatívne nastavenie spracúvania a prístupu k údajom v systéme e-kasa možné považovať za súladné s ústavou. Podľa tohto výkladu však údaje zo systému e-kasa možno používať len zo strany finančnej správy a len na účely kontroly povinností vyplývajúcich zo ZoERP. Rozšírenie okruhu štátnych orgánov si vyžaduje explicitnú právnu úpravu a jej osobitné posúdenie, čo sa týka proporcionality.

146. Ústavný súd zároveň identifikoval niekoľko existujúcich zákonných povinností, ktoré zatiaľ neboli dostatočne štátnym orgánom implementované.

147. Napokon ústavný súd ozrejmil, prečo ústavnokonformný výklad súčasnej právnej úpravy neumožňuje finančnej správe používať údaje zo systému e-kasa na automatizované analytické

posudzovanie rizikovosti podnikateľov. Aby to bolo možné, je nevyhnutná zmena zákona, ktorá zabezpečí takéto posudzovanie pred chybami.

148. Znenie charty a dohovoru, ktorých ustanovenia a súvisiaca judikatúra už boli obsiahlo a konkrétne ústavným súdom zohľadnené, podporujú tu vyslovené závery ústavného súdu.
S poukazom na závery uvedené v čl. III.2 tohto odôvodnenia ústavný súd návrhu navrhovateľov na vyslovenie nesúladu dotknutých ustanovení s čl. 8 dohovoru a čl. 7, čl. 8 a čl. 52 ods. 1 charty nevyhovel (bod 2 výroku).

V.
Účinky nálezu

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

150. Podľa čl. 125 ods. 6 ústavy rozhodnutie ústavného súdu vydané podľa odsekov 1, 2 a 5 sa vyhlasuje spôsobom ustanoveným na vyhlasovanie zákonov. Právoplatné rozhodnutie ústavného súdu je všeobecne záväzné.

151. Podľa § 68 ods. 2 zákona o ústavnom súde rozhodnutia ústavného súdu v konaní o súlade právnych predpisov, v konaní o súlade medzinárodných zmlúv, v konaní o súlade predmetu referenda, v konaní o výklade ústavy a ústavných zákonov, v konaní o sťažnosti proti výsledku referenda, v konaní o sťažnosti proti výsledku ľudového hlasovania, v konaní o uvoľnení funkcie prezidenta a v konaní o neplatnosti právnych predpisov sa vyhlasujú v Zbierke zákonov Slovenskej republiky v rozsahu ustanovenom týmto zákonom.

152. Podľa § 91 ods. 1 zákona o ústavnom súde právny predpis, jeho časť alebo jeho ustanovenie, ktorých nesúlad s právnym predpisom vyššej právnej sily ústavný súd vyslovil, strácajú účinnosť dňom vyhlásenia nálezu ústavného súdu v Zbierke zákonov Slovenskej republiky a platnosť za podmienok ustanovených v § 91 ods. 2 zákona o ústavnom súde.

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

V Košiciach 10. novembra 2021

Ivan Fiačan
predseda Ústavného súdu
Slovenskej republiky