Univerzita Komenského v Bratislave
Právnická fakulta

Učebnica

Vybrané kapitoly práva informačných technológií I

Jozef Andraško
Matej Horvat
Matúš Mesarčík

VYBRANÉ KAPITOLY PRÁVA INFORMAČNÝCH TECHNOLÓGIÍ I
Učebnica

Vypracovali: JUDr. Jozef Andraško, PhD.
doc. JUDr. Matej Horvat, PhD.
JUDr. Matúš Mesarčík, LL.M

Recenzenti: Mgr. Martin Daňko, PhD.
Mgr. Rastislav Munk, PhD.

Vybrané kapitoly práva informačných technológií I. Jozef Andraško – Matej Horvat – Matúš Mesarčík. 1. vyd. – Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2019, 142 strán.

ISBN: 978-80-7160-523-2
EAN: 9788071065232
- Právo informačných a komunikačných technológií
- Správne právo

ISBN: 978-80-7160-523-2

Táto učebnica bola vydaná v rámci riešenia rozvojového projektu MŠVVaŠ SR č. 002UK-2-1/2018 - Vzdelávanie pre informačnú spoločnosť.

JEDNOTLIVÉ ČASTI SPRACOVALI

JUDr. Jozef Andraško, PhD.	Kapitola 3
doc. JUDr. Matej Horvat, PhD.	Kapitola 1
JUDr. Matúš Mesarčík, LL.M	Kapitola 2

OBSAH

O AUTOROCH

JUDr. Jozef Andraško, PhD., je absolventom Právnickej fakulty Univerzity Komenského v Bratislave. Témou jeho dizertačnej práce bolo Poskytovanie a využívanie elektronických služieb verejnej správy prostredníctvom informačných a komunikačných technológií. Od roku 2017 pôsobí ako odborný asistent na Ústave práva informačných technológií a práva duševného vlastníctva Právnickej fakulty Univerzity Komenského v Bratislave, kde vedie predmety ako Úvod do štúdia práva a právna informatika, Počítačové právo a IT Law. Absolvoval študijné pobyty na University of Iceland so zameraním na medzinárodné právo a na Tilburg University so zameraním na právo informačných a komunikačných technológií a právo duševného vlastníctva. V rámci výskumnej práce a publikačnej činnosti sa venuje najmä otázkam eGovernmentu, elektronickej identity, otvorených údajov, informačnej a kybernetickej bezpečnosti a umelej inteligencie. Kontakt: jozef.andrasko@flaw.uniba.sk

doc. JUDr. Matej Horvat, PhD., je absolventom Právnickej fakulty Univerzity Komenského v Bratislave, kde na Katedre správneho a environmentálneho práva obhájil dizertačnú prácu a v roku 2019 sa habilitoval na docenta v odbore 3.4.4 správne právo. V súčasnosti na tejto katedre pôsobí aj ako zástupca vedúceho katedry. Je aktívnym riešiteľom viacerých domácich aj zahraničných grantov (Vyšehradský grant, APVV, VEGA). Je autorom vedeckej monografie Administratívnoprávna zodpovednosť právnických osôb, komentára k zákonu o sťažnostiach a hlavným autorom komentára k Živnostenskému zákonu a navigátora Správny súdny poriadok v Automatizovanom systéme právnych informácií (ASPI). Spolupodieľal na tvorbe viacerých učebných textov. Vo svojej vedeckej práci sa venuje najmä správnemu trestaniu, všeobecnému správnemu konaniu a právu na prístup k informáciám. Výsledky jeho vedeckej práce boli prezentované na mnohých medzinárodných aj domácich vedeckých konferenciách. Kontakt: matej.horvat@flaw.uniba.sk

JUDr. Matúš Mesarčík, LL.M je absolventom Právnickej fakulty Univerzity Komenského v Bratislave v odbore právo (2016). V roku 2017 ukončil postgraduálne vzdelanie v odbore Právo a technológie na Tilburg University v Holandskom kráľovstve a získal titul LL.M. Je držiteľom Diplomu z anglického práva a práva Európskej únie (British Law Centre Diploma), ktorý udeľuje British Law Centre v spolupráci s University of Cambridge (Veľká Británia). V súčasnosti pôsobí ako interný doktorand v odbore správne právo na Katedre správneho a environmentálneho práva Právnickej fakulty, Univerzity Komenského v Bratislave s témou dizertačnej práce Dynamika pojmu osobný údaj vo svetle nových technológií. Takisto pôsobí v rámci Ústavu práva informačných technológií a práva duševného vlastníctva Právnickej fakulty Univerzity Komenského v Bratislave, kde okrem iných vedie semináre z predmetov Ochrana osobných údajov a Právo informačných technológií. Pravidelne publikuje v domácich a zahraničných vedeckých periodikách a zúčastňuje sa domácich a zahraničných konferencií. Poskytuje ad hoc konzultačné služby v oblasti ochrany osobných údajov. Kontakt: matus.mesarcik@flaw.uniba.sk.

ÚVOD

Milí čitatelia,

do rúk sa Vám dostáva učebnica s názvom Vybrané kapitoly práva informačných technológií, pričom ide o jej prvú časť. Právo informačných technológií je pomerne široká a dynamicky sa rozvíjajúca súčasť právnej úpravy. Vzhľadom na jej rozmanitosť a rozsah sme sa rozhodli túto učebnicu koncipovať ako „vybrané kapitoly," to znamená poskytnúť čitateľovi iba prehľad niektorých otázok vzhľadom na profiláciu jednotlivých autorov. Každý z nás má však osobitný štýl písania a techniku citovania. Z tohto dôvodu je možné nazerať na každú kapitolu ako samostatné dielo.

Voľba prirodzene padla na oblasti elektronického výkonu verejnej moci, ochrany osobných údajov či základov elektronickej identity, identifikácie a autentifikácie. Ambíciou autorov nebolo komplexne analyzovať danú oblasť. Cieľom je poskytnúť študentom a laickej verejnosti základný prehľad a úvod do danej problematiky. Na túto prvú časť učebnice nadviažeme druhým dielom, ktorý sa bude venovať otázkam zodpovednosti a bezpečnosti naprieč právnymi odvetviami.

Dúfame, že predkladaná učebnica pomôže študentom, ale aj laickej verejnosti zorientovať sa vo vybraných témach týkajúcich sa práva informačných technológií, ktoré sa stáva alfou a omegou právnej regulácie s nástupom nových technológií.

Bratislava, 15.12.2019 *Autori*

KAPITOLA 1 ELEKTRONICKÁ PODOBA VÝKONU VEREJNEJ MOCI

1.1 Úvodné poznámky

Už od prvopočiatkov svojej existencie si ľudstvo vytvára mechanizmy, ktoré mu napomáhajú v ďalšom vývoji. Tieto mechanizmy mali za úlohu zjednodušiť život ľudí, ako aj životu dať určité pravidlá. Cieľom bolo zabrániť chaosu v spoločenských vzťahoch prostredníctvom normovania správania. V prvopočiatkoch ľudského vývoja bolo zrejmé, že ľudia si vystačia so správou, ktorú si vykonávali sami, avšak s neskorším následným zaľudňovaním sa vysporiadali tak, že sa postupne vzdávali samosprávnych aktivít v prospech iných. V prvom rade to bol vládca (panovník), ktorý vytváral na správu svojej ríše rozličné úrady, do ktorých delegoval sebe verné osoby. Neskôr, v súvislosti s prechodom k republikánskym zriadeniam, sa tento proces postupne demokratizoval a dochádzalo k vytváraniu moderného (modernejšieho) poňatia spravovania štátu.

Správa vecí verejných na našom území doznala od roku 1989 mnohých zmien, od základnej transformácie systémových zmien vynútených novým spoločenským zriadením a novou ústavnoprávnou úpravou, cez viaceré reformy až po niekoľko modernizácií.[1]

Za najväčšiu výzvu súčasného výkonu verejnej moci na Slovensku možno považovať jej modernizáciu, pričom príkladom jej modernizácie je aj jej elektronizácia. Slovenský zákonodarca pretavil myšlienky elektronizácie verejnej moci do podoby zákona o e-governmente, t. j. zákona č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov (ďalej len „E-govZ“).

Vecná pôsobnosť tohto zákona je veľmi široká; vzťahuje sa na výkon verejnej moci ako takej. Podľa tohto zákona je elektronickým výkonom verejnej moci konanie orgánu verejnej moci v rozsahu podľa osobitných predpisov, vo veciach práv, právom chránených záujmov a povinností fyzických osôb alebo právnických osôb, pričom táto verejná moc sa vykonáva prostredníctvom elektronickej úradnej komunikácie.[2]

V nasledujúcich podkapitolách si postupne vysvetlíme pojmy, ktoré súvisia s elektronizáciou verejnej moci na Slovensku, pričom sa zameriame na pojem verejná moc a jej uplatňovanie (výkon) v elektronickej podobe. Z hľadiska elektronického výkonu verejnej

[1] Pozri viac KOŠIČIAROVÁ, S. *Správne právo hmotné. Všeobecná časť.* Plzeň : Aleš Čeněk, 2015, s. 93.

moci sa budeme venovať dvom veľkým tematikám, a to elektronickej schránke (jej zriadeniu, aktivácii, prístupu, deaktivácii a zrušeniu) a elektronickému doručovaniu.

1.2 Verejná moc

Verejná moc je veľmi významným pojmom v rámci teórie fungovania štátu. Bez toho, aby štát bol nositeľom verejnej moci, si nemožno predstaviť reálny výkon zabezpečenia potrieb obyvateľstva štátu. Verejnú moc majú preto nevyhnutne v rukách všetky zložky štátnej moci, či už sa venujeme moci zákonodarnej, súdnej alebo výkonnej. Platí samozrejme, že nie vždy zložky štátnej moci dosahujú svoje úlohy za využitia verejnomocenských prostriedkov.

Napríklad služby verejného záujmu sa nie vždy realizujú s využitím verejnomocenských oprávnení.[3] Asi ťažko si predstaviť verejnomocenské donucovanie obyvateľov obce, aby využívali služby obecnej knižnice, pripadne donucovanie využívania diaľnic. V našej učebnej pomôcke sa v ďalších riadkoch budeme preto budeme venovať len verejnomocenskému pôsobeniu zložiek štátnej moci, pretože len naň sa vzťahuje elektronický výkon verejnej moci.

Čo je to teda verejná moc? Pojem verejná moc je vymedzený v právnej úprave, ale aj v súdnej judikatúre. Právne predpisy pojem verejnej moci často využívajú, ale definujú ho len výnimočne. Tam, kde tieto definície nachádzame, tak sú tieto definície vymedzené len na účely toho-ktorého zákona. Inými slovami, nejde o všeobecné definície použiteľné na všetky prípady. Na druhej strane nám však ponúkajú základný pohľad na tento pojem a jeho základné charakteristické znaky.

Napríklad podľa zákona č. 514/2003 Z. z. o zodpovednosti za škodu spôsobenú pri výkone verejnej moci sa výkonom verejnej moci rozumie rozhodovanie a úradný postup orgánov verejnej moci o právach, právom chránených záujmoch a povinnostiach fyzických osôb alebo právnických osôb. Obdobne podľa už spomenutého E-govZ sa výkonom verejnej moci rozumie konanie orgánu verejnej moci v rozsahu podľa osobitných predpisov, vo veciach práv, právom chránených záujmov a povinností fyzických osôb alebo právnických osôb.

[3] ŠKROBÁK, J. Kategória verejnej moci a jej význam vo verejnej správe a vo vede správneho práva. *In Míľniky práva v stredoeurópskom priestore 2008. Bratislava* : VO PraF UK, 2008, s. 655.

V obidvoch prípadoch tieto zákony vychádzajú z toho, že verejná moc predstavuje rozhodovanie (konanie, postup) o právach (právom chránených záujmoch, povinnostiach) iných osôb. Inými slovami, ako znak verejnej moci vymedzujú oprávnenie určitého subjektu vystupovať v nadradenej pozícii k inému subjektu. Dôsledkom tejto nerovnosti je možnosť autoritatívne rozhodovať o zmene právnej situácie tohto druhého subjektu, t. j. o zmene v oblasti jeho práv, právom chránených záujmov alebo povinností.

Predmetné vymedzenie vychádza zo súdneho chápania pojmu verejná moc. Prvýkrát bolo vymedzené ešte Ústavným súdom Československej federatívnej republiky 9. júna 1992. Podľa uznesenia Ústavného súdu ČSFR je verejnou mocou taká moc, ktorá autoritatívne rozhoduje o právach a povinnostiach subjektov, či už priamo alebo sprostredkovane. Subjekt, o ktorého právach alebo povinnostiach rozhoduje orgán verejnej moci, nie je v rovnoprávnom postavení s týmto orgánom a obsah rozhodnutia tohoto orgánu nezávisí od vôle subjektu. Verejnú moc vykonáva štát predovšetkým prostredníctvom orgánov moci zákonodarnej, výkonnej a súdnej a za určitých podmienok ju môžu vykonávať aj prostredníctvom ďalších subjektov. Kritériom pre určenie, či iný subjekt koná ako orgán verejnej moci, je skutočnosť, či konkrétny subjekt rozhoduje o právach a povinnostiach iných osôb a tieto rozhodnutia sú štátnou mocou vynútiteľné, či môže štát do týchto práv a povinností zasahovať.[4]

Vo všetkých týchto prípadoch sa zameriava definovanie tohto pojmu na prípady, keď sa rozhoduje o individuálnych právach, právom chránených záujmoch a povinnostiach. Z daného dôvodu tieto definície nemožno považovať za plne uspokojivé. Právna teória pripomína, že obchádza iné javové formy, v ktorých sa verejná moc prejavuje - iné druhy právomoci, nič nehovorí o právotvorbe (normotvorbe), mlčí o rozhodovacích procesoch uskutočňovaných pri výkone riadiacej a organizátorskej činnosti, mlčí o rozhodovacích procesoch verejnej správy pri uzatváraní verejnoprávnych zmlúv, nezaoberá sa uskutočňovaním rôznych bezprostredných zákrokov a iných opatrení obdobnej povahy.[5]

Vo všetkých prípadoch však prichádza k zhode, že verejná moc je mocou autoritatívnou a jej nositeľmi sú zásadne orgány verejnej moci.

Pojem orgán verejnej moci je pojmom, ktorý sa bežne používa v legislatívnej úprave, právnej praxi, ako aj v bežnom živote. Čo sa ním rozumie?

---

[4] Uznesenie Ústavného súdu ČSFR sp. zn. I. ÚS 191/92 z 9. júna 1992.

[5] ŠKROBÁK, J. Kategória verejnej moci a jej význam vo verejnej správe a vo vede správneho práva. *In Míľniky práva v stredoeurópskom priestore 2008. Bratislava* : VO PraF UK, 2008, s. 652-653.

V legislatívnej praxi sa stretávame predovšetkým s pojmami ako napríklad orgán verejnej moci, orgán štátnej správy, orgán verejnej správy, štátny orgán, a podobne.

V rámci výkladu sa budeme venovať najprv hmotnoprávnym pojmom orgán verejnej moci, štátny orgán, orgán verejnej správy, orgán štátnej správy. Pre tieto pojmy platí, že ich definíciu nevymedzuje zákon (neexistuje ich legálna definícia), a preto ich vymedzenie je ponechané na právnu teóriu. Pojem správny orgán je procesnoprávnym pojmom a budeme sa mu venovať na záver tejto state.

Najširším pojmom zo všetkým hmotnoprávnych pojmov, ktoré sme použili, je pojem orgán verejnej moci. Ide o orgán, ktorý je zo zákona držiteľom verejnej moci. Ide o typ orgánu, ktorý v sebe kombinuje všetky orgány verejnej správy, štátne orgány, ako aj orgány štátnej správy. Platí preto, že všetky orgány verejnej moci, štátnej moci a orgány štátnej správy sú zároveň orgánmi verejnej moci. Prejdime si všetky zvolené pojmy a poukážme si na rozdiely medzi nimi.

Jedným zo základných pojmov správneho práva je pojem orgán verejnej správy. Ide o pojem, ktorý je užší ako orgán verejnej moci (nie všetky orgány verejnej moci sú aj orgánmi verejnej správy) a naopak širší ako napríklad štátny orgán a orgán štátnej správy. Orgánom verejnej správy sú okrem orgánov štátnej správy aj orgány územnej a záujmovej samosprávy a právnické osoby, ak im zákon zveruje rozhodovanie o právach, právom chránených záujmoch a povinnostiach v oblasti verejnej správy.[6]

Orgán verejnej správy môže, ale aj nemusí byť štátnym orgánom. Dôležité je, či danému orgánu je alebo nie je zverená rozhodovacia právomoc v oblasti verejnej správy. Z daného dôvodu preto orgánom verejnej správy sú všetky orgány štátnej správy, ale neplatí, že všetky štátne orgány sú aj orgánmi verejnej správy. Napríklad štátnym orgánom, ktorý nie je orgánom verejnej správy, je prezident, verejný ochranca práv, Najvyšší kontrolný úrad SR, súdy alebo prokuratúra. A naopak, orgánom verejnej správy, ktorý je aj štátnym orgánom, sú napríklad ministerstvá, okresné úrady, regionálne úrady verejného zdravotníctva a tak ďalej.

Pojem orgán verejnej správy je strešný pojem pre početnú množinu subjektov rôzneho druhu, ktoré uskutočňujú podzákonnú a organizujúcu aktivitu vo verejných záležitostiach. Inými slovami povedané, orgán verejnej správy je subjekt vykonávajúci

[6] SREBALOVÁ, M. Vývoj terminológie verejnej správy (s osobitným zreteľom na pojem správny orgán) v súčasnosti. *In Správní právo, roč. 39, č. 4/2006*, s. 252.

podzákonnú a organizujúcu činnosť vo verejných záležitostiach ako prejav výkonnej moci v štáte.[7]

Štátny orgán je orgán štátnej moci, ide o synonymické pojmy. Štátny orgán je súčasťou štátneho mocenského mechanizmu, je nadaný určitou pôsobnosťou a právomocou, ktorej cieľom je zabezpečenie plnenia štátnych úloh. Najväčšiu skupinu štátnych orgánov tvoria orgány štátnej správy. Platí pravidlo, že každý orgán štátnej správy je zároveň štátnym orgánom, ale nie každý štátny orgán musí byť aj orgánom štátnej správy. Ako príklad môže slúžiť prezident, Najvyšší kontrolný úrad SR, súdy, prokuratúra, Národná banka Slovenska alebo verejný ochranca práv. V týchto prípadoch ide o štátne orgány, ktoré nie sú orgánmi štátnej správy. Štátnymi orgánmi, ktoré sú aj orgánmi štátnej správy, sú opäť napríklad ministerstvá, okresné úrady, regionálne úrady verejného zdravotníctva a tak ďalej.

Orgán štátnej správy predstavuje v teórii a v praxi rozlične vnímaný pojem. Jednotne akceptovaná definícia tohto pojmu chýba. Zrejme najzákladnejšie vymedzenie orgánu štátnej správy vychádza z pozitívnoprávnej úpravy. Podľa tohto vymedzenia orgánom štátnej správy je ten orgán, ktorý je takto zákonom vytvorený, t. j. zákon priamo pomenuje niektorý orgán za orgán štátnej správy.[8]

K základným črtám orgánov štátnej správy sa zaraďuje to, že:

a) ide o štátny orgán, ktorý má všetky základné črty tohto orgánu, je vybavený právomocou a pôsobnosťou a má možnosť použiť prostriedky štátneho donútenia,
b) ide o osobitný druh štátneho orgánu, ktorého osobitosť spočíva v činnosti, ktorú vykonáva, t. j. štátnu správu, ktorou uskutočňuje úlohy a funkcie štátu metódami a prostriedkami štátnej správy,
c) tvorí relatívne samostatnú organizačnú jednotu, ktorá je oddelená od iných organizačných jednotiek v štátnom aparáte.[9]

K ďalším špecifickým znakom orgánov štátnej správy možno zaradiť aj to, že jeho činnosť má výkonný a nariaďovací charakter; môže na základe splnomocnenia vydávať všeobecne záväzné právne predpisy; jeho činnosť možno v rámci práva determinovať aj smernicami a inými vnútornými predpismi nadriadených orgánov.[10]

---

[7] TÓTHOVÁ, K. Niekoľko úvah k pojmom správny orgán, orgán štátnej správy a orgán verejnej správy. *In Pocta profesorovi Slovinskému. Bratislava : Univerzita Komenského v Bratislave*, Právnická fakulta, 2009, s. 104.
[8] Napríklad podľa § 2 ods. 1 zákona č. 180/2013 Z. z. o organizácii miestnej štátnej správy okresný úrad je miestny orgán štátnej správy.
[9] ŠKULTÉTY, P. *In ŠKULTÉTY, P. a kol. Správne právo hmotné. Všeobecná časť.* Bratislava : VO PraF UK, 2005, s. 51.
[10] KOŠIČIAROVÁ, S. Správne právo hmotné. *Všeobecná časť.* Plzeň : Aleš Čeněk, 2015, s. 45-46.

Zhrňujúco povedané, orgány štátnej správy sú relatívne samostatné súčasti štátneho mechanizmu dotované právomocou, ktorých prostredníctvom štát plní svoje úlohy v oblasti verejnej správy. Musia byť zriadené zákonom ako orgány štátnej správy. Prevažnú časť ich činnosti tvorí výkon štátnej správy.[11] Orgán štátnej správy nemusí vykonávať nevyhnutne len štátnu správu. Orgány štátnej správy vykonávajú aj iné aktivity ako napríklad rôzne úkony občianskoprávneho, obchodnoprávneho, či pracovnoprávneho charakteru, propagačné činnosti a pod.

Veľmi dôležité je tiež dopovedať, že za každých okolností, na to, aby sme mohli uvažovať o orgáne štátnej správy, je nevyhnutné, aby prevažujúca časť jeho aktivít bola výkonom štátnej správy.[12]

Posledným pojmom, ktorému sa na tomto mieste chceme venovať, je pojem správny orgán. Na rozdiel od zvyšných pojmov, pojem správny orgán je procesnoprávnym termínom, ktorý je aj legálne definovaný. To znamená, že priamo právne predpisy tento pojem vymedzujú a neponechávajú jeho definíciu na právnu teóriu a prax. Priamu definíciu tohto pojmu nachádzame v Správnom poriadku (zákon č. 71/1967 Zb. o správnom konaní [správny poriadok]). Podľa § 1 ods. 2 Správneho poriadku správnym orgánom je štátny orgán, orgán územnej samosprávy, orgán záujmovej samosprávy, fyzická osoba alebo právnická osoba, ktorej zákon zveril rozhodovanie o právach, právom chránených záujmoch alebo povinnostiach fyzických osôb a právnických osôb v oblasti verejnej správy.

Dôležitosť tohto pojmu spočíva v tom, že na základe pravidiel určených v ďalších ustanoveniach Správneho poriadku[13] dokážeme určiť presne jeden orgán, ktorý bude tým jediným vykonávateľom verejnej správy v jednotlivo určenom prípade, teda tým, ktorý bude v našej veci rozhodovať.

Napríklad, ak na základe hmotnoprávnej úpravy vieme, že okresné úrady vykonávajú štátnu správu na úseku živnostenského podnikania, tak na tomto základe ešte nevieme určiť, na ktorý zo všetkých okresných úradov sa musíme obrátiť s ohlásením živnosti, ak chceme prevádzkovať živnosť. Na to slúži právna úprava určovania príslušnosti správnych orgánov. Na jej základe sa presunieme zo všeobecného vymedzenia okresný úrad (zo všeobecnej

[11] ŠKROBÁK, J. *In VRABKO, M. a kol. Správne právo hmotné*. Všeobecná časť. Bratislava : C. H. Beck, 2012, s. 20.
[12] TÓTHOVÁ, K. Niekoľko úvah k pojmom správny orgán, orgán štátnej správy a orgán verejnej správy. *In Pocta profesorovi Slovinskému. Bratislava : Univerzita Komenského v Bratislave*, Právnická fakulta, 2009, s. 99.
[13] Ide o ustanovenia o príslušnosti. Rozoznávame príslušnosť vecnú, miestnu a funkčnú. Tieto pravidlá nie sú upravené len v Správnom poriadku, ale môžu byť predmetom právnej úpravy aj v osobitných právnych predpisoch (napríklad v Daňovom poriadku, zákone o sociálnom poistení a tak ďalej).

hmotnoprávnej pôsobnosti tohto orgánu) k jednotlivo určenému okresnému úradu, napríklad Okresný úrad Bratislava, Okresný úrad Pezinok alebo Okresný úrad Košice, a tak ďalej[14] (t. j. k procesnoprávnej úprave miestnej príslušnosti správneho orgánu) a zároveň ku konkrétnej vnútornej organizačnej jednotke tohto úradu, ktorá je príslušná na ohlasovanie živnosti (tzv. funkčná príslušnosť) – v prípade živností je to odbor živnostenského podnikania okresného úradu. Zhrňujúco povedané, procesnoprávnou kategóriou správneho orgánu sme zistili, že vo veciach ohlásenia živnosti je orgánom zodpovedným za jej ohlásenie v konkrétnom prípade[15] (napríklad) Okresný úrad Bratislava, odbor živnostenského podnikania.

Možno si tiež povšimnúť, že pri definovaní pojmu správny orgán vychádzal zákonodarca z hmotnoprávnych pojmov ako štátny orgán alebo orgán územnej samosprávy. Z daného vyplýva, že správne orgány nemajú svoju druhovú identitu a nie sú špecifickým druhom orgánov v oblasti verejnej správy.[16] Pojem správny orgán znamená určitú pozíciu pre všetky tie subjekty, ktoré zákon označí ako realizátorov mocenského rozhodovania o právach, právom chránených záujmoch a povinnostiach fyzických osôb a právnických osôb v oblasti verejnej správy (teda označí ich za správne orgány – pozn. autora). Správne orgány teda nie sú samostatným druhom orgánov verejnej správy.[17]

Z definície verejnej moci ďalej vyplýva, že orgány verejnej moci rozhodujú o právach, právom chránených záujmoch alebo o povinnostiach fyzických osôb alebo právnických osôb.

Rozhodovanie predstavuje autoritatívne ovplyvňovanie právneho postavenia fyzických osôb a právnických osôb, ktoré prebieha práve na základe tejto činnosti, pričom postup orgánov verejnej moci a ďalších subjektov na tomto postupe je regulovaný právnym poriadkom.

Rozhodovacie procesy sa niekedy nazývajú aj pojmom aplikačné procesy. Podstatou aplikačných rozhodovacích procesov je rozhodovanie o (hmotnoprávnych) právach, právom chránených záujmoch alebo o povinnostiach konkrétnych účastníkov tohto procesu. Platí, že súkromné osoby môžu konať, čo nie je zákonom zakázané, a nikoho

[14] Vychádza sa z pravidla, že živnosť sa ohlasuje tomu okresnému úradu, kde fyzická osoba má trvalý pobyt, alebo kde právnická osoba má sídlo.
[15] Teda tým orgánom, ktorý v tejto veci vykonáva verejnú správu.
[16] Ako je to v prípade hmotnoprávnych pojmov, ktoré sú uvedené v predchádzajúcom texte.
[17] TÓTHOVÁ, K. Sú správne orgány samostatným druhom orgánov verejnej správy? *In MASLEN, M. (ed.) Správne súdnictvo a jeho rozvojové aspekty. Bratislava : Ikarus.sk – Eurounion,* 2011, s. 332.

nemožno nútiť, aby konal niečo, čo zákon neukladá.[18] Uplatňovanie niektorých práv je však v právnom štáte niekedy naviazané na predchádzajúci úkon zo strany verenej moci, ktorým buď umožňuje uplatnenie určitého práva,[19] alebo potvrdzuje existenciu daného práva. Výsledkom aplikačného rozhodovacieho procesu je vydanie aktu, ktorým sa definitívnym spôsobom upravuje právne postavenie konkrétnej osoby v konkrétnom prípade.

Napríklad, ak vodič motorového vozidla prekročí povolenú rýchlosť, tak v rozhodovacom aplikačnom procese príslušný orgán rozhodne o tom, že toto jeho konanie naplnilo skutkovú podstatu správneho deliktu (priestupku) a rozhodne o uložení pokuty tomuto vodičovi. V rámci tohto procesu sa teda rozhodlo o konkrétnej (novej) povinnosti vodiča motorového vozidla, ktoré spočíva v povinnosti zaplatiť peňažnú pokutu.

Rozhodovanie sa týka práv, právom chránených záujmov alebo povinností. Právo osoby sa v právnej teórii definuje ako možnosť a) správať sa určitým spôsobom, ktorý má svoje zákonné medze, b) požadovať určité správanie od iných osôb (minimálne, aby sa zdržali rušenia oprávneného správania), c) požadovať od verejno-mocenského orgánu právnu ochranu svojho práva pred jeho neoprávneným rušením. Právna teória definuje právom chránený záujem ako taký záujem fyzickej osoby alebo právnickej osoby, ktorému právne predpisy poskytujú osobitnú ochranu (a rozdiel od iných – faktických záujmov, ktorým sa právna ochrana neposkytuje). Právom chránené záujmy sú (...) vždy tesne zviazané so subjektívnymi právami a povinnosťami, o ktorých sa rozhoduje. Pretože o subjektívnych záujmoch nemožno rozhodovať (nemožno ich zakladať, meniť, rušiť), a pretože sú dané platnou úpravou, nemôžu byť ani predmetom (...) konania. Ich nositeľ ich presadzuje v konaní spolu so svojimi subjektívnymi právami alebo ich uplatňuje pri rozhodovaní o právach a povinnostiach iných osôb. Povinnosť osoby sa v právnej teórii vymedzuje ako nevyhnutnosť správať sa určitým spôsobom (konať, zdržať sa konania, niečo strpieť).[20]

Fyzickou osobou má na mysli akákoľvek osoba, a to bez ohľadu na jej štátne občianstvo, trvalý pobyt, či prechodný pobyt. Je tiež irelevantné, či ide o cudzinca alebo o osobu bez štátneho občianstva, či s viacerými štátnymi občianstvami.

[18] Pozri čl. 2 ods. 3 Ústavy Slovenskej republiky.
[19] Môže pritom dôjsť aj k vymedzeniu limitov uplatňovania práva.
[20] KOŠIČIAROVÁ, S. *Správne právo procesné. Všeobecná časť.* Šamorín : Heuréka, 2017, s. 120.

Právnickú osobu vymedzuje Občiansky zákonník ako a) združenie fyzických alebo právnických osôb, b) účelové združenie majetku, c) jednotku územnej samosprávy, d) iné subjekty, o ktorých to ustanovuje zákon.[21]

Združenia fyzických osôb alebo právnických osôb sú najmä obchodné spoločnosti a družstvá, občianske združenia, politické strany a hnutia, cirkvi a náboženské spoločnosti, či združenia právnických osôb. Účelové združenia majetku sú fondy a nadácie. Jednotky územnej samosprávy sú obce a vyššie územné celky (samosprávne kraje). Iné subjekty, o ktorých to ustanovuje zákon, sú najmä štátne podniky, rozpočtové organizácie a príspevkové organizácie zriadené orgánmi štátnej správy alebo orgánmi územnej samosprávy a ďalšie subjekty, o ktorých to ustanovuje zákon.

1.3 Výkon verejnej moci elektronicky

V predchádzajúcej kapitole sme si vymedzili, čo sa rozumie pojmom verejná moc. Tento krok bol nevyhnutný z toho dôvodu, lebo E-govZ sa venuje elektronickému výkonu verejnej moci. Na základe základného vymedzenia verejnej moci sme si ozrejmili, čo by zásadne malo podliehať elektronizácii (jej elektronickému výkonu).

Uvedené teoretické vymedzenie pojmu verejná moc v zásade kopíruje vymedzenie tohto pojmu v E-govZ. Podľa § 3 písm. a) tohto zákona sa výkonom verejnej moci rozumie konanie orgánu verejnej moci v rozsahu podľa osobitných predpisov, vo veciach práv, právom chránených záujmov a povinností fyzických osôb alebo právnických osôb. Vidno, že všetky pojmy, ktoré sú tu využité, sme vymedzili v predchádzajúcej kapitole. Konaním sa rozumie rozhodovanie o právach, právom chránených záujmoch a povinnostiach. V rozsahu podľa osobitných predpisov sa rozumie vymedzenie pôsobnosti orgánu verejnej moci v tom-ktorom zákone. Pojmy orgán verejnej moci, fyzická osoba a právnická osoba boli taktiež predmetom predchádzajúceho výkladu.

E-govZ nevymedzuje výkon verejnej moci elektronicky len pozitívne, t. j. na čo všetko sa vzťahuje, ale vymedzuje ho aj negatívne, t. j., na aký výkon verejnej moci elektronicky sa nevzťahuje. Negatíve vymedzenie pôsobnosti zákona, a teda aj výkonu verejnej moci elektricky, nájdeme v § 2 E-govZ. Toto vymedzenie je dané predovšetkým zachovaním verejného záujmu, keď v niektorých záležitostiach výkonu verejnej moci nie je vhodné, aby sa komunikovalo elektronicky. Ako príklad možno uviesť výkon verejnej moci elektronicky a

[21] § 18 ods. 2 Občianskeho zákonníka.

elektronickú komunikáciu orgánov verejnej moci navzájom, ak sú ich obsahom utajované skutočnosti alebo citlivé informácie, ďalej informačné systémy verejnej správy, ktoré sa týkajú zabezpečenia obrany Slovenskej republiky, bezpečnosti Slovenskej republiky alebo ktoré obsahujú utajované skutočnosti, či informačné systémy verejnej správy, ktoré obsahujú údaje spracúvané na účely poskytovania zdravotnej starostlivosti, a na informačné systémy obsahujúce údaje o zdravotnom stave osoby na účely výkonu verejného zdravotného poistenia.

V nasledujúcich riadkoch sa už budeme zaoberať výkonom verejnej moci elektronicky v pozitívnom slova zmysle. Výkonom verejnej moci elektronicky sa rozumie výkon verejnej moci prostredníctvom elektronickej úradnej komunikácie, t. j. ide o prenos elektronických správ elektronickými prostriedkami medzi komunikujúcimi subjektmi obsahujúci identifikáciu odosielateľa a adresáta, pri ktorej je prenášaná elektronická úradná správa, ktorá je tvorená jedným elektronickým podaním alebo elektronickým úradným dokumentom vrátane príloh k nim, ak sa prílohy pripájajú.

Rozdiel medzi elektronickým podaním a elektronickým úradným dokumentom spočíva v tom, od koho takáto elektronická úradná správa pochádza. V prípade elektronického podania ide o účastníka konania (fyzickú osobu, právnickú osobu) a v prípade elektronického úradného dokumentu ide o orgán verejnej moci.

Elektronickým podaním sú údaje vyplnené podľa elektronického formulára, ktoré na účely výkonu verejnej moci elektronicky alebo na účely jeho začatia zasiela orgánu verejnej moci osoba, ktorá je účastníkom konania. Elektronickým úradným dokumentom sú údaje vyplnené podľa elektronického formulára,

a) ktorý je výsledkom konania orgánu verejnej moci pri výkone verejnej moci elektronicky,
b) ktorý pri výkone verejnej moci elektronicky alebo na účely jeho začatia zasiela orgán verejnej moci osobe, ktorá je účastníkom konania, alebo
c) ktorým orgán verejnej moci vyznačuje právne skutočnosti týkajúce sa elektronického úradného dokumentu, najmä údaje o jeho právoplatnosti alebo vykonateľnosti.

Elektronickým formulárom je elektronický dokument obsahujúci automatizovane spracovateľné pravidlá, prostredníctvom ktorých je možné elektronickými prostriedkami vyplniť a prezentovať vyplnené údaje v štruktúrovanej forme, spracovateľnej aj automatizovaným spôsobom informačnými systémami.

Na účely výkonu verejnej moci elektronicky zabezpečujú orgány verejnej moci, v rozsahu svojej pôsobnosti podľa zákona, vytvorenie a prevádzku

a) prístupových miest,

b) spoločných modulov a

c) agendových systémov.

Z uvedeného je na účely elektronickej komunikácie najdôležitejšie bližšie sa venovať prístupovému miestu. Je to tak preto, lebo elektronická komunikácia medzi orgánom verejnej moci a fyzickou osobou alebo právnickou osobou prebieha práve prostredníctvom prístupového miesta. E-govZ vymedzuje, že prístupové miesta sú komunikačné rozhrania, ktorých prostredníctvom je možné vykonávať elektronickú komunikáciu, ktoré sú určené na zabezpečenie kontaktu medzi orgánom verejnej moci a osobami, o ktorých právach, právom chránených záujmoch a povinnostiach orgány verejnej moci pri výkone verejnej moci elektronicky konajú alebo vo vzťahu ku ktorým verejnú moc vykonávajú.

Prístupovými miestami sú

a) ústredný portál verejnej správy,

b) špecializované portály,

c) integrované obslužné miesta,

d) ústredné kontaktné centrum.

Ústredný portál verejnej správy je prevádzkovaný prostredníctvom webového sídla www.slovensko.sk. Jeho prostredníctvom možno centrálne vykonávať elektronickú úradnú komunikáciu s ktorýmkoľvek orgánom verejnej moci a pristupovať k spoločným modulom.

Správcom ústredného portálu verejnej správy je Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu (ďalej len „ÚPPV"). ÚPPV zabezpečuje na ústrednom portáli zverejnenie zoznamu všetkých orgánov verejnej moci spolu s označením konaní o právach, právom chránených záujmoch a povinnostiach osôb, ktorých sa týka. Úlohou jednotlivých orgánov verejnej moci je zabezpečiť tvorbu informačného obsahu o svojej činnosti pre verejnosť a ten zverejňovať a aktualizovať prostredníctvom ústredného portálu verejnej správy. Zodpovednosť za správnosť a úplnosť údajov nesie orgán verejnej moci a nie ÚPPV.

Na rozdiel od ústredného portálu verejnej správy, špecializovaný portál slúži na elektronickú komunikáciu s jedným alebo viacerými orgánmi verejnej správy. Špecializovaný portál preto nemá centrálny, zastrešujúci charakter, ale slúži len

konkrétnemu orgánu verejnej moci; nevyužíva sa preto na elektronickú komunikáciu s akýmkoľvek orgánom verejnej moci. Ak sa tak orgány verejnej moci dohodnú medzi sebou navzájom, môže špecializovaný portál slúžiť aj viacerým orgánom verejnej moc na elektronickú komunikáciu.

Ako príklad špecializovaných portálov možno uviesť portál Finančnej správy Slovenskej republiky, portál elektronických služieb Ministerstva vnútra Slovenskej republiky, elektronické služby Ministerstva spravodlivosti Slovenskej republiky, eHealth, či elektronické verejné obstarávanie.

Aj keď orgán verejnej moci prevádzkuje špecializovaný portál, je naďalej povinný umožniť elektronickú komunikáciu s fyzickými osobami či právnickými osobami a umožniť využívanie elektronickej služby verejnej správy aj prostredníctvom ústredného portálu verejnej správy, t. j. aj prostredníctvom webového sídla www.slovensko.sk.

Zatiaľ čo ústredný portál verejnej správy a špecializovaný portál slúžia na elektronickú komunikáciu, ktorú fyzická osoba alebo právnická osoba vykonáva sama, integrované obslužné miesto slúži na asistovanú elektronickú úradnú komunikáciu fyzických osôb a právnických osôb s orgánmi verejnej moci pri výkone verejnej moci elektronicky. Prostredníctvom integrovaného obslužného miesta je možné vykonávať zaručenú konverziu[22] a elektronicky komunikovať s orgánom verejnej moci na účely výkonu verejnej moci elektronicky, ako aj vykonávať ďalšie činnosti, ak tak ustanoví zákon.

Integrované obslužné miesto prevádzkuje každá obec alebo mestská časť, ktoré sú matričným úradom. Obce (mestské časti) sú integrovanými obslužnými miestami *ex lege*, teda priamo zo zákona. Na základe žiadosti a následného zápisu do registra prevádzkarní integrovaných obslužných miest môže integrované obslužné miesto prevádzkovať aj iný orgán verejnej moci alebo poštový podnik poskytujúci univerzálnu službu (t. j. Slovenská pošta, a. s.).

Pracovník integrovaného obslužného miesta je na žiadosť a so súhlasom toho, kto prostredníctvom integrovaného obslužného miesta žiada o asistovanú elektronickú komunikáciu s orgánmi verejnej moci pri výkone verejnej moci elektronicky, oprávnený pri výkone činností integrovaného obslužného miesta autorizovať právny úkon žiadateľa

[22] Konverzia je postup, pri ktorom je celý, bežne zmyslami vnímateľný, informačný obsah pôvodného a) elektronického dokumentu transformovaný do novovzniknutého dokumentu v listinnej podobe, b) dokumentu v listinnej podobe transformovaný do novovzniknutého elektronického dokumentu alebo c) elektronického dokumentu transformovaný do novovzniknutého elektronického dokumentu. Zaručenou konverziou je konverzia s cieľom zachovania právnych účinkov pôvodného dokumentu a jeho použiteľnosti na právne úkony vykonaná postupom pre zaručenú konverziu podľa E-govZ.

použitím kvalifikovaného elektronického podpisu vyhotoveného s použitím mandátneho certifikátu, ku ktorému pripojí kvalifikovanú elektronickú časovú pečiatku alebo s použitím autorizácie prostredníctvom na to určenej funkcie informačného systému prístupového miesta a po úspešnej autentifikácii osoby, ktorá autorizáciu vykonáva, zodpovedajúcej najmenej úrovni zabezpečenia „pokročilá“, ak sa autentifikuje s použitím úradného autentifikátora.

Ak je elektronický dokument autorizovaný pracovníkom integrovaného obslužného miesta a súčasne aj autorizovaný správcom informačného systému integrovaného obslužného miesta, považuje sa takýto elektronický dokument za autorizovaný osobou, ktorá prostredníctvom integrovaného obslužného miesta vykonáva asistovanú elektronickú komunikáciu s orgánmi verejnej moci, ak sa nepreukáže opak.

Pracovník integrovaného obslužného miesta je oprávnený na prístup a disponovanie s elektronickou schránkou na účely preberania alebo sprístupnenia elektronických správ, ak ho o to osoba oprávnená na prístup a disponovanie s elektronickou schránkou písomne požiada a ak sa úspešne autentifikuje; takýto prístup a disponovanie sú možné len prostredníctvom informačného systému integrovaného obslužného miesta a na základe každej žiadosti je možné pristúpiť a disponovať s elektronickou schránkou len jednorazovo.

V praxi sa s integrovaným obslužným miestom možno najčastejšie stretnúť prostredníctvom vybraných pobočiek Slovenskej pošty, a. s., pričom k najčastejším úkonom, ktoré sú poskytované, patria žiadosti o výpisy a odpisy z registra trestov, výpis z Listu vlastníctva a výpis z obchodného registra.

Ústredné kontaktné centrum slúži na poskytovanie informácií o výkone verejnej moci elektronicky a o činnosti orgánov verejnej moci s tým súvisiacej, ak také poskytovanie informácií nie je v rozpore s osobitnými predpismi a ako jednotné miesto na nahlasovanie technických problémov znemožňujúcich postup podľa E-govZ a potvrdzovanie existencie týchto problémov a ich trvania. Ústredné kontaktné centrum je prevádzkované prostredníctvom telefónneho čísla +421 2 35 803 083 (pracovné dni v pondelok až v piatok, od 8.00h do 18.00 h, v stredu od 8.00 h do 21.00 h), ako aj prostredníctvom webového sídla https://helpdesk.slovensko.sk/new-incident/.

Ústredné kontaktné centrum funguje od novembra 2013, pričom za prvých päť rokov svojej existencie vybavili vyše 210 000 požiadaviek.[23]

V rámci ústredného portálu verejnej správy ÚPPV vytvára spoločné moduly (t. j. spoločné komunikačné rozhrania pre všetky orgány verejnej moci). Tie sú určené na zabezpečenie elektronickej komunikácie. ÚPPV je zodpovedný za ich aktualizáciu. Spoločné moduly sú napríklad modul elektronických schránok, autentifikačný modul, platobný modul, modul centrálnej elektronickej podateľne, modul elektronických formulárov, modul elektronického doručovania, notifikačný modul. Orgány verejnej moci sú povinné využívať modul elektronických schránok, autentifikačný modul, modul elektronických formulárov a modul elektronického doručovania. Ak tak ustanovuje zákon, sú povinné využívať aj platobný modul. Príkladom právneho predpisu, ktorý takúto povinnosť upravuje, je napríklad § 9 ods. 2 zákona č. 71/1992 Zb. o súdnych poplatkoch a poplatku za výpis z registra trestov alebo § 7 ods. 2 zákona č. 145/1995 Z. z. o správnych poplatkoch. Túto povinnosť tieto osobitné zákony označujú ako povinnosť (možnosť) vykonať úhradu prostredníctvom integrovaného obslužného miesta.

1.3.1 Zriadenie, aktivácia, prístup, deaktivácia a zrušenie elektronickej schránky

Významnou súčasťou E-govZ je právna úprava dotýkajúca sa elektronickej schránky. Možno dokonca povedať, že ide o gro daného právneho predpisu, pretože predstavuje vôbec predpoklad elektronickej komunikácie. Bez elektronickej schránky zriadenej príslušným subjektom si elektronickú komunikáciu nemožno predstaviť.

Zriadením elektronickej schránky sa má na mysli jej vytvorenie, t. j. elektronická schránka reálne existuje a možno do nej získať prístup. Zriadená elektronická schránka ešte neznamená, že aj slúži na ten účel, na ktorý vznikla, teda na elektronickú komunikáciu, ktorá má aj právne účinky. Na to slúži až aktivácia elektronickej schránky (pozri ďalej v texte).

Zriaďovateľom elektronickej schránky je správca modulu elektronických schránok, ktorým je ÚPPV.

Z E-govZ vyplýva rozsah subjektov, ktorým sa priamo zo zákona (*ex lege*) zriaďuje elektronická schránka. Povinné zriadenie elektronickej schránky sa týka orgánu verejnej moci, právnickej osoby, fyzickej osoby, podnikateľa a subjektu medzinárodného práva.

[23] Dostupné na internete: <https://www.nases.gov.sk/ustredne-kontaktne-centrum-za-pat-rokov-pomohlo-vyse-200-tisic-ludom/>, cit. 2019-09-16.

Okrem toho sa môže zriadiť elektronická schránka aj organizačnej zložke alebo organizácii, avšak len za podmienky, že ide o organizačnú zložku orgánu verejnej správy alebo organizáciu, ktorá nemá vlastnú právnu subjektivitu a plní úlohy podľa osobitných predpisov, ak je odôvodnené, aby na účely elektronického doručovania mala zriadenú samostatnú elektronickú schránku

Elektronickú schránku musí mať zriadený aj akýkoľvek ďalší subjekt, o ktorom to ustanoví osobitný právny predpis.

Zákon vymedzuje, že každá elektronická schránka musí spĺňať určité úlohy súvisiace s jej používaním. Elektronické schránky musia byť dostupné, zabezpečené tak, aby tu bola možnosť ich aktivácie, zmeny a zrušenia, musia uchovávať elektronické správy a elektronické dokumenty s obsahom totožným, v akom boli do elektronickej schránky prijaté a zaznamenávať dátum a čas napríklad prístupu do elektronickej schránky či odoslania a prijatia elektronickej správy do elektronickej schránky.

ÚPPV zriaďuje elektronickú schránku bezodplatne. Spoplatneniu podlieha zvýšenie kapacity elektronickej schránky v súčasnosti ustanovenej na 1 GB.[24] Podľa vyhlášky Úradu vlády Slovenskej republiky 8/2014 Z. z. ktorou sa vykonávajú niektoré ustanovenia zákona o e-Governmente náklady za zvýšenie základnej úložnej kapacity elektronickej schránky na obdobie jedného roka sú ustanovené tak, že zvýšenie o 1 GB je spoplatnené sumou 10 eur, o 10 GB 100 eur a o 100 GB 1 000 eur. Z výročnej správy za rok 2018 Národnej agentúry pre sieťové a elektronické služby vyplýva, že za rok 2018 bolo podaných 1044 takýchto žiadostí.[25]

Bezodplatnosť sa tiež týka aj situácie, ak osoba, ktorej bola schránka zriadená, sa nachádza vo viacerých postaveniach. Čo to znamená?

Treba povedať, že fyzické osoby sa môžu nachádzať v rôznom právnom postavení vo vzťahu k tretím subjektom. Môžu vystupovať ako súkromná osoba, môžu vystupovať ako osoba konajúca v mene inej osoby, prípadne môžu vystupovať aj ako orgán verejnej moci. Napríklad notár vystupuje v právnych vzťahoch ako samostatná súkromná fyzická osoba (napríklad nákup v potravinách), ale taktiež vystupuje ako notár (orgán verejnej moci), ktorý

[24] Na úplnosť uvediem, že podľa E-govZ ÚPPV upovedomí pri dosiahnutí určenej úrovne naplnenia úložnej kapacity majiteľa elektronickej schránky o tejto skutočnosti, a ak je majiteľ elektronickej schránky nečinný, môže zabezpečiť odstránenie elektronických správ a notifikácií v poradí od najskôr uložených až do dosiahnutia určitej voľnej úložnej kapacity, pričom neodstraňuje elektronické správy a notifikácie, ktoré neboli prečítané; odstránenie je možné vykonať najskôr po uplynutí 60 dní odo dňa doručenia upovedomenia a na tretí deň nasledujúci po dni prečítania elektronickej správy alebo notifikácie.

[25] NÁRODNÁ AGENTÚRA PRE SIEŤOVÉ A ELEKTRONICKÉ SLUŽBY. Výročná správa za rok 2018, s. 22. Dostupné na internete <https://www.nases.gov.sk/wp-content/uploads/2019/05/NASES_Vyrocna_sprava_2018.pdf >, cit. 2019-09-19.

na základe poverenia zabezpečuje napríklad dedičské konania. Iným príkladom môže byť daňový poradca, ktorý tiež vystupuje ako súkromná fyzická osoba, ďalej ako daňový poradca (t. j. podnikateľ) a taktiež nie je vylúčené, aby figuroval ako napríklad štatutárny zástupca nejakej právnickej osoby (obchodenej spoločnosti).

S cieľom, aby nedochádzalo k zamieňaniu právneho postavenia, v ktorom vystupuje daná osoba, zákon ustanovuje, že každému je možné zriadiť len jednu elektronickú schránku pre jedno právne postavenie. Ak je majiteľ elektronickej schránky súčasne osobou vo viacerých právnych postaveniach, zriaďuje sa mu elektronická schránka pre každé z týchto právnych postavení. To znamená, že ak by daňový poradca vystupujúci v našom príklade bol súkromnou osobou, poradcom a štatutárom, pre každé toto postavenie musí mať zriadenú jednu elektronickú schránku, t. j. v tomto prípade by išlo o tri elektronické schránky.

Štátnym orgánom, obciam (mestám) a vyšším územným celkom sa vždy zriaďuje iba jedna elektronická schránka. Iným subjektom ako napríklad zdravotným poisťovniam, školám, Sociálnej poisťovniam sa vytvárajú dve; jedna ako orgánu verejnej moci a jedna ako právnickej osobe.[26]

Subjekt, ktorému bola zriadená elektronická schránka, je zároveň aj jej majiteľom. To z pohľadu súkromného práva by vo všeobecnosti malo znamenať, že elektronická schránka je spôsobilým predmetom jednotlivých scudzovacích úkonov, t. j. je predmetom kúpy, darovania alebo zámeny. Kúpa, darovanie a zámena elektronickej schránky by však bola zjavne v rozpore s predmetom a účelom E-govZ, pretože by znemožňovala efektívnu elektronickú komunikáciu; uvedená činnosť by do elektronickej komunikácie vniesla chaos, pretože by bolo len ťažko sledovateľné, kto je konečným užívateľom elektronickej schránky. Na uvedené zákonodarca pamätal, a preto vylúčil dané úkony z dispozičného oprávnenia (oprávnenia nakladať so schránkou) majiteľa elektronickej schránky. Zákon priamo ustanovuje, že elektronická schránka nie je predmetom vlastníckeho práva a majiteľ elektronickej schránky je oprávnený disponovať s ňou len spôsobom ustanoveným týmto zákonom.

Elektronická schránka sa zriaďuje dvojakým spôsobom, a to priamo povinne zo zákona (*ex lege*) alebo na základe žiadosti.

Povinne sa zriaďuje elektronická schránka:

a) orgánu verejnej moci, právnickej osobe a zapísanej organizačnej zložke

[26] Pozri GREGUŠOVÁ, D., HALÁSOVÁ, Z. Zákon o e-Governmente. Komentár. Žilina : Eurokódex, 2018, s. 91-92.

b) fyzickej osobe podnikateľovi (napríklad živnostníkovi),

c) fyzickej osobe, ktorá nie je podnikateľom a ktorá dosiahla 18. rok veku.

Na základe žiadosti sa zriaďuje elektronická schránka:

a) všetkým vyššie uvedeným subjektom, ak došlo k zrušeniu ich elektronickej schránky a zároveň pominuli dôvody na deaktiváciu tejto elektronickej schránky (k príkladu pozri ďalej v texte),

b) subjektu medzinárodného práva,

c) právnickej osobe, ktorá nemá sídlo na území Slovenskej republiky,

d) fyzickej osobe, ktorá nie je štátnym občanom Slovenskej republiky,

e) štátnemu občanovi Slovenskej republiky mladšieho ako 18 rokov

f) subjektu, o ktorom to ustanoví osobitný predpis.

V prípade povinného zriadenia elektronickej schránky zákon ustanovuje, že elektronická schránka sa zriaďuje bezodkladne. Zákon bližšie neupravuje, čo možno týmto pojmom myslieť (ide o tzv. právne neurčitý pojem, resp. právne pohyblivý pojem), avšak na strane druhej treba povedať, že ide o lehotu kratšiu ako päť pracovných dní, ktorú zákon ustanovuje ako lehotu na zriadenie elektronickej schránky na žiadosť.

Ak ide o zriaďovanie elektronických schránok zo zákona, ÚPPV ich musí zriadiť bezodkladne potom, ako nastala právna skutočnosť, na ktorú je naviazané zriadenie schránky. Ak ide o orgány verejnej moci, právnické osoby a zapísané organizačné zložky, touto právnou skutočnosťou je ich vznik (napríklad zápis do obchodného registra alebo nadobudnutie účinnosti zákona). Ak ide o fyzickú osobu podnikateľa, tak okamihom vzniku podnikateľského oprávnenia (napríklad ohlásenie živnosti) a ak ide o fyzickú osobu, ktorá nie je podnikateľom (súkromná fyzická osoba), je týmto okamihom dovŕšenie 18. roku veku (deň 18. narodenín).

Vzhľadom na to, že ÚPPV nedisponuje údajmi, ktoré sú uvedené vyššie, zákon ustanovuje, že orgány verejnej moci, ktoré sú držiteľmi týchto informácií, o nich bezodkladne informujú ÚPPV. Orgánom verejnej moci, ktorý vedie register fyzických osôb (súkromných) je Ministerstvo vnútra SR. Orgánom verejnej moci, ktorý vedie register právnických osôb, podnikateľov (vrátane podnikateľov fyzických osôb) a orgánov verejnej moci je Štatistický úrad Slovenskej republiky.

V prípade elektronických schránok, ktoré sa zriaďujú na žiadosť, má ÚPPV zákonom ustanovenú lehotu piatich pracovných dní (počítaných od podania žiadosti), dokedy musí

elektronickú schránku zriadiť (samozrejme, za predpokladu, že žiadosť je úplná). Z dôvodu právnej istoty treba usúdiť, že lehota sa začína počítať od prvého pracovného dňa, ktorý nasleduje po riadnom doručení žiadosti.

Podľa E-govZ sa žiadosť podáva prostredníctvom na to určenej funkcie ústredného portálu a musí byť autorizovaná žiadateľom alebo v listinnej podobe s úradne osvedčeným podpisom žiadateľa. Ak ide o elektronickú schránku maloletého, žiadosť autorizujú alebo podpisujú obaja rodičia alebo iný zákonný zástupca a k žiadosti sa prikladá dokument preukazujúci oprávnenie zastupovať maloletého pri právnych úkonoch, ak toto oprávnenie nevyplýva z referenčného údaja.

Vo vzťahu k maloletému treba uviesť, že dané zákonné ustanovenie sa vzťahuje len na maloletého, ktorý neuzatvoril manželstvo so súhlasom súdu. Takéto manželstvo môže uzatvoriť maloletý, ktorý dovŕšil 16. rok svojho veku. Podľa Občianskeho zákonníka, ak dôjde k takejto situácii, fyzická osoba uzatvorením manželstva nadobudla plnoletosť, a teda je plne spôsobilá na právne úkony; takto nadobudnutá plnoletosť sa nestráca ani zánikom manželstva ani vyhlásením manželstva za neplatné. Z daného dôvodu, ak by došlo k zániku manželstva alebo k vyhláseniu manželstva za neplatné ešte pred dovŕšením 18. roku veru fyzickej osoby a táto osoba by zároveň žiadala o zriadenie elektronickej schránky, nepotrebuje na túto žiadosť autorizáciu alebo podpis oboch rodičov, prípadne iného zákonného zástupcu.

Na úplnosť musíme uviesť, že v prípade, ak jeden z rodičov nemá oprávnenie konať za dieťa (napríklad na základe rozhodnutia súdu alebo ak takýto rodič zomrel), tak samozrejme ÚPPV nemôže žiadať o podpis takéhoto rodiča; na podanie žiadosti bude v takom prípade stačiť podpis len druhého rodiča.

Vyššie sme spomínali, že žiadosť môžu podať aj osoby, ktorým bola pôvodne elektronická schránka zriadená *ex lege*, avšak došlo k jej deaktivácii a zrušeniu. Tieto subjekty môžu požiadať o zriadenie elektronickej schránky v prípade, ak bola elektronická schránka zrušená a zároveň pominuli dôvody deaktivácie elektronickej schránky. Ako príklad môže slúžiť situácia, ak fyzická osoba bola rozhodnutím súdu vyhlásená za mŕtvu. Ide o jeden z dôvodov na deaktiváciu elektronickej schránky; táto schránka je deaktivovaná ku dňu uvedenému v právoplatnom rozhodnutí o vyhlásení za mŕtveho ako deň smrti fyzickej osoby. K zrušeniu elektronickej schránky a vymazaniu jej obsahu dôjde po uplynutí troch rokov odo dňa vyhlásenia jej majiteľa za mŕtveho. V prípade, ak by daný majiteľ predsa len

bol nažive a prihlásil by sa po uplynutí týchto troch rokov, tak pri ňom prichádza do úvahy využitie možnosti podania žiadosti o zriadenie elektronickej schránky.

ÚPPV zverejňuje na ústrednom portáli verejnej správy zoznam adries elektronických schránok orgánov verejnej moci a zároveň sprístupňuje orgánom verejnej moci zoznam adries všetkých elektronických schránok.

Aktivácia elektronickej schránky predstavuje proces, ktorého výsledkom je, že zriadená elektronická schránka sa bude využívať na elektronické doručovanie, pričom toto doručovanie už bude realizované v intenciách E-govZ, a teda už bude mať právne účinky riadneho doručovania. Zdôrazňujeme tú skutočnosť, že aktivácia sa dotýka len toho, či elektronická schránka bude využívaná na doručovanie do nej samotnej. To, že elektronická schránka nie je aktivovaná, neznamená, že ju nemožno použiť na elektronickú komunikáciu s orgánmi verejnej moci. Aj neaktivovanú elektronickú schránku možno využiť na elektronickú komunikáciu (elektronické doručovanie) orgánom verejnej moci; tie v takomto prípade budú mať povinnosť doručiť odpoveď „po starom", t. j. prostredníctvom (napríklad) poštového podniku.

E-govZ rozlišuje spôsoby aktivácie podľa toho, či ide o

a) orgán verejnej moci, právnickú osobu a zapísanú organizačnú zložku alebo

b) inú osobu (napríklad fyzickú osobu, fyzickú osobu podnikateľa).

V prípade subjektov uvedených v písmene a) sa aktivácia začína úkonom ÚPPV vykonaným dňom zriadenia elektronickej schránky a končí sa prvým prístupom oprávnenej osoby do elektronickej schránky, najneskôr však uplynutím desiateho dňa odo dňa vykonania úkonu ÚPPV podľa toho, čo nastane skôr. V prípade subjektov uvedených pod písmenom b) ide o úkon ÚPPV, ktorým na žiadosť majiteľa elektronickej schránky umožní využívanie elektronickej schránky na elektronické doručovanie; žiadosť sa podáva prostredníctvom aktivačnej funkcie elektronickej schránky, a to ku dňu uvedenému v žiadosti, najskôr tretí pracovný deň po doručení žiadosti.

E-govZ v § 13 ods. 4 vymedzuje, kto všetko je oprávnený na prístup do elektronickej schránky.

Vo vzťahu k prístupu do elektronickej schránky platí pravidlo, že do nej má prístup ten, kto je jej majiteľom.[27] Okrem majiteľa schránky môže mať prístup k jeho elektronickej

[27] Inými slovami, ak ide o
a) fyzickú osobu, tak tá fyzická osoba, pre ktorú bola elektronická schránka zriadená,
b) fyzickú osobu podnikateľa, tak tá fyzická osoba podnikateľ, pre ktorú bola elektronická schránka zriadená,

schránke aj ďalšia osoba (ďalšie osoby), a to na základe poverenia majiteľa elektronickej schránky a v ním určenom rozsahu. Udelenie oprávnenia na prístup a disponovanie s elektronickou schránkou a zmena v oprávneniach na prístup a disponovanie s elektronickou schránkou je právny úkon majiteľa elektronickej schránky, ktorým identifikuje osobu oprávnenú na prístup a disponovanie s elektronickou schránkou a určí rozsah jej oprávnení na prístup a disponovanie s elektronickou schránkou. Udelenie oprávnenia na prístup a disponovanie s elektronickou schránkou a zmenu v oprávneniach na prístup a disponovanie s ňou vykoná majiteľ elektronickej schránky, a to elektronickým dokumentom autorizovaným majiteľom, ktorý doručí ÚPPV prostredníctvom na to určenej funkcie elektronickej schránky alebo dokumentom v listinnej podobe s úradne osvedčeným podpisom. Prístup a disponovanie s elektronickou schránkou v rozsahu udeleného oprávnenia zabezpečí ÚPPV bezodkladne, a ak je vykonané dokumentom v listinnej podobe, tak do desiatich pracovných dní odo dňa jeho doručenia.

Na samotný prístup do elektronickej schránky sa pritom vyžaduje identifikátor osoby v spojení s autentifikátorom (alternatívne autentifikačným certifikátom).

Proces preukazovania elektronickej identity sa nazýva identifikácia osoby a proces overovania elektronickej identity sa nazýva autentifikácia osoby.[28]

Zákon vymedzuje, že identifikáciou je deklarovanie identity objektu vrátane osoby, a to najmä pri prístupe k informačnému systému verejnej správy alebo pri elektronickej komunikácii. Identifikátorom osoby, ak ide o

a) fyzickú osobu, je zásadne jej rodné číslo v spojení s menom a priezviskom a ak ide o zahraničnú fyzickú osobu, obdobné číslo alebo identifikátor, ktorý jej je pridelený alebo určený na účely jednoznačnej identifikácie podľa právneho poriadku štátu, ktorého je štátnym občanom, v spojení s menom a priezviskom,
b) orgán verejnej moci, tak identifikačné číslo organizácie,
c) právnickú osobu, fyzickú osobu podnikateľa alebo zapísanú organizačnú zložku, ich identifikačné číslo organizácie, a ak ide o obdobný zahraničný subjekt, obdobné číslo

c) právnickú osobu, tak tá právnická osoba, ktorej bola elektronická schránka zriadená, jej štatutárny orgán alebo člen jej štatutárneho orgánu,
d) orgán verejnej moci, tak ten orgán verejnej moci, pre ktorý bola elektronická schránka zriadená, a vedúci tohto orgánu verejnej moci,
e) zapísanú organizačnú zložku, tak vedúci tejto organizačnej zložky a štatutárny orgán právnickej osoby alebo člen štatutárneho orgánu právnickej osoby, o ktorej zapísanú organizačnú zložku ide,
f) oprávnenú osoba, tak tú, ktorej toto oprávnenie vyplýva zo zákona alebo z rozhodnutia orgánu verejnej moci.

[28] GREGUŠOVÁ, D., HALÁSOVÁ, Z. *Zákon o e-Governmente. Komentár.* Žilina : Eurokódex, 2018, s. 113.

alebo iný identifikátor, ktorý je im pridelený alebo určený na účely jednoznačnej identifikácie podľa právneho poriadku štátu, v ktorom má sídlo alebo miesto podnikania.

Autentifikáciou treba rozumieť preukazovanie identity identifikovaného objektu, spravidla prostredníctvom autentifikátora. Úradným autentifikátorom je

a) občiansky preukaz s elektronickým čipom a bezpečnostný osobný kód[29] alebo

b) doklad o pobyte cudzinca s elektronickým čipom a bezpečnostný osobný kód.[30]

Okrem toho, Ministerstvo vnútra Slovenskej republiky na základe žiadosti vydáva aj alternatívny autentifikátor (o alternatívny autentifikátor môže požiadať iba ten, kto nie je držiteľom ani jedného úradného autentifikátora. O vydanie alternatívneho autentifikátora môže požiadať fyzická osoba, ktorá a) je štatutárnym orgánom právnickej osoby so sídlom na území Slovenskej republiky zapísanej v obchodnom registri [pôjde spravidla o štatutárov, ktorí nie sú občanmi Slovenskej republiky a nemajú povolený pobyt na území Slovenskej republiky alebo o štatutárov, ktorí síce sú občania Slovenskej republiky, ale nemajú pobyt na území Slovenskej republiky] alebo b) je vedúcim jej organizačnej zložky zapísanej v obchodnom registri[31]).

Zatiaľ čo zriadenie, aktivácia a prístup do elektronickej schránky sa týkajú jej využívania, deaktivácia a zrušenie sa týkajú ukončenia jej využívania zo strany majiteľa. Zrušeniu elektronickej schránky predchádza jej deaktivácia.

Deaktivácia elektronickej schránky je úkon, ktorým sa zabezpečí, aby elektronickú schránku nebolo možné ďalej použiť na účely elektronického doručovania. Ak ide o prípady úmrtia majiteľa elektronickej schránky, jeho vyhlásenia za mŕtveho alebo o zánik majiteľa bez právneho nástupcu (prípad sa týka právnických osôb), ÚPPV zabezpečí majiteľovi elektronickej schránky, jeho právnemu nástupcovi, ak o ňom vie, a osobám oprávneným na prístup a disponovanie s elektronickou schránkou prístup k obsahu elektronickej schránky aj po jej deaktivácii, a to po dobu troch rokov, od kedy došlo k spomínanej právnej udalosti. V ostatných prípadoch deaktivácie schránky je zabezpečený prístup do nej bez časového obmedzenia.

[29] Pozri zákon č. 395/2019 Z. z. o občianskych preukazoch a o zmene a doplnení niektorých zákonov.
[30] Pozri § 73 a 73a zákona č. 404/2011 Z. z. o pobyte cudzincov.
[31] GREGUŠOVÁ, D., HALÁSOVÁ, Z. *Zákon o e-Governmente. Komentár.* Žilina : Eurokódex, 2018, s. 120.

K deaktivácii elektronickej schránky môže dôjsť na základe právnej udalosti (majiteľom schránky zásadne neovplyvniteľnej okolnosti) alebo na základe právneho úkonu (žiadosti).

Zo zákona na základe právnej udalosti dochádza k deaktivácii v prípadoch, ako sú smrť fyzickej osoby, deň uvedený v právoplatnom rozhodnutí o vyhlásení za mŕtveho ako deň smrti fyzickej osoby, deň právoplatnosti rozhodnutia o pozbavení spôsobilosti na právne úkony alebo rozhodnutia o obmedzení spôsobilosti na právne úkony, ak toto obmedzenie zahŕňa aj právne úkony spojené s dispozíciou s elektronickou schránkou a doručovanie alebo deň zániku právnickej osoby alebo orgánu verejnej moci bez právneho nástupcu, skončenia výkonu činnosti orgánu verejnej moci, ak ide o fyzickú osobu, alebo výmazu zapísanej organizačnej zložky zo zákonom ustanovenej evidencie (napríklad obchodného registra).

Deaktivovať elektronickú schránku možno aj na základe právneho úkonu majiteľa, ktorým je žiadosť. Majiteľ si v takom prípade môže sám zvoliť dátum, ku ktorému dochádza deaktivácii. Tento deň musí byť najskôr tretím pracovným dňom po doručení žiadosti. Ak by žiadosť bola dourčená neskôr, uplatní sa predpoklad, že týmto dňom je tretí pracovný deň po doručení žiadosti. Túto žiadosť môže podať len fyzická osoba (vrátane podnikateľa) a ten, o kom to ustanoví osobitný predpis; žiadosť o deaktiváciu nemôže podať právnická osoba.[32] Deaktivovať nemožno ani elektronickú schránku orgánu verejnej moci. V týchto dvoch prípadoch je možnosť deaktivácie z logických dôvodov vylúčená.

So súhlasom majiteľa možno deaktivovať elektronickú schránku aj v prípade, ak je vo väzbe alebo výkone trestu odňatia slobody. Žiadosť v tomto prípade podáva ústav na výkon väzby, ústav na výkon trestu odňatia slobody, ústav na výkon trestu odňatia slobody pre mladistvých a nemocnice pre obvinených a odsúdených. Dátum deaktivácie v tomto prípade nastane ku dňu uvedenému v žiadosti.

Deaktivovanú schránku možno na základe žiadosti opätovne aktivovať, a to v každom zo spomínaných prípadov. My sa budeme venovať len postupu, ktorý sa týka opätovnej aktivácie, ak bola elektronická schránka deaktivovaná na základe žiadosti. Zákon

[32] Tu treba povedať, že z § 14 E-govZ to priamo nevyplýva, ale systematickým výkladom zákona treba dospieť k záveru, že žiadosť môže podať právnická osoba, avšak len tá, ktorá sa nezapisuje do obchodného registra, a to najneskôr do 1. júna 2020, kedy dôjde k povinnej aktivácii elektronických schránok aj týchto právnických osôb; porovnaj aj SLOVENSKO.SK. Postup pri deaktivácii elektronickej schránky na doručovanie, s. 2. dostupné na internete: <https://www.slovensko.sk/_img/CMS4/Navody/Nove_ES/navod_deaktivacia_schranky.pdf>, cit. 2019-09-19.

časovo obmedzuje možnosť podania žiadosti o opätovnú aktiváciu elektronickej schránky, ktorú možno podať najskôr

a) po uplynutí šiestich mesiacov odo dňa poslednej deaktivácie,

b) po uplynutí 12 mesiacov odo dňa poslednej deaktivácie, ak bola elektronická schránka deaktivovaná dvakrát za bezprostredne predchádzajúcich 15 mesiacov.

Žiadosť sa podáva prostredníctvom na to určenej funkcie elektronickej schránky alebo v listinnej podobe s úradne osvedčeným podpisom žiadateľa. Ak ide o elektronickú žiadosť, tá je spoplatnená podľa zákona o správnych poplatkoch sumou 5 eur a ak ide o listinnú žiadosť, tak sumou 10 eur.

Ak je elektronická schránka deaktivovaná, elektronické správy, ktoré neboli doručené do okamihu jej deaktivácie, sa vrátia odosielateľovi s informáciou o deaktivácii elektronickej schránky.

Posledným úkonom v procese zániku elektronických schránok, je ich zrušenie, na ktorý je naviazané aj vymazanie obsahu elektronickej schránky.

V prípade, ak dôvodom deaktivácie schránky bola smrť majiteľa, vyhlásene jej majiteľa za mŕtveho alebo o zánik jej majiteľa bez právneho nástupcu, dôjde k zrušeniu a vymazaniu elektronickej schránky po uplynutí troch rokov odo dňa, keď sa o tom ÚPPV dozvedel.

Vo vzťahu k zákonnej formulácii možno mať viacero výhrad. V prvom rade je to k pojmu „dozvedel sa“, čo je subjektívne zistenie danej skutočnosti, ktoré možno len ťažko objektívne postihnúť.[33] Z hľadiska *de lege ferenda* sa domnievam, že by bolo vhodnejšie, aby lehota bola naviazaná na okamih, kedy došlo k daným právnym udalostiam a nie, kedy sa o nich ÚPPV dozvedel. Druhá námietka sa týka využitia pojmu „po uplynutí troch rokov“. Vhodnejším pojmom by bol pojem „deň po uplynutí troch rokov“. Uveďme si príklad, ktorým toto zdôvodním. Ak sa ÚPPV dozvedel o úmrtí majiteľa elektronickej schránky 7.9.2019, trojročná doba uplynie 7.9.2022. Ak by zákon využil pojem „deň po uplynutí“, tak k zrušeniu a výmazu musí dôjsť 8.9.2022, avšak zákon využil pojem „po uplynutí“, čo znamená, že ak dôjde o zrušeniu a výmazu elektronickej schránky aj napríklad 21.12.2050, stále sme v dobe určenej zákonom, lebo aj tento dátum je predsa „po“ uplynutí zákonom určenej doby.

[33] Platí to o to viac, keď príslušné orgány sú podľa § 16 E-govZ povinné tieto právne udalosti bezodkladne nahlasovať UPPV.

V prípade, ak ide o elektronickú schránku organizačnej zložky orgánu verejnej moci alebo organizácie bez právnej subjektivity, ktorú má tento orgán vo svojej zriaďovateľskej pôsobnosti, tak k zrušeniu a vymazaniu obsahu dôjde v lehote uvedenej v žiadosti orgánu verejnej moci o deaktiváciu schránky. V tomto prípade si myslím, že vhodnejším pojmom by bol pojem „k dátumu určenému orgánom verejnej moci", než „v lehote". Z logického hľadiska osoby skôr rozmýšľajú o deaktivácii k určitému dátumu, a nie v lehote (napríklad tri mesiace), ku ktorej sa má niečo udiať.

1.3.2 Elektronické doručovanie a súvisiace právne inštitúty

Orgány verejnej moci sú povinné vykonávať verejnú moc elektronicky. Z toho pravidla existujú niektoré výnimky, kedy elektronická podoba výkonu verejnej moci buď nie je žiadúca, alebo nie je efektívna. Zákon vymedzuje tri takéto situácie. Po prvé sú to situácie, keď priamo osobitný zákon ustanovuje, že úkony orgánu verejnej moci majú listinnú formu. Príkladom takéhoto právneho predpisu je zákon č. 480/2002 Z. z. o azyle (§ 52), zákon č. 404/2011 Z. z. o pobyte cudzincov (§ 120), zákon č. 55/2017 Z. z. o štátnej službe (za predpokladu, že uchádzač si zvolí listinnú formu – § 43 ods. 2). Po druhé, ak ide o úkony ústne, konkludentné alebo ak ide o predloženie veci, ktorá nemá listinnú podobu alebo elektronickú podobu. Po tretie, ak ide o ústne pojednávanie, miestne zisťovanie, výkon kontroly alebo dohľadu priamo u kontrolovaného subjektu alebo dohliadaného subjektu, obhliadka, nazeranie do spisov, predvedenie a iné obdobné úkony, ktoré sa vykonávajú mimo úradnej budovy, v ktorej sídli orgán verejnej moci. V druhom a treťom prípade ide teda o úkony, ktoré nemožno spájať s ich konverziou do elektronickej podoby, keďže najčastejšie pôjde o úkony faktické a bezprostredné, ktoré sa udiali na určitom mieste a v určitý čas. Ich „elektronizácia" preto neprichádza do úvahy, prípadne je z logiky veci priamo vylúčená.

V rámci elektronickej komunikácie do elektronickej schránky treba rozlišovať situácie, keď komunikuje

a) orgán verejnej moci s účastníkom konania,
b) účastník konania s orgánom verejnej moci,
c) orgán verejnej moci s iným orgánom verejnej moci.

Ak ide o prípad uvedený sub a), môže orgán verejnej moci komunikovať elektronicky, t. j. doručovať do elektronickej schránky účastníka konania len v takom prípade, ak má

účastník zriadenú elektronickú schránku a tá je zároveň aj aktivovaná. Ak je elektronická schránka účastníka konania aktivovaná, orgán verejnej moci má povinnosť komunikovať s účastníkom konania výlučne elektronicky.

Účastník konania vo vzťahu k orgánu verejnej moci [prípad sub b)] si môže zvoliť, či bude komunikovať elektronicky alebo listinne. To platí aj v prípade, ak má aktivovanú elektronickú schránku. Zvoliť si nebude môcť len v takom prípade, ak by osobitný právny predpis určil konkrétnu formu komunikácie, či už výlučne elektronicky alebo výlučne listinne. Doručovať orgánu verejnej moci môže účastník konania aj v listinnej podobe, a to aj napriek tomu, že orgány verejnej moci majú aktivované elektronické schránky. Na strane druhej, ako som už uviedol vyššie, ak má účastník elektronickú schránku aj aktivovanú, tak orgán nemá na výber a musí doručovať účastníkovi elektronicky.

Ak ide o komunikáciu medzi orgánmi verejnej moci navzájom, tak tie sú povinné komunikovať do elektronickej schránky len v takom prípade, ak sú vo vzájomnom postavení orgán verejnej moci – účastník konania (t. j. v podstate ide o prípad, ktorý sme popísali sub b)]. Ak nejde o tento prípad, potom orgány verejnej moci môžu komunikovať medzi sebou prostredníctvom modulu procesnej integrácie a integrácie údajov[34] alebo priamou formou elektronickej komunikácie medzi sebou, a to aj automatizovaným spôsobom, bez toho, aby pri elektronickej komunikácii doručovali do elektronickej schránky. Priama forma elektronickej komunikácie prebieha prostredníctvom (napríklad) mailovej komunikácie. Možno konštatovať, že by malo ísť o komunikáciu, ktorá prebieha medzi oficiálnymi mailovými adresami vytvorenými tým-ktorým orgánom verejnej moci, t. j. nesmie ísť o komunikáciu zo súkromných mailových adries ako napríklad z gmail.com, yahoo.com, zoznam.sk a podobne.

Za priamu formu elektronickej komunikácie možno označiť aj takú (za predpokladu, že by orgán verejnej moci mali vytvorenú takú platformu), keď by sa využívali technológie, ktoré umožňujú instantné zasielanie správ ako napríklad umožňuje Skype, ICQ, Messanger, či Yammer.

Vzhľadom na uvedené, treba povedať, že elektronická komunikácia medzi orgánom verejnej moci a fyzickou osobou alebo právnickou osobou (t. j. výkon verejnej moci na účely E-govZ) bude prebiehať najmä prostredníctvom elektronického dourčovania do

[34] Modul procesnej integrácie a integrácie údajov zabezpečuje prostredie pre elektronickú komunikáciu medzi informačnými systémami v správe rôznych orgánov verejnej moci pri výkone verejnej moci elektronicky, pričom, okrem iného, zabezpečuje aj výmenu elektronických správ medzi orgánmi verejnej moci – § 10 ods. 11 E-govZ.

elektronickej schránky. Keďže fyzické osoby alebo právnické osoby nemusia každý deň kontrolovať svoju elektronickú schránku, z operatívnych dôvodov upravuje E-govZ tzv. notifikácie.

Využitie notifikácií však nie je naviazané len na elektronické doručovanie, keďže vo všeobecnosti sa notifikácie môžu posielať o priebehu a stave konania o právach, právom chránených záujmoch a povinnostiach osobám, ktoré sú účastníkom konania alebo ktorých sa vec týka. Notifikácia predstavuje právne nezáväznú informáciu, ktorú zasiela orgán verejnej moci a ktorej obsah ustanovuje zákon.

Z praktického hľadiska využitie notifikácií je vhodné práve pri elektronickom doručovaní do elektronickej schránky pri osobách, ktoré si nekontrolujú elektronickú schránku každý deň. Notifikácia ich upozorní na to, že došlo k uloženiu správy do ich elektronickej schránky. Nastavenie notifikácií nie je automatickým úkonom, ale ak ich chce majiteľ využívať, musí sa na tieto účely zaregistrovať (vo všeobecnosti) alebo si môže zvoliť zasielanie notifikácií v konkrétnej veci. Registrácia v oboch prípadoch je bezodplatná.

V prípade, ak si majiteľ elektronickej schránky zvolí možnosť registrovania na účely zasielania notifikácií, musí si zvoliť spôsob, ktorým bude notifikovaný o úkone, ku ktorému došlo, t. j. v prípade doručovania o doručení elektronickej správy do jeho elektronickej schránky. Môže si pritom zvoliť spôsob zasielania SMS správ na zvolené telefónne číslo alebo napríklad aj zaslanie notifikácie do jeho súkromnej e-mailovej schránky. Výhoda spôsobu zasielania do e-mailovej schránky spočíva v tom, že je vždy bezodplatná, zatiaľ čo ostatné spôsoby, ak sú spojené s nákladmi pre orgán verejnej moci, môžu byť spoplatnené. O spoplatnení však musí byť adresát vopred informovaný.

Ak si adresát zvolil možnosť zasielania notifikácií, bezodkladne po uložení elektronickej úradnej správy je mu zaslaná notifikácia o uložení elektronickej úradnej správy, ktorá obsahuje meno a priezvisko alebo obchodné meno alebo názov odosielateľa a adresáta a deň uplynutia úložnej lehoty.

Povinnosť elektronického doručovania sa týka elektronického podania aj elektronického úradného dokumentu. Ako sme už spomínali, rozdiel medzi nimi, okrem iného, spočíva v tom, kto je ich „autorom“. V prípade elektronického podania ide o účastníka konania a v prípade elektronického úradného dokumentu ide o orgán verejnej moci. Oba tieto dokumenty sa doručujú elektronickými prostriedkami, a to do elektronickej schránky adresáta za podmienky, že je aktivovaná. Spôsob doručovania sa realizuje podľa ustanovení

E-govZ, pokiaľ osobitný predpis neustanoví osobitné pravidlá (pravidlo *lex specialis derogat lex generalis*).

Doručovanie podľa E-govZ predstavuje všeobecnú právnu úpravu, ktorá sa uplatní všade tam, kde osobitný právny predpis neurčí inak. Čo však bude platiť zásadne vždy, je, že elektronické dourčovanie sa realizuje do elektronickej schránky. Z tohto pravidla tiež môže existovať výnimka, kedy bude možné doručovať napríklad aj do súkromnej mailovej schránky – v súčasnosti túto výnimku zakotvuje zákon č. 211/2000. Z. z. o slobodnom prístupe k informáciám (zákon o slobode informácií). Vyplýva to z § 14 ods. 1 tohto zákona, podľa ktorého žiadosť možno podať písomne, ústne, faxom, elektronickou poštou alebo iným technicky vykonateľným spôsobom, ako aj z § 16 ods. 1, podľa ktorého sa informácie sprístupňujú najmä ústne, nahliadnutím do spisu vrátane možnosti vyhotoviť si odpis alebo výpis, odkopírovaním informácií na technický nosič dát, sprístupnením kópií predlôh s požadovanými informáciami, telefonicky, faxom, poštou, elektronickou poštou. V oboch týchto ustanoveniach sa využíva pojem elektronická pošta, čím sa myslia práve bežné mailové adresy.

Príkladom ďalšej výnimky môžu byť ustanovenia osobitných predpisov, ktoré upravujú pravidlá, ako má postupovať príslušný orgán v prípade, ak mu je zaslané podanie do inej, než elektronickej schránky. Napríklad podľa zákona č. 71/1967 Zb. o správnom konaní (správny poriadok) podanie vo veci samej urobené v elektronickej podobe bez autorizácie podľa osobitného predpisu o elektronickej podobe výkonu verejnej moci treba do troch pracovných dní doplniť v listinnej podobe, v elektronickej podobe autorizované podľa osobitného predpisu o elektronickej podobe výkonu verejnej moci, alebo ústne do zápisnice. Obdobné pravidlo obsahuje aj zákon č. 160/2015 Z. z. Civilný sporový poriadok.

Aj sám E-govZ ustanovuje, kedy sa nebude doručovať elektronicky, ale listinným spôsobom:

a) ak osobitný predpis priamo ustanovuje, že sa doručuje výlučne v listinnej forme,

b) ak sa doručuje osobám vo výkone trestu odňatia slobody, vo väzbe, osobám umiestneným v zariadeniach pre výkon ústavnej starostlivosti a ochrannej výchovy alebo tomu, kto požíva diplomatické výsady a imunity, ak orgán verejnej moci vie, že doručuje takej osobe.

Hoci to E-govZ neustanovuje, elektronicky sa nebude doručovať ani vtedy, ak aplikáciu tohto zákona vylúči osobitný právny predpis. Ako príklad môže slúžiť § 66a zákona

č. 301/2005 Z. z. Trestný poriadok, podľa ktorého na doručovanie elektronickými prostriedkami podľa tohto zákona sa nevzťahuje osobitný predpis o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci.

Spôsoby elektronického doručovania, ktoré upravuje E-govZ, sú dva, a to elektronické doručovanie do vlastných rúk a iné (bežné) elektronické doručovanie.

Zákon ustanovuje, že doručením do vlastných rúk sa na účely elektronického doručovania rozumie doručenie, pri ktorom sa vyžaduje potvrdenie doručenia zo strany adresáta alebo osoby, ktorej je podľa osobitných predpisov možné doručovať namiesto adresáta[35] (ďalej len „prijímateľ"), formou elektronickej doručenky odoslanej odosielateľovi. Do vlastných rúk sa elektronicky doručujú elektronické dokumenty, ktoré sú z hľadiska právnych účinkov totožné s dokumentom v listinnej podobe, o ktorom osobitné predpisy ustanovujú, že sa doručujú do vlastných rúk. Napríklad Správny poriadok v § 24 ods. 1 ustanovuje, že dôležité písomnosti, najmä rozhodnutia, výzvy a predvolania, sa doručujú do vlastných rúk.

Doručenie do vlastných rúk podľa E-govZ sa vyznačuje tým, že musí byť potvrdené ako doručené zo strany prijímateľa vo forme elektronickej doručenky. Elektronická doručenka sa vytvára aj v prípade bežného doručovania, avšak v takomto prípade sa vytvára automaticky; nevyžaduje sa jej potvrdenie zo strany prijímateľa. Samotná elektronická doručenka sa vyznačuje tým, že obsahuje:

a) údaj o dni, hodine, minúte a sekunde elektronického doručenia,
b) identifikátor osoby prijímateľa,
c) identifikátor osoby odosielateľa a
d) identifikáciu elektronickej úradnej správy a elektronických dokumentov, ktoré sa elektronicky doručujú.

V prípade, ak bola elektronická doručenka potvrdená, považujú sa údaje na nej uvedené za pravdivé, a to až do okamihu, kým nie je preukázaný opak. Zákon tu vytvára tzv. predpoklad pravdivosti elektronickej doručenky, avšak pripúšťa o ňom dôkaz o opaku. Tento dôkaz bude musieť predložiť ten, kto tvrdí, že údaje na elektronickej doručenke nie sú pravdivé.

[35] Na základe plnomocenstva si možno zvoliť zástupcu pre to-ktoré konanie, v ktorom sa bude adresátovi doručovať. Zvyčajným príkladom je plnomocenstvo udelené advokátovi.

Ak ide o doručovanie orgánu verejnej moci, doručenie sa potvrdzuje prostredníctvom funkcie elektronickej podateľne. Ak ide o doručovanie inej osobe, elektronická doručenka sa vytvára automatizovaným spôsobom prostredníctvom modulu elektronického doručovania. ÚPPV je povinný zabezpečiť, aby modul elektronických schránok bol vytvorený tak, aby prijímateľ pri preberaní doručovaného elektronického dokumentu bol vždy povinný potvrdiť doručenie elektronického úradného dokumentu, a to ešte pred sprístupnením obsahu tohto dokumentu.

Elektronická doručenka sa vytvára aj v prípade, ak elektronická schránka nebola aktivovaná.[36] Naopak, elektronická doručenka sa nevytvára vtedy, ak jej odosielateľ nie je známy alebo ak nemá zriadenú elektronickú schránku.

Novinkou, ktorú zavádza E-govZ, je tzv. centrálne úradné doručovanie. To je upravené v § 31a. Centrálne úradné doručovanie sa týka všetkých orgánov verejnej moci, ktoré sú štátnou rozpočtovou organizáciou,[37] pričom ho zabezpečuje správca modulu elektronického doručovania. Na základe dohody so správcom modulu elektronického doručovania sa centrálne úradné doručovanie vzťahuje aj na orgány verejnej moci, ktoré nie sú štátnou rozpočtovou organizáciou. Správcom modulu elektronického doručovania je Národná agentúra pre sieťové a elektronické služby (ďalej aj ako „NASES").

V čom spočíva centrálne úradné doručovanie? E-govZ vychádza zo základnej premisy, že orgány verejnej moci vykonávajú verejnú moc už len v elektronickej podobe a nie v listinnej. To sa týka aj doručovania ako takého. Z daného dôvodu sa preto doručovanie zo strany orgánov verejnej moci uskutočňuje už len v elektronickej podobe.

Orgán verejnej moci odošle elektronický úradný dokument prostredníctvom modulu elektronického doručovania správcovi modulu elektronického doručovania (NASES), ktorý prostredníctvom modulu elektronického doručovania bezodkladne zabezpečí jeho doručenie do elektronickej schránky adresáta. V prípade, ak elektronická schránka je aktivovaná, došlo k riadnemu doručeniu elektronického úradného dokumentu.

Centrálne úradné doručovanie sa však uplatňuje aj v prípade, ak elektronická schránka nie je aktivovaná. V takom prípade NASES zabezpečí jeho doručenie adresátovi v listinnej podobe prostredníctvom poštového podniku, a to spôsobom podľa osobitného predpisu upravujúceho konanie v danej veci (t. j. „bežné" doručenie alebo doručenie do

[36] K dôvodu pozri ďalej v texte o centrálnom úradnom doručovaní.
[37] Zjednodušene povedané, štátnou rozpočtovou organizáciou sú všetky štátne orgány; pozri aj § 21 ods. 1 zákona č. 523/2004 Z. z. o rozpočtových pravidlách verejnej správy.

vlastných rúk). Práve v tomto možno vidieť dôvod, prečo sa vytvára elektronická doručenka aj v prípade elektronických schránok, ktoré nie sú aktivované. Je to preto, aby orgán verejnej moci, ktorý doručuje elektronický úradný dokument, mal o tejto skutočnosti vedomosť, a aby mal vedomosť o tom, že sa bude doručovať v listinnej podobe.

Doručovanie v listinnej podobe však nebude zabezpečovať orgán verejnej moci, ale opäť ho bude realizovať NASES, a to tak, že vytvorí listinný rovnopis elektronického úradného dokumentu. Listinný rovnopis elektronického úradného dokumentu je vyhotovenie elektronického úradného dokumentu, vrátane jeho príloh, v listinnej podobe vrátane identifikácie toho, kto elektronický úradný dokument autorizoval a informácie o spôsobe autorizácie a čase autorizácie. Má rovnaké právne účinky ako elektronický úradný dokument, z ktorého bol vyhotovený. Doručenie listinného rovnopisu elektronického úradného dokumentu má rovnaké právne účinky ako doručenie elektronického úradného dokumentu.

Dôvod, kvôli ktorému sa doručuje týmto spôsobom, vyplýva z dôvodovej správy k zákonu č. 238/2017 Z. z., ktorý novelizoval E-govZ tak, že do jeho ustanovení zakotvil centrálne úradné doručovanie. Podľa dôvodovej správy, v súvislosti s listinným doručovaním úradných zásielok je potrebné na strane orgánov verejnej moci zabezpečovať vytvorenie zásielok a ich podanie na poštovú prepravu. Štát to stojí nemalé finančné prostriedky a pre orgány to zase predstavuje administratívnu záťaž. Orgány verejnej moci si tieto procesy zabezpečujú individuálne a nejednotne, pričom vytváranie a podávanie úradných zásielok si zabezpečujú buď vo vlastnej réžii, alebo prostredníctvom externých služieb. Zabezpečovanie procesov vo vlastnej réžii je pritom závislé od úrovne technického vybavenia a od príslušných nákladov na papier, tonery, obálky, od odpisov technických zariadení, od spotreby energie, ako aj od osobných nákladov administratívnych pracovníkov zabezpečujúcich vytvorenie a podanie zásielok. Výsledkom sú nejednotné formáty, rôzne procesy doručovania, individuálne obstarávanie materiálov a služieb a tým aj rôzna výška nákladov na jednotlivú listinnú zásielku. Orgány verejnej moci majú povinnosť vykonávať verejnú moc elektronicky a úradné dokumenty doručovať elektronicky do aktivovaných elektronických schránok. Pre adresátov, ktorí nemajú aktivované elektronické schránky, sa doručujú úradné rozhodnutia naďalej v listinnej podobe, vo forme rovnopisu. Aj napriek povinnej aktivácii elektronických schránok pre právnické osoby zapísané v obchodnom registri sa stav v doručovaní úradných zásielok zásadne nemení. Veľká časť elektronických

schránok môže byť stále neaktivovaných (fyzické osoby) a orgány verejnej moci musia doručovať úradné zásielky naďalej v listinnej podobe. To kladie na doručovanie ešte väčšie nároky, keďže musia pred odoslaním úradnej zásielky preveriť, či je elektronická schránka aktivovaná alebo nie a podľa toho zvoliť formu aj spôsob doručovania. Pri elektronickom doručovaní je administratívna a finančná náročnosť tiež závislá od technického vybavenia príslušných orgánov. Niektoré inštitúcie už majú automatizované riešenia pre overovanie aktívnych elektronických schránok, ako aj riešenia na hromadné odosielanie elektronických podaní. Sú však aj inštitúcie s nízkou mierou automatizácie čo zvyšuje ich administratívnu náročnosť doručovania. Navrhované riešenie vychádza z predpokladu, že orgány verejnej moci vytvárajú úradné dokumenty už len v elektronickej podobe a doručujú ich s použitím modulu elektronického doručovania. Tento modul teda môže prijať elektronické úradné dokumenty a automatizovaným spôsobom vyhodnotiť, či príslušný adresát má alebo nemá aktivovanú elektronickú schránku. Na základe výsledku vyhodnotenia systém buď doručí úradné dokumenty do aktivovanej elektronickej schránky, alebo zvolí listinné doručovanie. Následne prevádzkovateľ integrovaného obslužného miesta vytvorí rovnopisy a vyhotoví listinné úradné zásielky, ktorých doručenie bude zabezpečené prostredníctvom poštového podniku. Riešenie bude automatizovaným spôsobom poskytovať informácie o výsledkoch doručenia príslušným orgánom. Z pohľadu adresáta bude úradný dokument doručený buď do aktivovanej elektronickej schránky, alebo vo forme listinnej zásielky. Na strane orgánu verejnej moci už nebude potrebné skúmať, či adresát má alebo nemá aktivovanú elektronickú schránku a vytvárať listinné zásielky, čím odpadá celý rad administratívnych úkonov, ako aj nákladov na tlačenie, pečiatkovanie a podpisovanie, obálkovanie a podanie zásielok na poštovú prepravu.[38]

Ak ide o doručovanie listinného rovnopisu elektronického úradného dokumentu, platí, že orgán verejnej moci si odoslaním elektronického úradného dokumentu vyhradil, že poštová zásielka, ktorej obsahom je listinný rovnopis tohto dokumentu, nemá byť vrátená; poštový podnik takú poštovú zásielku, ak ju nemožno dodať adresátovi, zničí do 30 dní odo dňa doručenia informácie o výsledku doručenia. Na účely doručenia podľa osobitných

[38] NÁRODNÁ RADA SLOVENSKEJ REPUBLIKY. Vládny návrh zákona, ktorým sa mení a dopĺňa zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony, s. 35-36. Dostupné na internete: <https://www.nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=439315>, cit. 2019-09-20.

predpisov sa za deň vrátenia poštovej zásielky odosielateľovi považuje deň doručenia informácie o výsledku doručovania.

Náklady spojené s vytváraním listinného rovnopisu elektronického úradného dokumentu a zabezpečenie jeho doručovania, sú nákladmi NASES-u.

Ak ide o doručovanie orgánu verejnej moci, ktorý nie je štátnou príspevkovou organizáciou, ktorá si nedohodla doručovanie s NASES-om, musí listinné doručenie zabezpečiť sám tento orgán a na vlastné náklady.

Z právneho hľadiska je veľmi dôležitou úprava uloženia elektronickej úradnej správy (zásielky), pretože na ňu je naviazaná objektívna možnosť oboznámenia sa adresáta s jej obsahom. To rešpektuje aj E-govZ, ktorý týmto spôsobom vymedzuje tento pojem.

Počas plynutia úložnej lehoty sa zásielka stále považuje za nedoručenú; nachádza sa zatiaľ len v dispozičnej sfére adresáta, ktorý sa s ňou má možnosť riadne oboznámiť, aj keď k skutočnému oboznámeniu sa ešte nedošlo. E-govZ ustanovil úložnú lehotu na 15 kalendárnych dní, pričom táto lehota začína plynúť v deň nasledujúci po dni uloženia elektronickej úradnej správy. Osobitný právny predpis môže ustanoviť aj inú lehotu (či už kratšiu alebo aj dlhšiu).

Ak sa elektronicky doručuje do vlastných rúk, adresát je povinný potvrdiť doručenie elektronickej úradnej správy formou elektronickej doručenky; potvrdenie doručenia je podmienkou sprístupnenia obsahu elektronickej úradnej správy prijímateľovi v jeho elektronickej schránke. Elektronická úradná správa sa sprístupní v momente potvrdenia doručenia.

Zákon presne vymedzuje, kedy možno elektronickú úradnú správu považovať za doručenú, pričom rozlišuje, či sa doručuje orgánu verejnej moci, súkromnej osobe do vlastných rúk alebo súkromnej osobe bežným doručením. Ak je adresátom orgán verejnej moci, považuje sa správa za doručenú uložením elektronickej úradnej správy. Ak sa doručuje súkromnej osobe a do vlastných rúk, považuje sa správa za doručenú dňom, hodinou, minútou a sekundou uvedenými na elektronickej doručenke alebo márnym uplynutím úložnej lehoty podľa toho, ktorá skutočnosť nastane skôr, a to aj vtedy, ak sa adresát o tom nedozvedel (tzv. fikcia doručenia[39]). Ak nie je adresátom orgán verejnej moci a nedoručuje

[39] Fikcia doručenia predstavuje situáciu, kedy zákon za splnenia určitých predpokladov, považuje určitý fakt, ktorý nastal, za právne relevantný a spôsobilý právnych následkov, hoci v reálnom svete nastať nemusel. Inými slovami finguje sa tu určitá skutočnosť. Pri fikcii doručenia sa finguje to, že zásielka bola adresátovi doručená a že sa s ňou mal možnosť oboznámiť.

sa do vlastných rúk, považuje sa správa za doručenú deň bezprostredne nasledujúci po uložení elektronickej úradnej správy.

Po doručení elektronickej úradnej správy zostáva elektronická úradná správa, vrátane všetkých elektronických dokumentov, ktoré obsahuje, uložená v elektronickej schránke adresáta.

Zákon osobitne upravuje počítanie lehôt, ktoré sú spojené s plnením povinností (napríklad povinnosť niečo predložiť alebo niekam sa dostaviť). Tu treba osobitne upozorniť, že oproti zaužívanému postupu (pri listinnom doručovaní), kedy táto lehota na plnenie začína plynúť najbližší nasledovný kalendárny deň, je v prípade elektronického doručovania istý rozdiel.

V prípade elektronického doručovania, ak k elektronickému doručeniu dôjde v deň štátneho sviatku alebo v deň pracovného pokoja, lehota na konanie alebo na vykonanie úkonu, ktorej začiatok je spojený s okamihom elektronického doručenia, začne plynúť najbližší nasledujúci pracovný deň; to neplatí, ak osobitný predpis ustanovuje alebo z povahy konania alebo úkonu vyplýva, že orgán verejnej moci alebo iná osoba sú povinní konať aj v deň, ktorý je štátnym sviatkom, alebo v deň pracovného pokoja.

Pracovné dni a štátne sviatky sú vymedzené v zákone č. 241/1993 Z. z. o štátnych sviatkoch, dňoch pracovného pokoja a pamätných dňoch. Podľa tohto zákona sa za deň štátneho pokoja považujú štátne sviatky,[40] iné sviatky[41] a nedele. Možno si povšimnúť, že sobota sa nepovažuje za deň pracovného pokoja; zrejmou chybou zákonodarcu tu došlo k opomenutiu tejto skutočnosti, a preto z dôvodu právnej istoty by bolo vhodné, aby *de lege ferenda* bola do § 32 ods. 9 E-govZ doplnená aj sobota. Za súčasného stavu sa preto, podľa môjho názoru, do tejto lehoty musí započítavať aj sobota.

Zákon potom osobitne upravuje situácie ako postupovať v prípade, ak medzi okamihom odoslania elektronickej úradnej správy a okamihom márneho uplynutia úložnej lehoty bola elektronická schránka deaktivovaná, alebo ak orgán verejnej moci rozhodne, že elektronické doručenie je neúčinné.[42]

---

[40] 1. január, 5. júl, 29. august, 1. september a 17. november.

[41] 6. január, Veľký piatok, Veľkonočný pondelok, 1. máj, 8. máj, 15. september, 1. november, 24. december, 25. december a 26. december.

[42] Rozhodovanie o neúčinnosti elektronického doručovania je akousi obdobou rozhodovania o náhradnom doručení. Rozhodnúť o neúčinnosti doručenia možno vtedy, ak adresát objektívne nemohol prevziať elektronickú úradnú správu z dôvodu, ktorý nenastal na jeho strane alebo jeho pričinením, alebo ak na jeho strane nastali také dôvody, ktoré mu objektívne neznemožnili prevziať elektronickú úradnú správu, avšak takéto prevzatie by bolo spojené s nepomernými ťažkosťami, ktorých prekonanie od neho nie je spravodlivé požadovať. Právnym dôsledkom rozhodnutia o neúčinnosti

Záverečným právnym inštitútom, ktorý súvisí s elektronickým doručovaním, ktorý je upravený E-govZ a ktorému sa budeme venovať, je elektronická úradná tabuľa.[43]

Doručovať prostredníctvom elektronickej úradnej tabule sa bude vtedy, ak to ustanoví osobitný právny predpis. Ak osobitný právny ustanovuje, že sa doručuje prostredníctvom úradnej tabule, verejnou vyhláškou, na webovom sídle alebo iným obdobným spôsobom, zverejní sa úradný dokument aj v elektronickej podobe, a to na elektronickej úradnej tabuli orgánu verejnej moci. Podstatou vyvesenia dokumentu na elektronickej úradnej tabuli je, že sa s daným dokumentom môže oboznámiť neurčitý okruh osôb.

Ako príklady zverejňovania dokumentov na úradnej tabuli, verejnej vyhláške, webovom sídle alebo iným obdobným spôsobom môžu slúžiť: doručenie verejnou vyhláškou, ak účastníci konania alebo ich pobyt nie sú známi, alebo pokiaľ to ustanovuje osobitný zákon podľa Správneho poriadku; zverejniť oznámenia o dražbe alebo oznámenie o opakovanej dražbe na úradnej tabuli obce alebo na elektronickej úradnej tabuli obce, ak je predmetom dražby byt, dom, iná nehnuteľnosť, podnik alebo jeho časť podľa zákona č. 527/2002 Z. z. o dobrovoľných dražbách; zverejnenie návrhu územného plánu zóny na úradnej tabuli obce podľa Stavebného zákona; zverejnenie návrhu nariadenia obce na webovom sídle obce podľa zákona o obecnom zriadení.

Orgán verejnej moci vykoná zverejnenie na elektronickej úradnej tabuli v rovnaký deň, ako zverejní elektronický dokument na úradnej tabuli, verejnou vyhláškou, na webovom sídle alebo iným obdobným spôsobom zverejnenia pre neurčitý okruh osôb, a ak to z objektívnych dôvodov nie je možné, zverejní na elektronickej úradnej tabuli súčasne so zverejneným elektronickým dokumentom aj informáciu o tom, kedy bol zverejnený na úradnej tabuli, verejnou vyhláškou, na webovom sídle alebo iným obdobným spôsobom zverejnenia pre neurčitý okruh osôb.

Dokument sa považuje za doručený v okamihu, keď sú splnené podmienky doručenia podľa osobitného právneho predpisu, ktorý upravuje zverejnenie dokumentu na úradnej tabuli, verejnou vyhláškou, na webovom sídle alebo iným obdobným spôsobom. Ako príklad môže slúžiť právna úprava Správneho poriadku. Podľa § 26 ods. 2 tohto predpisu

doručenia je, že elektronická úradná správa vrátane všetkých elektronických dokumentov sa považuje za doručenú dňom, keď rozhodnutie o neúčinnosti elektronického doručenia nadobudlo právoplatnosť.

[43] Podľa E-govZ elektronická úradná tabuľa je elektronické úložisko, na ktoré sú zasielané a na ktorom sú zverejňované elektronické dokumenty, ak tak ustanovuje zákon.

doručenie verejnou vyhláškou sa vykoná tak, že sa písomnosť vyvesí po dobu 15 dní na úradnej tabuli správneho orgánu. Posledný deň tejto lehoty je dňom doručenia. Správny orgán zverejňuje písomnosť súčasne na svojom webovom sídle, ak ho má zriadené a ak je to vhodné aj iným spôsobom v mieste obvyklým, najmä v miestnej tlači, rozhlase alebo na dočasnej úradnej tabuli správneho orgánu na mieste, ktorého sa konanie týka.

Z uvedeného ustanovenia vyplýva, že lehota 15 dní začne plynúť až vtedy, ak sú splnené dve podmienky, a to 1) vyvesenie písomnosti na úradnej tabuli a 2) zverejnením na webovom sídle. Ak dôjde k vyveseniu a zverejneniu v rovnaký deň, potom lehota začne plynúť deň nasledujúci po vyvesení/zverejnení a za deň doručenia sa považuje posledný 15. deň tejto lehoty. Ak však vyvesenie a zverejnenie prebehne v iné dni, potom lehota začne plynúť až deň nasledujúci potom, ako sú splnené oba spôsoby, a teda ak k vyveseniu dôjde v pondelok a k zverejneniu v stredu, potom lehota začne plynúť až deň nasledujúci po strede (štvrtok), lebo až v stredu boli kumulatívne splnené podmienky na zverejnenie písomností na úradnej tabuli.

ZOZNAM POUŽITEJ LITERATÚRY

Literatúra

1) GREGUŠOVÁ, D., HALÁSOVÁ, Z. Zákon o e-Governmente. Komentár. Žilina : Eurokódex, 2018.
2) KOŠIČIAROVÁ, S. Správne právo hmotné. Všeobecná časť. Plzeň : Aleš Čeněk, 2015.
3) ŠKROBÁK, J. In VRABKO, M. a kol. Správne právo hmotné. Všeobecná časť. Bratislava : C. H. Beck, 2012.
4) ŠKULTÉTY, P. In ŠKULTÉTY, P. a kol. Správne právo hmotné. Všeobecná časť. Bratislava : VO PraF UK, 2005.
5) TÓTHOVÁ, K. Sú správne orgány samostatným druhom orgánov verejnej správy? In MASLEN, M. (ed.) Správne súdnictvo a jeho rozvojové aspekty. Bratislava : Ikarus.sk – Eurounion, 2011.

Časopisy a periodiká

6) SREBALOVÁ, M. Vývoj terminológie verejnej správy (s osobitným zreteľom na pojem správny orgán) v súčasnosti. In Správní právo, roč. 39, č. 4/2006, s. 252.

7) ŠKROBÁK, J. Kategória verejnej moci a jej význam vo verejnej správe a vo vede správneho práva. In Míľniky práva v stredoeurópskom priestore 2008. Bratislava : VO PraF UK, 2008, s. 655.
8) ŠKROBÁK, J. Kategória verejnej moci a jej význam vo verejnej správe a vo vede správneho práva. In Míľniky práva v stredoeurópskom priestore 2008. Bratislava : VO PraF UK, 2008, s. 652-653.
9) TÓTHOVÁ, K. Niekoľko úvah k pojmom správny orgán, orgán štátnej správy a orgán verejnej správy. In Pocta profesorovi Slovinskému. Bratislava : Univerzita Komenského v Bratislave, Právnická fakulta, 2009, s. 104.

Judikatúra

10) Uznesenie Ústavného súdu ČSFR sp. zn. I. ÚS 191/92 z 9. júna 1992.

Elektronické zdroje

11) <https://www.nases.gov.sk/ustredne-kontaktne-centrum-za-pat-rokov-pomohlo-vyse-200-tisic-ludom/>, cit. 2019-09-16.
12) NÁRODNÁ AGENTÚRA PRE SIEŤOVÉ A ELEKTRONICKÉ SLUŽBY. Výročná správa za rok 2018, s. 22. Dostupné na internete <https://www.nases.gov.sk/wp-content/uploads/2019/05/NASES_Vyrocna_sprava_2018.pdf >, cit. 2019-09-19.
13) NÁRODNÁ RADA SLOVENSKEJ REPUBLIKY. Vládny návrh zákona, ktorým sa mení a dopĺňa zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony, s. 35-36. Dostupné na internete: <https://www.nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=439315>, cit. 2019-09-20.

KAPITOLA 2 OCHRANA OSOBNÝCH ÚDAJOV

2.1 Úvodné poznámky

Ochrana osobných údajov predstavuje jednu z najdiskutovanejších problematík v súčasnosti a zároveň reflektuje určitý paradox. Vo svete, kde sa takmer všetky sociálne vzťahy a väzby presúvajú do online priestoru, je poskytovanie osobných údajov každodennou súčasťou ľudského života. Či už ide o registráciu na sociálnych sieťach ako Facebook alebo Twitter, využívanie rôznych služieb zdieľania obsahu ako Youtube alebo Spotify, či využívanie elektronických služieb verejnej správy,[44] používanie týchto služieb vyžaduje od užívateľov spracúvanie osobných údajov. Zároveň však badať tendencie, že ochrana osobných údajov sa stáva predmetom čoraz obsiahlejšej regulácie a zároveň katalyzátorom politických či akademických diskusií. Leitmotívom je táto téma aj vďaka početným únikom dát etablovaných miliardových spoločností z globálneho IT prostredia.[45]

Z vyššie uvedených dôvodov sme považovali za nevyhnutné do našej učebnice vložiť aj samostatnú kapitolu týkajúcu sa ochrany osobných údajov. Vzhľadom na to, že predkladané dielo predstavuje iba „vybrané kapitoly z práva informačných technológií," nie je na mieste obsiahnuť v rámci tejto časti predmetnú problematiku komplexne. Preto sa v tejto kapitole sústredíme iba na predstavenie základných postulátov a axióm právnej úpravy týkajúcej sa ochrany osobných údajov a stručnú charakteristiku platnej právnej úpravy v rámci Európskej únie.

Túto časť učebnice začíname analýzou vývoja odporúčaní a právnych aktov, ktoré sa týkali ochrany osobných údajov. Následne pozornosť zameriame na ľudsko-právnu úpravu práva na ochranu osobných údajov v rámci medzinárodných dokumentov a Ústavy Slovenskej republiky. Ochrana osobných údajov stojí a padá na implementácií tzv. princípov ochrany osobných údajov. Tieto sú zároveň reflektované v takmer každom právnom predpise, ktorý upravuje spracúvanie osobných údajov. Z tohto dôvodu je predmetom tretej kapitoly práve rozbor predmetných princípov, nakoľko ich pochopenie povedie

[44] LIGASOVÁ, Z. - RALBOVSKÁ – SOPÚCHOVÁ, S. : Je e-Government dostupný pre všetkých občanov? In MMK 2018: recenzovaný sborník příspěvků. - : 1. vyd. Hradec Králové : Magnanimitas akademické sdružení, 2018. - S. 306-314 alebo ANDRAŠKO, J. : Elektronický občiansky preukaz a iné spôsoby autentifikácie pri prístupe k elektronickým službám verejnej správy. In QUAERE 2017, roč. 7. Hradec Králové : Magnanimitas, 2017, s. 235-244.

[45] Napr. kauza Cambridge Analytica, https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook (dostupné 25.10.2019).

k poznaniu základných pilierov ochrany osobných údajov v prakticky každom právnom akte regulujúcom túto oblasť.

Posledná kapitola sa venuje implementácií týchto princípov a relevantnej legislatíve na európskom kontinente. Osobitne je pozornosť zameraná na Dohovor Rady Európy č. 108 o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov a nariadenie Európskeho parlamentu a Rady (EÚ) 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 alebo GDPR).

2.2 Stručný vývoj právnej ochrany osobných údajov

Právna ochrana osobných údajov sa nekreovala v roku 2016 prijatím mediálne známeho GDPR. Postuláty, na ktorých ochrana osobných údajov stojí a padá boli dávno predmetom záväzných či nezáväzných právnych aktov v národnom a medzinárodnom meradle.

Ak hovoríme o ochrane osobných údajov, prvý právny akt v podobe zákona týkajúci sa danej oblasti bol prijatý v roku 1970 v nemeckej spolkovej republike Hesensko známy pod názvom *Hessische Datenschutzgesetz*.[46] Tento zákon upravoval spracúvanie osobných údajov v rámci vládnych automatizovaných informačných registrov a aplikoval sa výlučne na verejný sektor. Zároveň slúžil ako inšpirácia pre ďalšie právne úpravy primárne na nemeckej pôde aj na úrovni federácie.

Niektorí autori[47] však argumentujú, že Hesenský zákon o ochrane osobných údajov nespĺňa parametre komplexnej právnej úpravy tejto oblasti, keďže neupravuje základné zásady resp. princípy spracúvania osobných údajov. Tie sa prvýkrát objavujú až v roku 1973 vo švédskom zákone o ochrane osobných údajov (*Datalog*).[48] Týmto zákonom bol zároveň založený aj švédsky dozorný orgán, ktorý mal dohliadať na spracúvanie osobných údajov. Švédsky zákon sa aplikoval na súkromný a aj verejný sektor a prvýkrát sa v ňom objavujú zásady spracúvania.

[46] Datenschutzgesetz (GVBl. II 300-10) vom 7. Oktober 1970. In: Gesetz- und Verordnungsblatt für das Land Hessen. 1970 Nr. 41, S. 625, online http://starweb.hessen.de/cache/GVBL/1970/00041.pdf#page=1 (dostupné 29.10.2019).
[47] GREENLEAF, G. : Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories. *In Journal of Law, Information & Science. Special issue from the Asian Privacy Scholars Network Conference*. December 2012.
[48] Datalog given in the Palace of Stockholm, May 11, 1973, SFS 1973:289.

Na tieto právne akty následne nadviazali národné právne úpravy vo Francúzsku a Nemecku. Onedlho na to sa spracúvaním osobných údajov a reguláciou tejto oblasti začali zaoberať aj medzinárodné organizácie.

Organizácia pre hospodársku spoluprácu a rozvoj (OECD) po dlhoročnej expertnej činnosti a diskusií v rámci interných odborných panelov vydala usmernenie ku ochrane súkromia a cezhraničnom prenose osobných údajov (*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data).*[49] Tento nezáväzný právny akt okrem iného vymenúva a opisuje medzinárodne akceptované princípy spracúvania osobných údajov. Predmetnému usmerneniu sa budeme venovať v nasledujúcich statiach tejto kapitoly.

Rada Európy sa taktiež nenechala dlho zahanbiť a kreovala prvý medzinárodný záväzný právny akt týkajúci sa oblasti ochrany osobných údajov - Dohovor Rady Európy č. 108 o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (Dohovor 108) prijatý v roku 1980. V roku 2018 bol revidovaný na modernejšiu verziu reflektujúcu vývoj nových technológií.[50] Ustanovenia Dohovoru 108 budú taktiež analyzované v nasledujúcich častiach učebnice.

Na úrovni Európskej únie bola v oblasti ochrany osobných údajov v roku 1995 prijatá smernica Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov[51] s cieľom zabezpečiť voľný pohyb osobných údajov v rámci Európskej únie a chrániť jednotlivca pred negatívnymi vplyvmi a dopadmi spracúvania osobných údajov. Tento právny rámec však o dve desaťročia nevyhnutne potreboval revíziu, nakoľko táto smernica bola prijatá ešte v čase, keď internet používalo iba mizivé percento populácie. Túto medzeru sa aktívne snažil zalepiť Súdny dvor Európskej únie svojou rozhodovacou činnosťou,[52] avšak čas ukazoval potrebu nového a modernejšieho legislatívneho rámca. Základný kameň progresívnejšej právnej úpravy ochrany osobných údajov na pôde Európskej únie tvorí už spomínané nariadenie Európskeho parlamentu a Rady (EÚ) 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 známe pod skratkou

[49] https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (dostupné 29.10.2019).
[50] https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168007c65bf (dostupné 29.10.2019).
[51] Smernica Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov, Úradný vestník L 281 , 23/11/1995 S. 0031 – 0050.
[52] Pozri napríklad rozhodnutia SDEÚ C-101/01- Lindqvist alebo C-131/12-Google Spain and Google.

GDPR – General Data Protection Regulation).[53] Spracúvanie osobných údajov pri tzv. trestnoprávnych účeloch ako napr. vyšetrovanie, odhaľovanie alebo stíhanie trestných činov kompetentnými orgánmi (v prostredí Slovenskej republiky ide predovšetkým o Policajný zbor SR alebo Zbor väzenskej a justičnej stráže či Národnú kriminálnu agentúru Finančnej správy SR) upravuje smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 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 a o zrušení rámcového rozhodnutia Rady 2008/977/SVV.[54] Zároveň Európska únia prijala osobitné pravidlá pri práci s osobnými údajmi pre inštitúcie Európskej únie v podobe nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES.[55] Vyššie uvedené právne akty tvoria právny rámec ochrany osobných údajov v Európskej únií.

V Slovenskej republike v ére samostatnosti bolo prijatých viacero zákonov, ktoré regulovali a regulujú oblasť ochrany osobných údajov. Konkrétne možno hovoriť o nasledovných právnych predpisoch:

- zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, ktorý predstavuje implementáciu GDPR v oblastiach, kde to samotné nariadenie povoľuje;
- zákon č. 122/2013 Z. z. o ochrane osobných údajov o zmene a doplnení niektorých predpisov, ktorý predstavoval implementáciu smernice 95/46/EHS;
- zákon č. 428/2002 Z. z. o ochrane osobných údajov a
- zákon č. 52/1998 Z. z. o ochrane osobných údajov v informačných systémoch.

[53] Nariadenie Európskeho parlamentu a Rady (EÚ) 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). Ú.v. EÚL 119, 4.5.2016, p. 1–88.

[54] Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 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 a o zrušení rámcového rozhodnutia Rady 2008/977/SVV. Ú. v. EÚ L 119, 4.5.2016, s. 89 – 131.

[55] Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES. Ú. v. EÚ L 295, 21.11.2018, s. 39 – 98.

Uvedený vývoj si dovoľujeme sumarizovať aj v nasledujúcej tabuľke, kde zároveň upozorňujeme aj na ľudsko-právny aspekt práva na ochranu osobných údajov vysvetlený v nasledujúcej stati.

ROK PRIJATIA	PRÁVNA ÚPRAVA
1970	Zákon o ochrane osobných údajov spolkovej republiky Hessensko (*Hessische Datenschutzgesetz*)
1973	Zákon o ochrane osobných údajov – Švédsko (*Datalog*)
1950	Právo na ochranu súkromia v článku 8 Dohovoru o ochrane ľudských práv a základných slobôd
1980	OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
1980	Dohovor Rady Európy č. 108 o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov
1995	Smernica Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov
2009	Právo na ochranu súkromia podľa článku 7 a právo na ochranu osobných údajov podľa článku 8 v Charte základných práv Európskej únie
2016	Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov; Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 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; Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov

2.2.1 Právo na ochranu osobných údajov ako základné ľudské právo

Právo na ochranu osobných údajov nie je predmetom úpravy iba špecifickej legislatívy, ale svoje korene a základy má v základných ľudských právach a slobodách. Vzhľadom na blízkosť a relevanciu európskej právnej kultúry je potrebné zosumarizovať poznatky týkajúce sa právnej úpravy v Dohovore Rady Európy o ochrane ľudských práv a základných slobôd z roku 1950 (Dohovor) a Charty základných práv Európskej únie (Charta),[56] ktorá tvorí záväznú časť Európskeho práva od účinnosti Lisabonskej zmluvy z roku 2009.

Dohovor zakotvuje v článku 8 právo na rešpektovanie súkromného a rodinného života. Napriek tomu, že názov predmetného článku nehovorí explicitne o „práve na súkromie," ako vyplýva z diskusií a materiálov ku legislatívnemu procesu,[57] práve toto právo je predmetom ochrany v rámci článku 8. Článok 8 Dohovoru znie:

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

Jednotlivé odseky reflektujú pozitívny a negatívny záväzok štátu chrániť právo na súkromie. Prvý odsek ustanovuje povinnosť štátu vytvoriť právne nástroje na rešpektovanie súkromného a rodinného života, obydlia a korešpondencie. Interpretovaním konkrétnych pojmov a mantinelov uvedených v danom ustanovení sa zaoberal Európsky súd pre ľudské práva (ESĽP) pomerne extenzívne vo svojej rozhodovacej praxi. Rozhodovaciu činnosť ESĽP v kontexte článku 8 Dohovoru možno rozdeliť v zmysle konkrétnych predmetov ochrany daného článku a to na ochranu (i) súkromného života, (ii) rodinného života, (iii) obydlia a (iv) korešpondencie.[58] Z pohľadu ochrany osobných údajov je predovšetkým potrebné upriamiť

[56] Charta základných práv Európskej únie. Ú. v. EÚ C 326, 26.10.2012, s. 391 – 407.
[57] Napr. FUSTER, G. : The Emergence of Personal Data Protection as a Fundamental Right of the EU. Springer. New York, 2014.
[58] K tomu pozri bližšie European Court of Human Rights: Guide on Article 8 of the European Convention on Human Rights. Right to respect for private and family life, home and correspondence.

pozornosť na predmet ochrany v podobe ochrany súkromného života, nakoľko Dohovor (na rozdiel od Charty – viď nižšie) neobsahuje explicitné zakotvenie práva na ochranu osobných údajov.

Ku výkladu pojmu súkromného života ESĽP pragmaticky judikoval, že nie je možné a ani nevyhnutné poskytnúť definíciu predmetného pojmu.[59] Zároveň však dodal, že rešpektovanie práva na súkromný život musí do určitej miery zahŕňať aj právo jednotlivca nadväzovať vzťahy s inými osobami. Pod tento pojem ESĽP vo svojej rozhodovacej praxi zahrnul viaceré aspekty súkromného života:

1) Fyzická, psychická a morálna integrita jednotlivca kde riešil problematiku napr. reprodukčných práv alebo poskytnutia zdravotnej starostlivosti;
2) Súkromie, kde ESĽP zaradzuje otázky týkajúce sa ochrany podobizní, reputácie, ohovárania, **ochrany osobných údajov** a práve na prístup k osobným údajom;
3) Otázky identity a autonómie v rámci právnych vzťahov ako napr. rodová identitia či právo dohľadať si informácie o svojom pôvode.[60]

Ako je už z vyššie uvedenej diferenciácie zrejmé, ESĽP vo svojej judikatúre v rámci interpretácie článku 8 Dohovoru riešil aj problematiku ochrany osobných údajov napriek tomu, že článok 8 o tejto oblasti výslovne nehovorí a Dohovor neobsahuje samostatné právo na ochranu osobných údajov. Predmetný vzťah jednoznačne ilustroval v prípade *Satakunnan Markkinapörssi Oy a Satamedia Oy proti Fínsku*,[61] kde uviedol, že ochrana osobných údajov je základným pilierom práva na rešpektovanie súkromného a rodinného života. Zároveň vo svojej rozhodovacej činnosti pomerne často judikoval v oblasti uchovávania či používania osobných údajov na súkromné či verejné účely.[62]

Druhý odsek článku 8 Dohovoru upravuje tzv. negatívny záväzok štátu chrániť súkromie. Ide o povinnosť štátu nezasahovať do práva na súkromie jednotlivcov a v prípade, že sa štát napriek generálnemu zákazu do tohto práva rozhodne zasiahnuť, musí tak urobiť za splnenia troch podmienok. Tieto podmienky ustanovujú, že takýto zásah musí byť (i)

[59] ESĽP, Niemitz proti Nemecku (sťažnosť č. 13710/88), 16 December 1992, bod 29.
[60] K diferenciácií pozri bližšie European Court of Human Rights: Guide on Article 8 of the European Convention on Human Rights. Right to respect for private and family life, home and correspondence, s. 18 – 45.
[61] ESĽP, Satakunnan Markkinapörssi Oy and Satamedia Oy proti Fínsku, sťažnosť č. *931/13*, 27. jún 2017, bod 133.
[62] Pozri napr. Rotaru proti Rumunsku [GC], sťažnosť č. 28341/95, Leander proti Švédsku, 26 Marec 1987, S. a Marper proti Spojenému kráľovstvu [GC], sťažnosť č. 30562/04 a 30566/04; M.M. proti Spojenému kráľovstvu sťažnosť č. 24029/07, 13 November 2012, a ďalšie.

v súlade s právnym poriadkom, (ii) legitímny (s legitímnym cieľom)[63] a (iii) nevyhnutný v demokratickej spoločnosti. Opätovne možno v tejto súvislosti zvýrazniť judikatúru ESĽP, ktorá jednotlivé podmienky interpretoval vzhľadom na konkrétne skutkové okolnosti.[64]

Z vyššie uvedeného teda možno vyvodiť, že článok 8 Dohovoru vzhľadom na extenzívnu judikatúru ESĽP obsahuje právo na ochranu osobných údajov napriek tomu, že v ňom nie je výslovne spomenuté.

Iná situácia nastáva v kontexte Charty. Článok 7 Charty upravuje právo na rešpektovanie súkromného a rodinného života.[65] Ide o zrkadlové ustanovenie voči článku 8 ods. 1 Dohovoru.

Článok 8 Charty výslovne zakotvuje právo na ochranu osobných údajov:

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

Prvý odsek článku 8 Charty obsahuje všeobecnú deklaráciu práva každého na ochranu osobných údajov.[66] Článok 8 ods. 2 upravuje základné dva piliere, na ktorých ochrana osobných údajov stojí a padá a to vymedzenie účelu a právneho základu. To znamená, že ak chce akákoľvek entita spracúvať osobné údaje v súlade s príslušnou legislatívou, musí presne určiť účel spracúvania osobných údajov (dôvod prečo osobné údaje spracúva) a na tento účel naviazať právny základ (právny dôvod), ktorý jej poskytuje právny poriadok. V súčasnosti špecifická legislatíva upravuje 6 právnych základov a to konkrétne súhlas, plnenie zmluvy, zákonnú povinnosť, životne dôležitý záujem, verejný záujem a oprávnený záujem.[67] Druhý odsek článku 8 Charty zároveň uznáva niektoré z práv dotknutej osoby a to konkrétne právo na prístup a právo na opravu. Legislatíva, ktorá špecifickejšie reguluje ochranu osobných údajov upravuje viac konkrétnych práv dotknutej

[63] Legitímne ciele upravuje priamo článok 8 ods. 2 Dohovoru. Ide o záujmy národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom alebo zločinnosti, ochrany zdravia alebo morálky alebo na ochranu práv a slobôd iných.

[64] Pozri napr. Uzun proti Nemecku, sťažnosť č. 35623/05; S.A.S. proti Francúzsku [GC], sťažnosť č. 43835/11, alebo Roman Zakharov proti Rusku [GC], sťažnosť č. 47143/06.

[65] *„Každý má právo na rešpektovanie svojho súkromného a rodinného života, obydlia a komunikácie."*

[66] Samotnú definíciu pojmu osobný údaj upravuje GDPR v článku 4 bode 1: *„osobné údaje sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby."* Bližšie sa tomuto pojmu budeme venovať v samostatnej časti kapitoly venovanej GDPR.

[67] Viď článok 6 GDPR.

osoby ako napr. právo na vymazanie alebo právo na prenosnosť.[68] Záverečné ustanovenie článku 8 Dohovoru zakotvuje povinnosť, aby členské štáty zriadili dozorné orgány, ktoré budú kontrolovať spracúvanie osobných údajov v danej krajine. V podmienkach Slovenskej republiky je týmto orgánom Úrad na ochranu osobných údajov Slovenskej republiky so sídlom v Bratislave, ktorý je orgánom štátnej správy s celoštátnou pôsobnosťou.

Charta teda na rozdiel od Dohovoru upravuje aj právo na súkromie (článok 7 Charty) a zároveň aj právo na ochranu osobných údajov (článok 8 Charty). Bližšie právo na ochranu osobných údajov rozvíja už vyššie spomínané všeobecné nariadenie o ochrane údajov – GDPR, ktorému sa budeme podrobnejšie venovať v závere tejto kapitoly.

Na doplnenie ešte uvádzame, že aj naša Ústava Slovenskej republiky[69] na viacerých miestach upravuje problematiku ochrany súkromia a ochrany osobných údajov.[70] Právo na ochranu osobných údajov najvýraznejšie reflektuje článok 19 ods. 3 Ústavy SR, podľa ktorého: *„Každý má právo na ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe."* Zároveň ochranu osobných údajov reflektuje aj článok 22 ods. 1 Ústavy SR v súvislosti s ochranou listového tajomstva.[71] K predmetnému prelínaniu sa vyjadril aj Ústavný súd Slovenskej republiky. Ústavný súd, že článok 19 ods. 3 vystupuje ako *lex generalis,* keďže chráni osobné údaje vo všeobecnosti a článok 22 chráni osobné údaje iba v rámci dôvernosti zasielaných správ.[72]

2.3 Základné princípy ochrany osobných údajov

Ako už bolo naznačené vyššie, prvým medzinárodným dokumentom, ktorý upravoval problematiku ochrany osobných údajov je usmernenie OECD ku ochrane súkromia a cezhraničnom prenose osobných údajov (Usmernenie OECD). Usmernenie OECD síce nie je právne záväzné, ale reflektuje požiadavky mnohých členských krajín OECD vo vzťahu ku spracúvaniu osobných údajov. Predmetom tejto state je teda priblíženie princípov v rámci Usmernenia OECD.

[68] K tomu bližšie pozri články 13 až 22 GDPR.
[69] 460/1992 Zb. Ústava Slovenskej republiky.
[70] K interakcií jednotlivých článkov pozri BRKAN, M. - PSYCHOGIOPULOU, E. : *Courts, Privacy and Data Protection in the Digital Environment.* Amsterdam : Edward Elgar Pub, 2017, s. 180 – 182.
[71] Článok 22 ods. 1 Ústavy SR: *„Listové tajomstvo, tajomstvo dopravovaných správ a iných písomností a ochrana osobných údajov sa zaručujú."*
[72] Napr. Rozhodnutie Ústavného súdu SR sp. zn. I. US 33/95, 29 november 1995.

2.3.1 Stručná charakteristika organizácie pre hospodársku spoluprácu a rozvoj (OECD)

Organizácia pre hospodársku spoluprácu a rozvoj (v anglickom znení Organization for Economic Co-Operation and Development, OECD) bola založená v roku 1961 s cieľom rozvoja spolupráce v oblastiach ekonomického vývoja a svetového obchodu.[73] V súčasnosti OECD tvorí 36 krajín naprieč kontinentami[74] s jedným štátom prizvaným ku spolupráci (Kolumbia). Slovenská republika je súčasťou OECD od februára 1994.

Štruktúru OECD tvoria tri prvky a to Rada OECD, komisie OECD a sekretariát OECD.[75] Radu OECD tvoria zástupcovia jednotlivých členských štátov a Komisie EÚ. Tento orgán zároveň prijíma rozhodnutia konsenzom a diskutuje o rôznych aspektoch globálnej ekonomiky a súvisiacich aktuálnych otázkach. V rámci OECD funguje viac ako 300 odborných komisií, skupín resp. panelov ktoré pripravujú odporúčania pre rôzne strategické dokumenty v oblastiach záujmu predmetnej organizácie. Sekretariát zabezpečuje činnosť celej organizácie a zároveň pripravuje návrhy konkrétnych dokumentov na prijatie Radou OECD.

V roku 1978 bola založená nová expertná skupina,[76] ktorá mala pripraviť usmernenie týkajúce sa ochrany súkromia a cezhraničných prenosov osobných údajov.[77] Pri príprave tohto usmernenia expertná skupina skúmala predovšetkým anglo-americkú doktrínu a americké odporúčania štátnych orgánov, pričom prípravy boli zároveň konzultované aj s delegáciu Rady Európy.[78] Po dvojročnej práci bolo nakoniec v septembri 1980 OECD prijaté odporúčanie týkajúce sa Usmernenia ku ochrane súkromia a cezhraničnom prenose osobných údajov (*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*). Za prijatie vtedy hlasovalo 21 členských krajín z 24.[79]

[73] Viac o OECD na https://www.oecd.org/about/# (dostupné 29.10.2019).
[74] Členské štáty OECD predstavujú Austrália, Rakúsko, Belgicko, Kanada, Čile, Česká republika, Dánsko, Estónsko, Fínsko, Francúzsko, Nemecko, Grécko, Maďarsko, Island, Írsko, Izrael, Taliansko, Japonsko, Južná Kórea, Lotyšsko, Litva, Luxembursko, Mexiko, Holandsko, Nový Zéland, Nórsko, Poľsko, Portugalsko, Slovenská Republika, Slovinsko, Španielskou, Švédsko, Švajčiarsko, Turecko, Spojené kráľovstvo a Spojené štáty americké.
[75] https://www.oecd.org/about/structure/ (dostupné 29.10.2019).
[76] Expert Group on Drafting Guidelines governing the Protection of Privacy and Transborder Data Flows of Personal Data.
[77] FUSTER, G. : The Emergence of Personal Data Protection as a Fundamental Right of the EU. Springer. New York, 2014, s. 77.
[78] Tamže, s. 78.
[79] Tamže, poznámka pod čiarou č. 17.

2.3.2 Usmernenie OECD ku ochrane súkromia a cezhraničnom prenose osobných údajov

Samotné Usmernenie OECD[80] sa skladá z piatich častí, pričom jeho text dopĺňa oficiálne odporúčanie OECD na implementácií tohto nezáväzného právneho aktu a dôvodová správa.

- Prvá časť pod názvom „Všeobecné definície" je tvorená časťami, ktoré definujú základné pojmy Usmernenia OECD (prevádzkovateľ, osobný údaj a cezhraničný prenos osobných údajov) a zároveň táto časť upravuje aj pôsobnosť;
- Druhú časť tvoria základné princípy pri národnej aplikácií právnej úpravy spracúvanie osobných údajov a upravuje základné zásady spracúvania osobných údajov, ktoré by mal obsahovať každý právny akt regulujúci oblasť ochrany osobných údajov;
- Tretia časť upravuje základné princípy medzinárodnej aplikácie (cezhraničné prenosy a ich legitímne obmedzenia);
- Štvrtá časť obsahuje konkrétne odporúčania a pravidlá pri národnej aplikácií druhej a tretej časti Usmernenia OECD; a
- Piata časť zakotvuje právny základ pre medzinárodnú spoluprácu.

Predmetný právny akt by mal byť považovaný za minimálny štandard pri regulácií spracúvania osobných údajov.[81] Usmernenie OECD sa aplikuje na verejný a aj na súkromný sektor[82] a nezakazujú špecifickú právnu úpravu určitých oblastí ako napr. kategorizácie osobných údajov,[83] aplikovanie Usmernenia OECD výlučne na automatizované spracúvanie osobných údajov[84] či vylúčenie aplikácie tohto právneho aktu na situácie, keď spracúvanie osobných údajov nepredstavuje riziko pre súkromie a osobné slobody.[85] Napriek tomu, že Usmernenie OECD v originálnom znení pracuje s pojmom ochrany súkromia (*privacy*), dôvodová správa uvádza, že pod týmto pojmom sa v kontinentálnej Európe rozumie skôr ochrana osobných údajov a zároveň akcentuje potrebu medzinárodnej úpravy nadväzujúcej na zákony o ochrane osobných údajov prijaté niektorými štátmi na európskom kontinente.[86]

---

[80] Dokument je dostupný v anglickom jazyku na https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (dostupné 29.10.2019).
[81] Usmernenie OECD, 1 (6).
[82] Usmernenie OECD, 1 (2) b).
[83] Usmernenie OECD, 1 (2) a).
[84] Usmernenie OECD, 1 (2) c).
[85] Usmernenie OECD, 3 (3).
[86] Dôvodová správa k Usmerneniu OECD, článok 4.

Usmernenie OECD definuje osobné údaje ako akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej osoby.[87] Prevádzkovateľ osobných údajov je v zmysle Usmernenia OECD strana, ktorá v súlade s národným právom má kompetenciu rozhodnúť o obsahu a použití osobných údajov bez ohľadu na to, či zbieranie, uchovávanie, spracúvanie alebo rozširovanie týchto údaje je vykonávané touto stranou alebo sprostredkovateľom v jej mene.[88] Pod pojmom cezhraničný prenos osobných údajov sa myslí pohyb osobných údajov cez hranice.[89]

Okrem základných princípov spracúvania osobných údajov si Usmernenie OECD kladie za cieľ zamedziť reštrikciám pri voľnom toku osobných údajov cez hranice.[90] Členské štáty by z tohto dôvodu mali brať do úvahy vplyv na ostatné krajiny pri spracúvaní osobných údajov a exporte dát z domovskej krajiny.[91] Zároveň by mali členské štáty podstúpiť kroky nato, aby prenos osobných údajov skrz daný členský štát bol bezpečný a neprerušovaný.[92] Usmernenie OECD prirodzene ponúka aj vágne výnimky za účelom nerešpektovania vyššie uvedených pravidiel.[93]

Štvrtá časť Usmernenia OECD formuluje konkrétne ciele pre jednotlivé členské štáty pri implementácií princípov v zmysle druhej a tretej časti Usmernenia OECD.[94] Tieto ciele sú nasledujúce:

- Prijať vhodnú národnú právnu úpravu;
- Podporovať samo-reguláciu napr. vo forme kódexov správania;
- Poskytnúť dotknutých osobám rozumné možnosť na výkon svojich práv;
- Upraviť adekvátne sankcie a možnosti nápravy pri porušení princípov v zmysle Usmernenia OECD;
- Zamedziť nespravodlivej diskriminácií voči dotknutých osobám pri spracúvaní osobných údajov.

Na záver tejto state si ešte dovoľujeme upozorniť, že Usmernenie OECD bolo v roku 2013 revidované a upravené s cieľom implementovať aspekty manažmentu rizík pri implementovaní jednotlivých opatrení a vylepšiť interoperabilitu regulačného rámca.[95] Na

[87] Usmernenie OECD, 1 (1) c).
[88] Usmernenie OECD, 1 (1) a).
[89] Usmernenie OECD, 1 (1) b).
[90] Usmernenie OECD, 3 (18).
[91] Usmernenie OECD, 3 (15).
[92] Usmernenie OECD, 3 (16).
[93] Usmernenie OECD, 3 (17).
[94] K tomu pozri Usmernenie OECD, článok 19.
[95] https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm (dostupné 29.10.2019).

ilustráciu možno uviesť, že oproti pôvodnej verzii Usmernenia OECD boli pridané články týkajúce sa dozorných orgánov, nahlasovaní porušení ochrany osobných údajov, či konkrétne aspekty princípu zodpovednosti.

2.3.3 Princípy spracúvania osobných údajov v zmysle Usmernenia OECD

Druhá časť Usmernenia OECD predstavuje princípy spracúvania osobných údajov, ktoré boli následne pretavené do množstva záväzných právnych predpisov regulujúcich spracúvanie osobných údajov. Napriek revízií Usmernenia OECD v roku 2013 ostali princípy spracúvania osobných údajov nedotknuté. Jedinými doplnkom je pridanie samostatnej časti venujúcej sa konkrétnym parametrom princípu zodpovednosti.[96]

Dôvodová správa k princípom Usmernenia OECD uvádza, že tieto princípy sa pri aplikácií a implementácií dopĺňajú a čiastočne prelínajú.[97] Podľa nášho názoru predmetné princípy predstavujú minimálny štandard, ktorý musí obsahovať každý predpis týkajúci sa spracúvania osobných údajov. Usmernenie OECD vymedzuje 8 princípov:

1) Princíp obmedzenia zbierania (Collection Limitation Principle);
2) Princíp kvality údajov (Data Quality Principle);
3) Princíp vymedzenia účelu (Purpose Specification Principle);
4) Princíp obmedzenia použitia (Use Limitation Principle);
5) Princíp bezpečnostných záruk (Security Safeguards Principle);
6) Princíp otvorenosti (Openess Principle);
7) Princíp individuálnej participácie (Individual Participation Principle);
8) Princíp zodpovednosti (Accountability Principle).

Ad 1) Princíp obmedzenia zbierania údajov znamená, že legislatíva by mala limitovať zber osobných údajov a tieto údaje by mali byť získané zákonný a spravodlivým spôsobom a kde je to vhodné, s vedomím a súhlasom dotknutej osoby.[98] Predmetný princíp má dve roviny. Prvá rovina predstavuje možnosť limitovania zberu určitých typov údajov. V rámci prijímania Usmernenia OECD sa členské štáty nevedeli dohodnúť na konkrétnom výpočte údajov, ktoré by mohli byť považované za citlivé. Európska právna kultúra už totiž v tom čase narábala a *priori* s niektorými údajmi ako citlivými (ako napr. údaje o rase, náboženskom presvedčení či

[96] Usmernenie OECD (revidovaná verzia 2013), článok 15.
[97] Dôvodová správa k Usmerneniu OECD, článok 50.
[98] Usmernenie OECD, článok 2 (7).

trestných záznamoch). Na druhej strane bol anglo-americký prístup, ktorý zvýrazňoval konkrétny kontext a použitie údajov a práve za týchto okolností mohli niektoré údaje reprezentovať citlivé informácie o dotknutých osobách. Vzhľadom na absenciu konsenzu sa teda zvolila možnosť ponechať úpravu citlivých osobných údajov na jednotlivé členské štáty.[99] Druhá rovina diskutovaného princípu spočíva v tom, že dotknuté osoby by nemali byť predmetom nelegálnych aktivít ako nezákonné odpočúvanie či podvody s cieľom poskytnúť informácie.[100]

Ad 2) Princíp kvality údajov reflektuje požiadavku na to, aby osobné údaje spracúvané na konkrétny účel boli relevantné a v nevyhnutnej miere presné, správne a aktuálne.[101] Pri koncipovaní daného princípu pracovná skupina akcentovala použitie údajov vhodných na konkrétny účel. Miera presnosti, správnosti a aktuálnosti by mala byť posúdená skrz otázku, či údaje v nedostatočnej kvalite môžu dotknutej osobe spôsobiť škodu.[102]

Ad 3) Princíp vymedzenia účelu znamená, že najneskôr pri zbere osobných údajov je potrebné určiť konkrétny účel (dôvod), na ktorý budú osobné údaje použité prípadne ak sú dáta použité na iné účely, tie musia byť kompatibilné (súladné) s pôvodnými účelmi.[103] Vymedzenie účelu by malo byť prezentované verejne, či už prostredníctvom podmienok ochrany súkromia alebo iným spôsobom, ktorým sa informujú dotknuté osoby. Predmetný princíp ďalej zakazuje spracúvanie osobných údajov na nové účely, ktoré sú nesúladné s pôvodnými účelmi a v prípade, ak účel zanikne a je to vhodné, osobné údaje by mali byť zničené prípadne anonymizované.[104]

Ad 4) Princíp obmedzenia použitia ustanovuje, že osobné údaje nesmú byť použité, zverejnené alebo inak použité na iné účely, ako účely vymedzené podľa princípu vymedzenia účelu s dvoma výnimkami. Tieto výnimky predstavujú prípady keď (i) dotknutá osoba poskytla súhlas so spracúvaním osobných údajov alebo (ii) spracúvanie vyžaduje právny poriadok (*authority of law*).[105] Daný princíp akcentuje použitie údajov iba na vymedzený účel.[106]

[99] K tomu viac Dôvodová správa k Usmerneniu OECD, článok 51.
[100] K tomu viac Dôvodová správa k Usmerneniu OECD, článok 52.
[101] Usmernenie OECD, článok 2 (8).
[102] K tomu viac Dôvodová správa k Usmerneniu OECD, článok 53.
[103] Usmernenie OECD, článok 2 (9).
[104] K tomu viac Dôvodová správa k Usmerneniu OECD, článok 54.
[105] Usmernenie OECD, článok 2 (10).
[106] K tomu viac Dôvodová správa k Usmerneniu OECD, článok 55.

Ad 5) Princíp bezpečnostných záruk reflektuje požiadavky bezpečnosti na spracúvanie osobných údajov. V zmysle dikcie daného princípu spracúvanie osobných údajov musí podliehať vhodným bezpečnostným zárukám proti rizikám ako strata alebo neoprávnený prístup, zničenie, použitie alebo úprava či zverejnenie údajov.[107] Tento princíp je potrebné vykladať široko a okrem iného zahŕňa implementáciu fyzických bezpečnostných opatrení (zámky alebo používanie čipových kariet pri vstupe do zariadenia), organizačných opatrení (napríklad úrovne prístupu k údajov vzhľadom na pracovnú pozíciu v organizácií), prípadne informatické riešenia (šifrovanie, monitorovanie kybernetických hrozieb v sieti).[108]

Ad 6) Princíp otvorenosti znamená, že entity spracúvajúce osobné údaje musia byť transparentné ohľadom výkonu spracovateľských operácií. Dotknuté osoby musia nevyhnutne poznať povahu spracúvaných osobných údajov, účely ich použitia a taktiež identitu a sídlo prevádzkovateľa.[109] Dotknuté osoby musia mať informácie o spracúvaní osobných údajov, ktoré sa jej týkajú a tieto informácie im musia byť ľahko dostupné bez neprimeraného úsilia, znalostí, cestovania prípadne nákladov.[110]

Ad 7) Princíp individuálnej participácie akcentuje konkrétne práva dotknutých osôb. Predmetný princíp konkrétne ustanovuje, že dotknuté osoby musia mať právo na (i) potvrdenie toho, či prevádzkovateľ o nej spracúva osobné údaje, pričom táto komunikácia zo strany prevádzkovateľa musí byť (ii) vo vhodnom časovom rámci, nie za neprimeraný poplatok (ak sa rozhodne žiadosť spoplatniť), vybavená vhodným spôsobom a vo forme, ktorá je pre dotknutú osobu ľahko zrozumiteľná. Dotknutá osoba má ďalej v prípade odmietnutia takejto žiadosti právo poznať dôvody odmietnutia a takéto negatívne rozhodnutie napadnúť. Zároveň Usmernenie OECD dáva dotknutej osobe právo napadnúť osobné údaje, ktoré prevádzkovateľ spracúva za účelom vymazania, opravy, zmeny a doplnenia.[111]

Ad 8) Posledným princípov v rámci Usmernenia OECD je princíp zodpovednosti. Podľa predmetného princípu je prevádzkovateľ zodpovedný (*accountable*) za súlad s opatrenia pri implementácií vyššie uvedených princípov.[112] Princíp zodpovednosti je bližšie upravený

[107] Usmernenie OECD, článok 2 (11).
[108] K tomu viac Dôvodová správa k Usmerneniu OECD, článok 56.
[109] Usmernenie OECD, článok 2 (12).
[110] K tomu viac Dôvodová správa k Usmerneniu OECD, článok 57.
[111] K tomu pozri Usmernenie OECD, článok 2 (13).
[112] Usmernenie OECD, článok 2 (13).

v článku 16 revidovaného Usmernenia OECD z roku 2013. V zmysle dikcie daného ustanovenia sa princíp zodpovednosti skladá z troch atribútov.

V prvom rade ide o vypracovanie a implementovanie tzv. *privacy management programme* v podobe konkrétnych opatrení pri implementovaní Usmernenia OECD. Tento program by mal brať do úvahy viaceré aspekty spracúvania osobných údajov v organizácií (rozsah, citlivosť, kvalitu a pod.) a mala by mu predchádzať analýza rizík. Implementované mechanizmy by mali byť integrálnou súčasťou organizácie a mali by zahŕňať okrem iného aj proces reakcie na bezpečnostné incidenty. Predmetný program by mal byť predmetom pravidelného preskúmania a doplnenia v prípade potreby. V rámci Slovenskej republiky túto úlohu tradične plnili tzv. bezpečnostné projekty, ktoré však s účinnosťou GDPR stratili opodstatnenie. Modernejšou formou zhmotnenia princípu zodpovednosti tak v súčasnosti sú interné politiky ochrany osobných údajov.

Druhým atribútom princípu zodpovednosti je, že v prípade kontroly dozorného orgánu (alebo iného monitorujúceho subjektu) je prevádzkovateľ povinný preukázať súlad s týmto princípom.

Tretím atribútom je povinnosť informovať dozorný orgán / dotknutú osobu o bezpečnostnom incidente v situácií, ak k nemu dôjde.

Vyššie uvedené princípy v zmysle Usmernenia OECD sú stabilnou súčasťou legislatívy regulujúcej oblasť ochrany osobných údajov. Nižšie uvádzame prehľadnú tabuľku integrácie daných princípov v nasledujúcich medzinárodných dokumentoch:

- Dohovor Rady Európy č. 108 o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (Dohovor 108);[113]
- Nariadenie Európskeho parlamentu a Rady (EÚ)[114] 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 (GDPR);
- APEC Privacy Framework (APEC);[115]

[113] Členské štáty Rady Európy dostupné na https://www.coe.int/en/web/about-us/our-member-states (dostupné 29.10.2019).

[114] Členské štáty Európskej únie dostupné na https://europa.eu/european-union/about-eu/countries_en (dostupné 29.10.2019).

[115] Nezáväzný medzinárodný dokument ázijských krajín združených v organizácií Asia-Pacific Economic Cooperation (APEC). Zoznam participujúcich ekonomík dostupných na http://www.apec.org/about-us/about-apec/member-economies.aspx (dostupné 29.10.2019).

- African Union Convention on Cyber Security and Personal Data Protection (AU);[116]
- Organization of Americas States Preliminary Principles on Privacy (OAS).[117]

[116] Dohovor Africkej únie o kybernetickej bezpečnosti a ochrane osobných údajov. Africká únia je medzinárodná organizácia združujúca štáty na africkom kontinente. Zoznam členských krajín dostupný na https://au.int/en/member_states/countryprofiles2 (dostupné 29.10.2019).

[117] Organizácia amerických štátov združujúcich krajiny zo Severnej Ameriky, Južnej Ameriky a Karibiku. Zoznam dostupný na http://www.oas.org/en/member_states/authorities.asp (dostupné 29.10.2019).

OECD	Dohovor 108	GDPR	APEC	AU	OAS
Princíp obmedzenia zbierania	Osobitné kategórie osobných údajov (článok 6)	• Zásada zákonnosti, spravodlivosti a transparentnosti (článok 5 ods. 1 písm. a) • Spracúvanie osobitných kategórií osobných údajov (článok 9) • Spracúvanie osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky (článok 10)	• Princíp prevencie škody (článok 20) • Princíp obmedzenia zbierania (článok 24)	• Princíp účelu, relevancie a úschovy (článok 13-3) • Spracúvanie citlivých osobných údajov (článok 14)	• Princíp zákonnosti a spravodlivosti • Princíp obmedzenia a nevyhnutnosti
Princíp kvality údajov	Legitimita a kvalita spracúvania (článok 5)	• Zásada zákonnosti, spravodlivosti a transparentnosti (článok 5 ods. 1 písm. a) • Zásada správnosti (článok 5 ods. 1 písm. d) • Zásada minimalizácie	Princíp integrity osobných údajov (článok 27)	• Princíp súhlasu a legitimity spracúvania (článok 13-1) • Princíp účelu, relevancie a úschovy (článok 13-3) • Princíp správnosti údajov (článok 13-4)	• Princíp zákonnosti a spravodlivosti • Princíp obmedzenia a nevyhnutnosti

		údajov (článok 5 ods. 1 písm. c)			
Princíp vymedzenia účelu	Legitimita a kvalita spracúvania (článok 5)	Zásada vymedzenia účelu (článok 5 ods. 1 písm. b)	• Princíp obmedzenia zbierania (článok 24) • Princíp obmedzenia použitia (článok 25)	Princíp účelu, relevancie a úschovy (článok 13-3)	• Princíp obmedzenia účelu • Princíp obmedzenia a nevyhnutnosti
Princíp obmedzenia použitia	Legitimita a kvalita spracúvania (článok 5)	• Zásada zákonnosti, spravodlivosti a transparentnosti (článok 5 ods. 1 písm. a) • Zásada vymedzenia účelu (článok 5 ods. 1 písm. b)	• Princíp prevencie škody (článok 20) • Princíp obmedzenia použitia (článok 25)	Princíp zákonnosti a spravodlivosti (článok 13-2)	Princíp zákonnosti a spravodlivosti
Princíp bezpečnostných záruk	Bezpečnosť osobných údajov (článok 7)	Zásada integrity a dôvernosti (článok 5 ods. 1 písm. f)	• Princíp integrity osobných údajov (článok 27) • Princíp bezpečnostných záruk (článok 28)	Princíp dôvernosti a bezpečnosti (článok 13-6)	Bezpečnostné záruky
Princíp otvorenosti	Transparentnosť spracúvania (článok 8)	Zásada zákonnosti, spravodlivosti a transparentnosti (článok 5 ods. 1 písm. a)	• Princíp upozornenia (článok 21) • Princíp voľby (článok 26)	Princíp transparentnosti (článok 13-5)	Princíp transparentnosti

Princíp otvorenej participácie	• Transparentnosť spracúvania (článok 8) • Práva dotknutej osoby (článok 9)	• Zásada zákonnosti, spravodlivosti a transparentnosti (článok 5 ods. 1 písm. a) • Práva dotknutej osoby (články 13-23)	• Princíp upozornenia (článok 21) • Princíp voľby (článok 26) • Princíp prístupu a opravy (článok 29, 30, 31)	Práva dotknutých osôb (články 16 až 19)	• Princíp transparentnosti • Práva dotknutých osôb
Princíp zodpovednosti	• Bezpečnosť osobných údajov (článok 7) • Dodatočné povinnosti (článok 10)	Zásada zodpovednosti (článok 5 ods. 2)	Princíp zodpovednosti (článok 32)	X	Princíp zodpovednosti

2.4 Ochrana osobných údajov v Európe

Vyššie uvedené princípy spracúvania osobných údajov sa vo výraznej miere premietli aj do legislatívy európskej právnej kultúry. Na tomto území je potrebné vymedziť dve pôsobiace medzinárodne organizácie: Rada Európy a Európska únia. Slovenská republika je členským štátom oboch zoskupení.

Základným dokumentom Rady Európy je už vyššie spomínaný Dohovor, ktorý v článku 8 upravuje právo na rešpektovanie súkromného a rodinného života, obydlia a korešpondencie. Na predmetný článok nadväzuje Dohovor 108 o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (Dohovor 108).

Na úrovní Európskej únie v rámci primárneho práva si pozornosť zasluhuje článok 8 Charty, na ktorý v rámci sekundárneho práva nadväzuje nariadenie Európskeho parlamentu a Rady (EÚ) 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 alebo GDPR).

Ustanovenia týchto dvoch právnych predpisov tvoria základ právnej úpravy v oblasti ochrany osobných údajov v Európe.

2.4.1 Dohovor 108

Prijatiu Dohovoru 108 predchádzali dlhoročné diskusie rôznych odborných skupín na úrovni Rady Európy. V rámci snáh o reakciu na vývoj počítačovej techniky možno spomenúť tri rezolúcie ministrov resp. odporúčania parlamentného zhromaždenia. Prvou „lastovičkou" bolo odporúčanie parlamentného zhromaždenia – Odporúčanie 509 (1968) o ľudských právach a modernom vedeckom a technologickom vývoji.[118] Následne boli Výborom ministrov prijaté ďalšie dve rezolúcie, ktoré sa týkali spracúvania osobných údajov:

- Rezolúcia Výboru ministrov Rady Európy (73) 22 o ochrane súkromia jednotlivcov prostredníctvom elektronických dátových úložiskách v súkromnom sektore;[119] a
- Rezolúcia Výboru ministrov Rady Európy (43) 29 o ochrane súkromia jednotlivcov prostredníctvom elektronických dátových úložiskách vo verejnom sektore.[120]

[118] Council of Europe, Recommendation 509 (1968) on Human Rights and Modern Scientific and Technological Developments, adopted by the Assembly on 31st January 1968 (16th Sitting).

[119] Committee of Ministers of the Council of Europe, Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies.

[120] Committee of Ministers of the Council of Europe, Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector, adopted by the Committee.

Obe vyššie uvedené rezolúcie otvorili cestu prijatiu záväzného dohovoru, ktorý by reguloval spracúvanie osobných údajov. Dohovor 108[121] bol prijatý 17 septembra 1980 Výborom Ministrov Rady Európy a účinný je od 1 októbra 1985. Z hľadiska ochrany osobných údajov je prijatie Dohovoru 108 signifikantné z troch dôvodov. Prvým dôvodom je, že ide o prvý medzinárodný záväzný právny akt, ktorý obsahuje slovné spojenie „ochrana osobných údajov" (*data protection*). Nezáväzné Usmernenie OECD hovorilo skôr o ochrane súkromia napriek tomu, že regulovalo spracúvanie osobných údajov. Druhým dôvodom je, že explicitne nadväzuje ochranu osobných údajov na základné ľudskí práva a slobody vo všeobecnosti. Po tretie, Dohovor 108 artikuluje úzku spojitosť medzi ochranou osobných údajov a článkom 8 Dohovoru – právom na súkromie.[122]

Dohovor 108 tvorí preambula a 7 kapitol:

- Prvú kapitolu tvoria všeobecné ustanovenia vymedzujúce predmet a účel Dohovoru 108, základné definície a pôsobnosť;
- Druhú kapitolu tvoria základné princípy ochrany údajov, ktorým sa budeme venovať nižšie;
- Tretia kapitola je venovaná cezhraničnému toku osobných údajov;
- Štvrtá kapitola ustanovuje vzájomnú pomoc medzi stranami Dohovoru 108 prípadne dotknutým osobám;
- Piata kapitola kreuje konzultatívny výbor s cieľom zlepšiť a monitorovať implementáciu Dohovoru 108;
- Šiesta a siedma kapitola upravujú formálne otázky zmien Dohovoru 108 a záverečné ustanovenia.

Účelom Dohovoru 108 je *„zabezpečiť pre každého jednotlivca na území každej strany dohovoru rešpektovanie jeho práv a základných slobôd, najmä práva na súkromie pri automatizovanom spracovaní osobných údajov o ňom."*[123] Na rozdiel od Usmernenia OECD sa Dohovor 108 na ochranu osobných údajov jednotlivca sa vzťahuje iba na spracúvanie v automatizovanej forme. Automatizované spracúvanie v zmysle Dohovoru 108 zahŕňa operácie, ktoré sa úplne alebo čiastočne vykonávajú automatizovanými prostriedkami ako

of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies.

[121] Slovenskú verziu Dohovoru 108 možno nájsť publikovanú ako Oznámenie Ministerstva zahraničných vecí Slovenskej republiky pod čiastkou 49/2001 Z.z.

[122] Pozri FUSTER, G. : The Emergence of Personal Data Protection as a Fundamental Right of the EU. Springer. New York, 2014, s. 89.

[123] Dohovor 108, článok 1.

napr. uchovávanie údajov, vykonávanie logických alebo aritmetických operácií s týmito údajmi, ich zmeny, výmaz, vyhľadanie alebo šírenie.[124] Členské štáty však môžu rozhodnúť, že budú tento právny akt aplikovať aj na manuálne spracúvanie osobných údajov.[125] Rovnako ako v Usmernení OECD sú osobné údaje definované ako *„všetky informácie, ktoré sa vzťahujú na nejakého identifikovaného alebo identifikovateľného jednotlivca."*[126]

V roku 2001 bol prijatý Dodatočný protokol ku Dohovoru 108, ktorý reguluje postavenie dozorných orgánov a cezhraničný prenos osobných údajov.[127] V roku 2018 bola vplyvom nových technológií a novej právnej úpravy v podobe GDPR prijatá Modernizovaná verzia Dohovoru 108. V ďalšom texte sa pre účely vysvetlenia vývoja daných princípov zameriavame na pôvodné princípy v zmysle Dohovoru 108 z roku 1980 vhodne doplnené komentár ku modernizovanej verzii.

4.1.1 Základné princípy spracúvania osobných údajov v Dohovore 108

Dohovor 108 síce v druhej kapitole upravuje základné princípy spracúvania osobných údajov, avšak s výnimkou názvu predmetnej časti výslovne neustanovuje katalóg konkrétnych princípov ako napr. Usmernenie OECD alebo GDPR. Napriek tomu sa domnievame, že pri rozbore jednotlivých ustanovení Dohovoru 108 v rámci druhej kapitoly je možné nájsť jednoznačné väzby na princípy Usmernenia OECD napriek faktu, že Dohovor 108 o nich výslovne nehovorí ako o princípoch.

Článok 5 Dohovoru 108 upravuje „kvalitu údajov." V predmetom článku sú upravené viaceré princípy, ktoré reflektuje aj Usmernenie OECD prípadne neskôr prijaté GDPR. V zmysle tohto článku osobné údaje musia byť získané a spracúvané korektným a zákonným spôsobom.[128] I keď Dohovor 108 priamo nehovorí o tom, čo je nutné si predstaviť pod pojmom „zákonné" a „korektné" spracúvanie osobných údajov, avšak vzhľadom na derivovanie tohto princípu z vtedy existujúcich národných právnych poriadkov pôjde predovšetkým o zákonnosť spracúvania ako takú prípadne spracúvanie osobných údajov musí byť vykonávané na vhodnom právnom základe (právnom dôvode).[129] Ďalej Dohovor

[124] Dohovor 108, článok 2 (c).
[125] Dohovor 108, článok 3 (c).
[126] Dohovor 108, článok 2 (a).
[127] Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108) regarding supervisory authorities and transborder data flows, Strasbourg, 8.11.2001.
[128] Dohovor 108, článok 5 (a).
[129] K tomu pozri Dôvodovú správu k Dohovoru 108, body 40 – 42.

108 ustanovuje pravidlo, že osobné údaje musia byť *„uchovávané na konkrétne a oprávnené účely a nesmú sa využívať spôsobom nezlučiteľným s týmito účelmi."*[130] Toto ustanovenie tak nadväzuje na zásadu vymedzenia účelu v zmysle Usmernenia OECD a taktiež obsahuje test kompatibility nových účelov s pôvodnými účelmi. Na toto ustanovenie nadväzuje článok 5 písm. c) Dohovoru 108, ktorý upravuje kvantitu údajov spracúvaných na konkrétne účely. Osobné údaje musia byť *„adekvátne, relevantné a nie nadbytočné vzhľadom na účely, na ktoré sa uchovávajú."* To znamená, že prevádzkovateľ by nemal spracúvať viac údajov ako je objektívne potrebné na dosiahnutie vymedzeného účelu. Dohovor 108 obsahuje v článku 5 taktiež aj zásadu správnosti.[131] Navyše, osobné údaje musia byť uchovávané iba po dobu nevyhnutnú na dosiahnutie daného účelu.[132]

Článok 6 upravuje spôsob, akým môže prevádzkovateľ legálne spracúvať osobitné kategórie osobných údajov. Tieto údaje sú definované ako osobné údaje, ktoré odhaľujú rasový pôvod, politické postoje alebo náboženskú vieru či iný svetonázor, ako aj osobné údaje o zdraví a sexuálnom živote a taktiež údaje, ktoré sa týkajú odsúdenia.[133] Tieto údaje možno spracúvať iba za podmienky, ak vnútroštátne právo poskytne primerané záruky na ich spracúvanie.[134]

Článok 7 Dohovoru 108 upravuje bezpečnosť údajov a je v ňom reflektovaný princíp bezpečnosti tak, ako ho poznáme z Usmernenia OECD. *„Prijmú sa primerané bezpečnostné opatrenia na ochranu osobných údajov v automatizovaných súboroch údajov pred náhodným alebo nepovoleným zničením alebo pred náhodnou stratou, ako aj pred nepovoleným prístupom, zmenami alebo šírením."*[135]

Článok 8 Dohovoru 108 (Ďalšie záruky pre dotknutú osobu) upravuje základný katalóg práv dotknutej osoby. V zmysle predmetných ustanovení má dotknutá osoba právo (i) na informácie o spracúvaní osobných údajov,[136] právo na prístup a právo na kópiu spracúvaných osobných údajov,[137] právo na opravu alebo vymazanie za predpokladu, že

[130] Dohovor 108, článok 5 (b).
[131] Dohovor 108, článok 5 (d): *„Osobné údaje musia byť... správne a v prípade potreby aj aktualizované."*
[132] Dohovor 108, článok 5 (e).
[133] Viď Dohovor 108, článok 6.
[134] Napríklad článok 9 ods. 2 GDPR upravuje výnimky, kedy je možné osobitné kategórie osobných údajov spracúvať.
[135] Dohovor 108, Článok 7.
[136] *„Komukoľvek bude umožnené... dozvedieť sa o existencii automatizovaného súboru osobných údajov, jeho hlavných účeloch, ako aj o totožnosti a obvyklom mieste pobytu alebo o hlavnom mieste pôsobenia prevádzkovateľa tohto súboru."*
[137] *„Komukoľvek bude umožnené... získavať v primeraných intervaloch a bez zbytočného odkladu alebo výdavkov potvrdenie o tom, či osobné údaje vzťahujúce sa na danú osobu sa uchovávajú v automatizovanom súbore údajov, a tiež získať tieto údaje v zrozumiteľnej podobe."*

spracúvanie sa nevykonáva v súlade s Dohovorom 108[138] a právo podať opravný prostriedok ak prevádzkovateľ nevyhovel žiadosti o výkon niektorého z vyššie uvedených práv.[139] Tieto práva je možné obmedziť v prípade, ak sa osobné údaje používajú na štatistické účely alebo vedecké účely.[140]

Modernizovaný Dohovor 108 navyše obsahuje v **článku 10** zásadu zodpovednosti, ktorá vyžaduje od prevádzkovateľov preukázať súlad so spracúvaním osobných údajov v zmysle vyššie uvedených princípov.

2.4.2 GDPR

Na úrovní Európskej únie bola viac ako 20 rokov v platnosti smernica Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov. Nakoľko však išlo o smernicu, členské štáty si povinnosti uvedené v nej implementovali do svojich národných právnych poriadkov odlišným spôsobom.

Od roku 2012 prebiehali odborné diskusie a debaty v rámci európskych štruktúr týkajúcich sa modernizácie daného právneho rámca. Výsledkom spoločnej snahy viacerých aktérov bolo prijatie nového legislatívneho rámca regulujúceho ochranu osobných údajov v podobe:

- Nariadenia Európskeho parlamentu a Rady (EÚ) 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 alebo GDPR); a
- Smernice Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 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 a o zrušení rámcového rozhodnutia Rady 2008/977/SVV (Policajná smernica).[141]

---

[138] *„Komukoľvek bude umožnené... v prípade potreby dosiahnuť opravu alebo výmaz týchto údajov, ak boli spracované v rozpore s ustanoveniami vnútroštátneho zákona, ktorým sa vykonávajú základné princípy uvedené v článkoch 5 a 6 tohto dohovoru."*

[139] *„Komukoľvek bude umožnené... uplatniť opravný prostriedok v prípade, že sa nevyhovelo žiadosti o potvrdenie, oznámenie, opravu alebo o výmaz uvedenej v písmenách b) a c) tohto článku."*

[140] Dohovor 108, článok 9 (3).

[141] Policajná smernica bola do slovenského právneho poriadku implementovaná v rámci 3. časti zákona č. 18/2018 Z. z. o ochrane osobných údajov. Dané ustanovenia regulujú spracúvanie osobných údajov tzv. kompletnými orgánmi (ako napr. Policajný zbor SR alebo Zbor väzenskej a justičnej stráže SR) pri trestnoprávnych účeloch, čiže vyšetrovanie,

Dôvodov na prijatie nového právneho rámca bolo viacero. V prvom rade bola predmetná legislatíva pomerne zastaralá v dôsledku dynamického vývoja nových technológií a dátovej analytiky. Ďalším dôvodom bola rozdielna implementácia staršej smernice na úrovní členských štátov. V neposlednom rade giganti IT priemyslu ako Facebook, Google či Apple boli častokrát zo strany dozorných orgánov či samotných jednotlivcov upozorňovaní, že nedodržiavajú súkromie užívateľov pri poskytovaní produktov alebo služieb. Tieto všetky faktory ovplyvňovali prijatie GDPR a Policajnej smernice.

Zároveň je potrebné dodať, že GDPR v určitých otázkach ponechalo voľnosť pre členské štáty a tie a tak v národných právnych poriadkoch mohli upraviť napr. vyváženie práva na ochranu osobných údajov a slobodu prejavu či právo na informácie, otázky mlčanlivosti, vek maloletých pri používaní služieb informačnej spoločnosti či ďalšie otázky.[142] Slovenská republika reflektovala aj tieto potreby v rámci úpravy zákona č. 18/2018 Z. z. o ochrane osobných údajov (Zákon o ochrane osobných údajov). Ten je síce pomerne extenzívne spracovaný (obsahuje 112 §), avšak reálne sa z neho vo väčšine prípadov uplatňuje iba určitá časť (hlavne § 78 a 79, piata časť upravujúca konanie a kontrolu pred Úradom na ochranu osobných údajov a šiesta čas upravujúca spoločné, záverečné a prechodné ustanovenia). Je to z toho dôvodu, že tretia časť Zákona o ochrane osobných údajov implementuje Policajnú smernicu a aplikuje sa len na vymedzený počet subjektov a druhá časť, ktorá doslova a do písmena kopíruje väčšinou ustanovení GDPR sa aplikuje na spracovateľské operácie, ktoré nepodliehajú právu Európskej únie. Na drvivú väčšinu prevádzkovateľ sa tak bude aplikovať GDPR ako všeobecná právna a úprava a štvrtá, piata a šiesta časť Zákona o ochrane osobných údajov.[143] Z tohto dôvodu sa teda budeme venovať právnej úprave obsiahnutej v GDPR.

GDPR je delené do deviatich kapitol a obsahuje 99 článkov.

- Kapitola I obsahuje všeobecné ustanovenia (predmet a ciel legislatívy, pôsobnosť, vymedzenie pojmov);
- Kapitola II obsahuje základné zásady spracúvania osobných údajov;

odhaľovanie prípadne výkon a ďalšie aktivity pred, pri a po trestnom stíhaní. Vzhľadom na špecifickosť danej úpravy sa Policajnej smernici a jej implementácií nebudeme v rámci tejto učebnice ďalej venovať.

[142] K tomu pozri kapitolu IX GDPR.

[143] Pozri viac https://dataprotection.gov.sk/uoou/sk/content/kedy-nariadenie-kedy-zakon-o-ochrane-osobnych-udajov (dostupné 29.10.2019).

- Kapitola III upravuje práva dotknutých osôb;
- Kapitola IV obsahuje úpravu vzťahu medzi prevádzkovateľom a sprostredkovateľom vrátane špecifických povinností ako viesť záznamy o spracúvaní osobných údajov či bezpečnostné opatrenia, oznamovanie porušení ochrany osobných údajov a pod.;
- Kapitola V upravuje prenosy osobných údajov do tretích krajín alebo medzinárodných organizáciám;
- Kapitola VI obsahuje úpravu nezávislých dozorných orgánov a ich úlohy;
- Kapitola VII upravuje spoluprácu a konzistentnosť rozhodovania dozorných orgánov v Európskej únii;
- Kapitola VIII ustanovuje špecifické požiadavky na zodpovednosť, prostriedky nápravy a sankcie;
- Kapitola IX obsahuje ustanovenia o osobitných situáciách spracúvania osobných údajov;
- Kapitola X upravuje delegované akty a vykonávacie akty;
- Kapitolu XI tvoria záverečné ustanovenia.

V nasledujúcich statiach sa zameriame na pôsobnosť GDPR (kedy sa GDPR aplikuje) a na základné zásady spracúvania osobných údajov a súvisiace inštitúty.

2.4.2.1 Pôsobnosť GDPR

V prvom rade považujeme za vhodné vymedziť, kedy sa GDPR aplikuje z hľadiska vecnej, územnej a osobnej pôsobnosti. V rámci toho je následne potrebné definovať aj základné pojmy, s ktorými GDPR operuje.

2.4.2.1.1 Vecná pôsobnosť GDPR

Vecná pôsobnosť GDPR je upravená v článku 2 ods. 1 GDPR: *„Toto nariadenie sa vzťahuje na spracúvanie osobných údajov vykonávané úplne alebo čiastočne automatizovanými prostriedkami a na spracúvanie inými než automatizovanými prostriedkami v prípade osobných údajov, ktoré tvoria súčasť informačného systému alebo sú určené na to, aby tvorili súčasť informačného systému.“* Daný článok upravuje pozitívnu vecnú pôsobnosť GDPR. V zmysle dikcie predmetného článku sa GDPR aplikuje na spracúvanie osobných údajov, ktoré je vykonávané (i) automatizovanými prostriedkami, (ii) čiastočne

automatizovanými prostriedkami alebo (iii) manuálne, ak osobné údaje tvoria súčasť informačného systému.

Spracúvanie osobných údajov je definované v článku 4 bode 1 GDPR a to demonštratívnymi výpočtom spracovateľských operácií, ktoré možno subsumovať pod definíciu spracúvania osobných údajov. V zmysle daného článku sa pod spracúvaním osobných údajov rozumie *„operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, **napríklad** získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami."* O čisto automatizované spracúvanie by išlo v prípade, ak by napríklad banka spracúvala údaje o žiadateľovi o úver a túto žiadosť by následne automatizovane posúdil algoritmus, ktorý by zároveň rozhodol o tom, či banka úvery poskytne alebo nie. V prípade čiastočne automatizovaného spracúvania by vo vyššie uvedenom prípade nakoniec o poskytnutí úveru rozhodol človek a v procese by bol prítomný ľudský zásah. Manuálne spracúvanie osobných údajov predstavuje napr. kartotéka pacientov u lekára zoradená podľa abecedy.[144]

Ústredným pojmom GDPR je však definícia osobného údaju. Osobným údajom *„je akékoľvek informácia týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby."*[145] Identifikovateľná fyzická osoba je taká osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä prostredníctvom odkazu na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby. Pojem identifikovateľnosti ďalej vykladá recitál 26 GDPR, ktorý uvádza: *„Na určenie toho, či je fyzická osoba identifikovateľná, by sa mali brať do úvahy všetky prostriedky, pri ktorých existuje primeraná pravdepodobnosť, že ich prevádzkovateľ alebo akákoľvek iná osoba využije, napríklad osobitným výberom, na priamu alebo nepriamu identifikáciu fyzickej osoby. Na zistenie toho, či je primerane pravdepodobné, že*

[144] Informačný systém je v zmysle článku 4 bod 6 GDPR definovaný ako *„akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe."* Je nutné poznamenať, že v rámci slovenskej právnej kultúry došlo ku dezinterpretácií tohto pojmu, avšak v zmysle staršej smernice a aj GDPR ide o manuálne spracúvanie údajov v rámci systému, v ktorom sa dá vyhľadávať podľa určitého kľúča.
[145] Článok 4 bod 1 GDPR.

sa prostriedky použijú na identifikáciu fyzickej osoby, by sa mali zohľadniť všetky objektívne faktory, ako sú náklady a čas potrebný na identifikáciu so zreteľom na technológiu dostupnú v čase spracúvania, ako aj na technologický vývoj." Tento recitál reprezentuje tzv. test primeranej pravdepodobnosti, ktorý odpovedá na to, či konkrétna dotknutá osoba je skutočne identifikovateľná. Predmetným testom sa zaoberal aj Súdny dvor Európskej únie *Patrick Breyer v Spolková republika Nemecko.*[146] Skutkovo sa prípad týkal otázky, či dynamická IP adresa predstavuje osobný údaje v zmysle staršej legislatívy na ochranu osobných údajov. Prevádzkovateľ webového sídla mal k dispozícií IP adresa užívateľa, avšak nemal priamo informáciu, na koho je táto IP adresa registrovaná. Tieto informácie má zvyčajne k dispozícií poskytovateľ internetového pripojenia. Otázka teda bola, či pre prevádzkovateľa webového sídla predstavuje IP adresa osobný údaj v zmysle legálnej definície. Luxemburský súd judikoval: *„...že dynamická IP adresa, ktorú poskytovateľ online mediálnych služieb uchováva v súvislosti s prehliadaním si určitou osobou internetovej stránky, ktorú tento poskytovateľ sprístupnil verejnosti, predstavuje pre tohto poskytovateľa osobný údaj v zmysle tohto ustanovenia, **ak má k dispozícii právne prostriedky**, na základe ktorých dokáže identifikovať dotknutú osobu vďaka ďalším informáciám, ktorými disponuje poskytovateľ internetového pripojenia tejto osoby."* Toto rozhodnutie tak znamená, že ak existujú právom dovolené prostriedky na identifikáciu jednotlivca, pôjde o osobné údaje. Napríklad univerzita má k dispozícií tzv. univerzitné osobné čísla študentov (číselný rad znakov). Tento údaj predstavuje pre univerzitu osobný údaj konkrétneho študenta, nakoľko univerzita disponuje aj ďalšími identifikátormi, ktoré k tejto informácií vie priradiť a identifikovať dotknutú osobu. Inou ilustráciou je situácia, ak dôjde ku kybernetickému útoku na webstránku orgánu verejnej moci a ten má k dispozícii iba IP adresu útočníka. V tomto prípade je IP adresa taktiež osobným údajom a to z toho dôvodu, že orgán verejnej moci má k dispozícií právne prostriedky na zistenie totožnosti útočníka (prostredníctvom orgánov činných v trestnom konaní, ktoré môžu požiadať prevádzkovateľa internetového pripojenia o stotožnenie IP adresy s konkrétnym páchateľom).

Ku pojmu osobný údaj teda možno záverom dodať, že nie každá informácia je automaticky osobným údajom. Vždy bude záležať od konkrétnych okolností a kontextu, či je daná osoba identifikovateľná alebo nie.

[146] C-582/14 Patrick Breyer proti Bundesrepublik Deutschland.

GDPR upravuje v článku 2 ods. 2 negatívnu pôsobnosť nariadenia. To znamená situácie, keď sa GDPR neaplikuje. Ide predovšetkým o situácie, na ktoré sa neaplikuje právo Európskej únie, otázky národnej bezpečnosti a tajných služieb či otázky patriace do pôsobnosti Policajnej smernice. Osobitne zaujímavou otázkou je výnimka z pôsobnosti, ktorá sa aplikuje v prípade, že spracúvanie osobných údajov prebieha fyzickou osobou v rámci výlučne osobnej alebo domácej činnosti.[147] GDPR však nedefinuje, o aké situácie konkrétne ide. Judikatúra SDEÚ však naznačuje určitý smer. O spracúvanie v rámci výlučne osobnej alebo domácej činnosti nepôjde vtedy, ak sú osobné údaje zverejnené na internete[148] prípadne monitorovanie ulice kamerovým systémom umiestneným nad dverami domu.[149] Napríklad, ak sa dve mamičky na pieskovisku rozprávajú o svojich ratolestiach, na túto situáciu sa nebude aplikovať GDPR, keďže takáto situácia nepatrí do pôsobnosti GDPR.

2.4.2.1.2 Územná pôsobnosť GDPR

GDPR upravuje územnú pôsobnosť v rámci článku 3 GDPR. Z predmetných ustanovení môžeme derivovať dva režimy územnej GDPR a to:

a) intra-teritoriálnu územnú pôsobnosť GDPR (článok 3 ods. 1 GDPR); a

b) extra-teritoriálnu územnú pôsobnosť GDPR (článok 3 ods. 2 a 3 GDPR).

Ad a) Intra-teritoriálna pôsobnosť GDPR

Intra-teritoriálnu pôsobnosť GDPR reflektuje článok 3 ods. 1 GDPR, ktorý ustanovuje, že *„toto nariadenie sa vzťahuje na spracúvanie osobných údajov v rámci činnosti prevádzky prevádzkovateľa alebo sprostredkovateľa v Únii, a to bez ohľadu na to, či sa spracúvanie vykonáva v Únii alebo nie.“* Aby sa aplikovalo GDPR v zmysle daného článku, musí ísť o spracúvanie osobných údajov v rámci činnosti prevádzky v Európskej únií. Pojem „prevádzka“ sa zvykne interpretovať pomerne široko, pričom najčastejšie môže ísť o dcérsku spoločnosť alebo výhradné obchodné zastúpenie.[150] V zmysle judikatúry je vykladaný pojem

[147] Článok 2 ods. 2 písm. c) GDPR.
[148] C-101/01- Lindqvist
[149] C-212/13-Ryneš
[150] K tomu Recitál 22 GDPR: *„Každé spracúvanie osobných údajov v kontexte činností prevádzkarne prevádzkovateľa alebo sprostredkovateľa v Únii by sa malo vykonávať v súlade s týmto nariadením bez ohľadu na to, či sa samotné spracúvanie uskutočňuje v Únii. Prevádzkareň znamená efektívny a skutočný výkon činnosti prostredníctvom stálych dojednaní. Právna forma takýchto dojednaní, či už ide o pobočku alebo dcérsku spoločnosť s právnou subjektivitou, nie je v tomto ohľade určujúcim faktorom.“*

„činnosť prevádzky“ taktiež extenzívne a zahŕňa čo i len minimálnu aktivitu danej prevádzkarne v rámci jedného z členských štátov Európskej únie.[151]

Príkladom, kedy sa daný článok bude aplikovať je napríklad situácia, ak má spoločnosť sídliaca v USA svoje sídlo v Kalifornií a pobočky v Berlíne, Paríži a Dubline, ktoré usmerňujú marketingové aktivity danej firmy.

Ad b) Extra-teritoriálna pôsobnosť GDPR

GDPR sa za určitých okolností aplikuje aj v prípadoch, ak spoločnosť nemá fyzicky prevádzkareň v rámci Európskej únie. Článok 3 ods. 2 GDPR ustanovuje, že nariadenie sa vzťahuje na spracúvanie osobných údajov dotknutých osôb, ktoré sa nachádzajú v Únii, prevádzkovateľom alebo sprostredkovateľom, ktorý nie je usadený v Únii, pričom spracovateľská činnosť súvisí (i) s ponukou tovaru alebo služieb týmto dotknutým osobám v Únii bez ohľadu na to, či sa od dotknutej osoby vyžaduje platba, alebo (ii) so sledovaním ich správania, pokiaľ ide o ich správanie na území Únie. To znamená, že ak zahraničná spoločnosť ponúka tovary a služby dotknutým osobám v EÚ prípadne sleduje ich správanie, GDPR sa na túto spoločnosť aplikuje. Nariadenie však nedefinuje, kedy ide o ponuku tovarov a služieb. Pre interpretáciu tohto pojmu je potrebné nahliadnuť do judikatúry SDEÚ, ktorá hovorí[152] že ponuka tovarov a služieb osobám v EÚ je vtedy ak napr. webstránka ponúka dovoz tovaru do krajiny EÚ, je v jazyku členského štátu EÚ, dá sa platiť v mene členských štátov EÚ prípadne stránka obsahuje referencie od obyvateľov EÚ. Sledovanie správania obyvateľov môže spoločnosť vykonávať napr. prostredníctvom behavioriálnej reklamy prípadne spracúvania IP adries či cookies.

Ďalším typom extra-teritoriálnej pôsobnosti GDPR sú prípady, ak spracúvanie osobných údajov vykonáva prevádzkovateľ, ktorý nie je usadený v Únii, ale na tomto mieste, sa na základe medzinárodného práva verejného uplatňuje právo členského štátu.[153] Typicky pôjde o prípady, spracúvania osobných údajov na ambasádach a konzulátoch.

[151] K tomu pozri napr. C-131/12-Google Spain and Google alebo C-230/14-Weltimmo.
[152] C-585/08 - Pammer a Hotel Alpenhof.
[153] Článok 3 ods. 3 GDPR.

2.4.2.1.1 Osobná pôsobnosť GDPR

Z hľadiska osobnej pôsobnosti je potrebné rozlišovať 5 typov entít v zmysle GDPR. Najdôležitejšími pojmami sú dotknutá osoba, prevádzkovateľ a sprostredkovateľ. Pre kompletnosť uvádzame aj definíciu pojmov príjemcov a tretej strany.

Dotknutá osoba znamená identifikovanú alebo identifikovateľnú osobu, ktorej sa osobné údaje týkajú. GDPR nedefinuje termín dotknutá osoba, ale jej vymedzenie možno odvodiť z ustanovení týkajúcich sa pojmu osobný údaj (článok 4 bod 1 GDPR).

Prevádzkovateľ[154] je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov, pričom platí, že ak sa účely a prostriedky tohto spracúvania stanovujú v práve Únie alebo v práve členského štátu, možno prevádzkovateľa alebo konkrétne kritériá na jeho určenie určiť v práve Únie alebo v práve členského štátu. Najdôležitejším aspektom definície prevádzkovateľa je „určenie účelu." Entita, ktorá určí účel spracúvania osobných údajov (dôvod, prečo sú osobné údaje spracúvané) je prevádzkovateľom. Napríklad univerzita poskytuje študentom vzdelávanie a na tento účel (poskytovanie štúdia) spracúva určité množstvo osobných údajov. Účel vymedzila univerzita a tá bude teda prevádzkovateľom. Spoloční prevádzkovatelia[155] sú dvaja alebo viacerí prevádzkovatelia, ktorí spoločne určia účely a prostriedky spracúvania. Ak dvaja alebo viacerí prevádzkovatelia spoločne určia účely a prostriedky spracúvania, sú spoločnými prevádzkovateľmi.

Sprostredkovateľ[156] je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa. To znamená, že v tomto prípade je nevyhnutné mať poverenie a pokyny od prevádzkovateľa ako spracúvať osobné údaje v jeho mene. Nie je vylúčené, že jedná entita môže figurovať aj ako prevádzkovateľ a aj ako sprostredkovateľ. Napríklad univerzita poverí externú firmu výrobou študentských čipových kariet. Na tento účel prenesie údaje tejto spoločnosti a tá následne tieto karty vyrobí. Účel však určila univerzita (študentské preukazy) a externá firma je len sprostredkovateľ, ktorý koná na základe pokynov univerzity. Avšak ak by si táto firma chcela vyhotovovať z dát vlastné štatistiky, na účely vytvárania štatistík bude prevádzkovateľom.

[154] Článok 4 bod 7 GDPR.
[155] Článok 26 ods. 1 GDPR.
[156] Článok 4 bod 8 GDPR.

Príjemca[157] je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorému sa osobné údaje poskytujú bez ohľadu na to, či je treťou stranou. Orgány verejnej moci, ktoré môžu prijať osobné údaje v rámci konkrétneho zisťovania v súlade s právom Únie alebo právom členského štátu, sa však nepovažujú za príjemcov. Príjemcami údajov, ktoré spracúva univerzita sú napríklad zamestnanci univerzity.

Tretia strana[158] je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt než dotknutá osoba, prevádzkovateľ, sprostredkovateľ a osoby, ktoré sú na základe priameho poverenia prevádzkovateľa alebo sprostredkovateľa poverené spracúvaním osobných údajov. Treťou stranou je napríklad daňový úrad, ktorý bude na základe zákonných oprávnení povinný skontrolovať daňové aspekty vyplácania miezd u konkrétneho zamestnávateľa.

2.4.2.1 Základné zásady spracúvania podľa GDPR

Podobne ako Usmernenie OECD či Dohovor 108, aj GDPR upravuje svoje vlastné zásady spracúvania osobných údajov. Ako bude jasné z výkladu nižšie, tie sú odvodené zo starších právnych aktov. Poukážeme aj na konkrétne inštitúty GDPR, ktoré jednotlivé zásady reflektujú prípadne predstavujú novinku v oblasti ochrany osobných údajov.

Článok 5 GDPR upravuje šesť zásad spracúvania osobných údajov:

a) Zásada zákonnosti (článok 5 ods. 1 písm. a) GDPR);
b) Zásada obmedzenia účelu (článok 5 ods. 1 písm. b) GDPR);
c) Zásada minimalizácie údajov (článok 5 ods. 1 písm. c) GDPR);
d) Zásada správnosti (článok 5 ods. 1 písm. d) GDPR);
e) Zásada minimalizácie uchovávania údajov (článok 5 ods. 1 písm. e) GDPR);
f) Zásada integrity a dôvernosti (článok 5 ods. 1 písm. f) GDPR);
g) Zásada zodpovednosti (článok 5 ods. 2 GDPR).

[157] Článok 4 bod 9 GDPR.
[158] Článok 4 bod 10 GDPR.

2.4.2.1.1 Zásada zákonnosti (spravodlivosti a transparentnosti)

Článok 5 ods. 1 písm. a) GDPR ustanovuje, že osobné údaje musia byť spracúvané zákonným spôsobom, spravodlivo a transparentne vo vzťahu k dotknutej osobe. Predmetná zásada obsahuje tri atribúty: zákonnosť, spravodlivosť a transparentnosť.

Zákonnosť spracúvania osobných údajov spočíva v dvoch úrovniach. V prvom rade je potrebné osobné údaje spracúvať na jednom alebo viacerých právnych základoch podľa článku 6 GDPR. To znamená, že každý účel vymedzený prevádzkovateľom musí byť previazaný s jedným alebo viacerými právnymi základmi podľa článku 6 GDPR. Predmetný článok upravuje 6 právnych základov: súhlas;[159] plnenie zmluvy;[160] zákonná povinnosť;[161] ochrana životne dôležitých záujmov dotknutej alebo inej fyzickej osoby;[162] verejný záujem[163] a oprávnený záujem prevádzkovateľa (legitímny záujem).[164] Napríklad ak univerzita spracúva osobné údaje na študijné účely, robí to na základe zákonnej povinnosti v zmysle právnej úpravy vysokých škôl. Osobné údaje svojich zamestnancov spracúva na základe zmluvy prípadne Zákonníka práce. Newsletter (posielanie ponúk alebo informácií mailom zákazníkovi) sa tradične posiela na právnom základe súhlasu. Súhlas je však najkrehkejší právny základ nakoľko ním plne disponuje dotknutá osoba a môže ho kedykoľvek odvolať.

Druhá úroveň zásady zákonnosti je, aby spracúvanie osobných údajov bolo ako také v súlade s celým právnym poriadkom. To znamená, že napríklad profilovanie tehotných žien a následne zasielanie zľavových kupónov by potenciálne narazilo na zásadu nediskriminácie ustanovenej v Ústave SR prípadne Dohovore či Charte, napriek tomu, že spracúvanie osobných údajov by bolo v súlade s GDPR.

Ďalším atribútom tejto zásady je spravodlivosť. Spracúvanie osobných údajov musí byť spravodlivé (*fair*) pre dotknuté osoby. V tomto smere je možné zvýrazniť aspekt dôvery medzi prevádzkovateľom a dotknutou osobou.[165]

---

[159] Článok 6 ods. 1 písm. a): *„dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov na jeden alebo viaceré konkrétne účely“*

[160] Článok 6 ods. 1 písm. b): *„spracúvanie je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo aby sa na základe žiadosti dotknutej osoby vykonali opatrenia pred uzatvorením zmluvy.“*

[161] Článok 6 ods. 1 písm. c): *„spracúvanie je nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa.“*

[162] Článok 6 ods. 1 písm. d): *„spracúvanie je nevyhnutné, aby sa ochránili životne dôležité záujmy dotknutej osoby alebo inej fyzickej osoby.“*

[163] Článok 6 ods. 1 písm. e): *„spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi.“*

[164] Článok 6 ods. 1 písm. f): *„spracúvanie je nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana, s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody dotknutej osoby, ktoré si vyžadujú ochranu osobných údajov, najmä ak je dotknutou osobu dieťa.“*

[165] Viac k tomu BERTHOTY, J. a kol. : Všeobecné nariadenie o ochrane osobných údajov. C.H. Beck. Praha, 2018, s. 203 – 204.

Posledným atribútom predmetnej zásady je transparentnosť. Táto požiadavka je reflektovaná vo viacerých požiadavkách a inštitútoch GDPR:

- Plnenie informačnej povinnosti v zmysle článkov 12,13 a 14 GDPR – dotknutá osoba má právo vedieť určité informácie o spracúvaní osobných údajov a prevádzkovatelia sú povinní im tieto informácie proaktívne poskytnúť;[166]
- Komunikácia práv dotknutej osoby – prevádzkovatelia musia dotknuté osoby upozorniť na ich konkrétne práva v zmysle GDPR;[167]
- Komunikácia porušení ochrany osobných údajov dotknutým osobám – v prípade ak dôjde ku bezpečnostnému incidentu (napr. hacknutie systému alebo únik údajov), ktorý možno kvalifikovať ako porušenie ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, tak prevádzkovateľ musí dotknutú osobu na to upozorniť.[168]

2.4.2.1.2 Zásada obmedzenia účelu

Zásada obmedzenia účelu podľa článku 5 ods. 1 písm. b) GDPR znamená, že osobné údaje musia byť získavané na konkrétne určené, výslovne uvedené a legitímne účely a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi. Účelom možno rozumieť cieľ resp. dôvod, s ktorým sa osobné údaje spracúvajú. Na základe účelu vieme určiť požadovanú správnosť osobných údajov, ich potrebnosť, dobu uchovávania a iné kľúčové faktory ovplyvňujúce spracúvanie osobných údajov. Účel musí byť konkrétny, výslovne uvedený a legitímny.[169] Prevádzkovatelia zvyknú vymedzovať účely všeobecnejšie a následne pripojiť charakteristiku, čo ktorý účel znamená. Napr. účel marketing môže znamenať analýzu údajov a profilovanie užívateľom pri zobrazení vhodnej reklamy.[170] Prevádzkovatelia účely zverejňujú v rámci plnenia informačnej povinnosti a majú ich zvyčajne niekoľko (napr. univerzita má študijne účely, ale aj účely týkajúce sa spracúvania dát zamestnancov, prípadne plnia zákonné povinnosti a podobne).

Ďalšie spracúvanie na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či štatistické účely sa v súlade s článkom 89 ods. 1 GDPR nepovažuje

[166] K tomu pozri viac článok 12 GDPR, ktorý upravuje akým spôsobom tieto informácie poskytnúť a články 13 a 14 GDPR, ktoré upravujú aké informácie poskytnúť a výnimky z informačnej povinnosti.
[167] GDPR upravuje výpočet práv dotknutej osoby v článkoch 13 až 22 GDPR.
[168] K tomu pozri článok 34 GDPR.
[169] K tomu pozri Article 29 Data Protection Working Party Opinion 03/2013 on purpose limitation, s. 15-16.
[170] Pozri napríklad účely Univerzity Komenského v Bratislave na https://uniba.sk/ochrana-osobnych-udajov (dostupné 29.10.2019).

za nezlučiteľné s pôvodnými účelmi. To znamená, že výskumné alebo štatistické účely za splnenia požiadaviek GDPR je možné robiť na základe už získaných dát automaticky.
V rámci zásady vymedzenia účelu posudzujeme aj test zlučiteľnosti účelov na inú spracovateľskú operáciu ako pôvodne vymedzenú. V prípade ak napr. spoločnosť predávajúca nábytok spracúva údaje o svojich zákazníkoch za účelom efektívnej donášky tovaru k zákazníkovi, nemôže použiť predmetné údaje na marketingové účely v podobe posielania letákov „ušitých na mieru" na základe predchádzajúcich nákupov. GDPR ustanovuje 5 faktorov, ktoré by mal prevádzkovateľ zohľadniť pri posúdení, či sú účely zlučiteľné alebo nie.[171] Tieto faktory predstavujú len minimálny štandard a prevádzkovateľ môže vziať do úvahy aj iné.

2.4.2.1.3 Zásada minimalizácie údajov

Zásada minimalizácie údajov v zmysle článku 5 ods. 1 písm. c) GDPR znamená, že osobné údaje musia byť primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú. Prevádzkovateľ je povinný prihliadať na spracúvanie dostatočne kvalitných (správnych) osobných údajov o dotknutej osobe na naplnenie vymedzeného účelu. Avšak zároveň je povinný nepracovať s viac údajmi ako je na výkon špecifickej spracovateľskej operácie potrebné. Prevádzkovateľ by tak mal vyhodnotiť proporcionalitu a nevyhnutnosť zozbieraných údajov voči určenému účelu. Napríklad univerzita by nemala spracúvať údaj o krvnej skupine svojich študentov, nakoľko tento údaj nie je nevyhnutný na poskytovania štúdia. Iná situácia by bola, ak by univerzita poskytovala študentom stáž v rámci rizikovejších povolaní ako napr. práca v bani.

2.4.2.1.4 Zásada správnosti

Zásada správnosti osobných údajov podľa článku 5 ods. 1 písm. d) GDPR znamená, že osobné údaje musia byť správne a podľa potreby aktualizované. Prevádzkovateľ je zároveň povinný prijať všetky potrebné opatrenia, aby sa zabezpečilo, že sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bezodkladne vymažú alebo opravia. Považujeme za nutné zvýrazniť, že zásada správnosti osobných údajov sa vždy musí posudzovať vzhľadom na účel spracúvania. V prípade, ak je účel spracúvania priam závislý od správnosti údajov, údaje musia byť aktuálne a správne. Napríklad univerzita si musí od

[171] Pozri článok 6 ods. 4 GDPR.

študentov pri prijímacom konaní overiť, či získali požadované stredoškolské vzdelanie. Nemusí však overovať študentom poskytnuté informácie v životopise o brigáde počas letných mesiacov.

2.4.2.1.5 Zásada minimalizácie uchovávania údajov

Zásada minimalizácie údajov podľa článku 5 ods. 1 písm. e) GDPR reflektuje požiadavku, že osobné údaje sú uchovávané vo forme, ktorá umožňuje identifikáciu dotknutých osôb najviac dovtedy, kým je to potrebné na účely, na ktoré sa osobné údaje spracúvajú. Osobné údaje sa môžu uchovávať dlhšie, pokiaľ sa budú spracúvať výlučne na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely (v súlade s článkom 89 ods. 1 GDPR) za predpokladu prijatia primeraných technických a organizačných opatrení. Predmetnú zásadu bližšie vykladá Recitál 39, v ktorom Nariadenie zvýrazňuje „obdobie, počas ktorého sa tieto osobné údaje uchovávajú, bolo obmedzené na nevyhnutný rozsah" a stanovenie lehoty na „vymazanie alebo pravidelné preskúmanie." Údaje, ktoré už nie sú potrebné a uplynie lehota na ich uchovávanie je potrebné zlikvidovať resp. vymazať. To neplatí v prípadoch, ak prevádzkovateľ prijal primerané bezpečnostné oprávnenia za účelom uchovania údajov na štatistický, vedecký alebo historický výskum, prípadne na účely archivácie vo verejnom záujme. Doby uchovávania v niektorých prípadoch určujú aj osobitné právne predpisy. Napríklad Zákonník Práce ustanovuje doby pre uchovávanie spisu zamestnanca. Doba uchovávania môže byť určená číselne alebo slovne (počas trvania zmluvy, pokým neuplynie premlčacia doba a podobne).

2.4.2.1.6 Zásada integrity a dôvernosti (bezpečnosť)

Článok 5 ods. 1 písm. f) upravuje zásadu bezpečnosti a integrity, ktorá znamená, že osobné údaje musia byť spracúvané spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení. Táto zásada sa nevzťahuje len na vonkajšie hrozby narušenia bezpečnosti (únik údajov spôsobený hackermi alebo krádež počítača z ambulancie, v ktorom sú uložené údaje o pacientoch), ale aj v rámci vnútornej štruktúry prevádzkovateľa (nedostatočne vyškolených zamestnancov). Bezpečnosť spracovateľských

operácií by mala byť predovšetkým zaručená prostredníctvom rôznych technických a organizačných opatrení ako napr. obmedzeným prístupom k údajom (autorizovaním konkrétnych osôb), konkrétnymi povereniami autorizovaných osôb, ktorí môžu pracovať s osobnými údajmi a implementáciou režimu obnovenia dát v prípade omylu alebo straty. Na bezpečnosť spracúvania osobných údajov nadväzujú predovšetkým dva inštitúty GDPR a to:

- Článok 32 GDPR (bezpečnosť spracúvania osobných údajov), ktorý ustanovuje, že prevádzkovatelia by mali prijať primerané bezpečnostné opatrenia so zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb;
- Nahlasovanie porušení ochrany osobných údajov v zmysle článkov 33 a 34 GDPR – prevádzkovatelia majú povinnosť nahlasovať bezpečnostné incidenty s charakterom porušenia ochrany osobných údajov dozornému orgánu prípadne dotknutým osobám podľa závažnosti incidentu a rizika.[172]

2.4.2.1.7 Zásada zodpovednosti

Zásada zodpovednosti je v GDPR koncipovaná veľmi stručne, napriek tomu v sebe subsumuje niekoľko povinností, na ktoré poukážeme. Podľa článku 5 ods. 2 je prevádzkovateľ zodpovedný za súlad s vyššie uvedenými zásadami a musí vedieť tento súlad preukázať. Na základe usmernenia Pracovnej skupiny čl. 29[173] zásadu zodpovednosti tvorí (i) aktívna a preventívna činnosť prevádzkovateľov (zavedenie opatrení, ktoré zaručia dodržiavanie pravidiel a politík ochrany osobných údajov) a dokumentárna/záznamová činnosť prevádzkovateľov (príprava dokumentov, ktoré preukazujú súlad s pravidlami ochrany osobných údajov).

GDPR reflektuje zásadu zodpovednosti vo viacerých inštitútoch. Niektoré z nich si dovolíme spomenúť a stručne charakterizovať nižšie.

- Špecificky navrhnutá a štandardná ochrana osobných údajov v zmysle článku 25 GDPR – ide o novú povinnosť v zmysle legislatívy na ochranu osobných údajov, ktorá znamená, že ochrana osobných údajov musí byť braná do úvahy už pred

[172] K tomu pozri článok 33 GDPR a článok 34 GDPR.
[173] Article 29 Data Protection Working Party Opinion 03/2010 on the principle of accountability, s. 9.

spracúvaním osobných údajov a osobitne pri tvorbe nových tovarov a služieb pracujúcich s dátami;[174]

- Vedenie záznamov o spracovateľských operáciách v zmysle článku 30 GDPR – prevádzkovatelia a sprostredkovatelia sú povinní viesť dokumenty, v ktorých detailne mapujú na aké účely osobné údaje spracúvajú, o akých osobách, kto k nim má prístup a podobne.;[175]
- Posúdenie vplyvu na ochranu údajov podľa článku 35 GDPR – ide o nový inštitút, ktorého cieľom je nahradiť reportovanie a notifikačné povinnosti dozorným orgánom, v rámci ktorého má prevádzkovateľ vykonať analýzu rizík pri spracúvaním osobných údajov, ktoré môže predstavovať riziko pre práva, slobody a záujmy dotknutých osôb;[176]
- Dezignovanie zodpovednej osoby podľa článkov 36-39 GDPR – v určitých prípadoch stanovených nariadením sú prevádzkovatelia povinní ustanoviť zodpovednú osobu, ktorej úlohou je monitorovanie, poradenstvo či figurovať ako kontaktný bod pre vonkajší svet v oblasti ochrany osobných údajov.[177]

[174] K tomuto inštitútu pozri viac článok 25 GDPR alebo MESARČÍK, M. : Naozaj sa bojím tmy? Naozaj sa bojím tmy? Zopár úvah o technologickom determinizme v kontexte ochrany osobných údajov. In Acta Facultatis Iuridicae Universitatis Comenianae. - Roč. 36, č. 2 (2017), s. 204-217.
[175] Pozri viac článok 30 GDPR.
[176] Pozri článok 35 GDPR prípadne HUDECOVA, I. – CYPRICHOVÁ, A. – MAKATURA, I. : Nariadenie o ochrane fyzických osôb pri spracúvaní osobných údajov/GDPR. Eurokódex: Žilina, 2018, s. 302-306.
[177] K tomu články 36-39 GDPR.

ZOZNAM POUŽITEJ LITERATÚRY

Literatúra

1) BERTHOTY, J. a kol. : Všeobecné nariadenie o ochrane osobných údajov. C.H. Beck. Praha, 2018;
2) BRKAN, M. - PSYCHOGIOPULOU, E. : Courts, Privacy and Data Protection in the Digital Environment. Amsterdam : Edward Elgar Pub, 2017;
3) FUSTER, G. : The Emergence of Personal Data Protection as a Fundamental Right of the EU. Springer. New York, 2014;
4) HUDECOVA, I. – CYPRICHOVÁ, A. – MAKATURA, I. : Nariadenie o ochrane fyzických osôb pri spracúvaní osobných údajov/GDPR. Eurokódex: Žilina, 2018, s. 302-306.

Časopisy

5) ANDRAŠKO, J. : Elektronický občiansky preukaz a iné spôsoby autentifikácie pri prístupe k elektronickým službám verejnej správy. In QUAERE 2017, roč. 7. Hradec Králové : Magnanimitas, 2017;
6) GREENLEAF, G. : Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories. In Journal of Law, Information & Science. Special issue from the Asian Privacy Scholars Network Conference. December 2012;
7) LIGASOVÁ, Z. - RALBOVSKÁ – SOPÚCHOVÁ, S. : Je e-Government dostupný pre všetkých občanov? In MMK 2018: recenzovaný sborník příspěvků. - : 1. vyd. Hradec Králové : Magnanimitas akademické sdružení, 2018;
8) MESARČÍK, M. : Naozaj sa bojím tmy? Naozaj sa bojím tmy? Zopár úvah o technologickom determinizme v kontexte ochrany osobných údajov. In Acta Facultatis Iuridicae Universitatis Comenianae. - Roč. 36, č. 2 (2017), s. 204-217.

Právne predpisy

9) Smernica Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov, Úradný vestník L 281 , 23/11/1995 S. 0031 – 0050;
10) Nariadenie Európskeho parlamentu a Rady (EÚ) 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). Ú.v. EÚL 119, 4.5.2016, p. 1–88;

11) Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 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 a o zrušení rámcového rozhodnutia Rady 2008/977/SVV. Ú. v. EÚ L 119, 4.5.2016, s. 89 – 131;
12) Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES. Ú. v. EÚ L 295, 21.11.2018, s. 39 – 98;
13) Charta základných práv Európskej únie. Ú. v. EÚ C 326, 26.10.2012, s. 391 – 407;
14) 460/1992 Zb. Ústava Slovenskej republiky.

Judikatúra

15) ESĽP, Niemitz proti Nemecku (sťažnosť č. 13710/88), 16 December 1992;
16) ESĽP, Satakunnan Markkinapörssi Oy and Satamedia Oy proti Fínsku, sťažnosť č. 931/13, 27. jún 2017;
17) SDEÚ, C-582/14 Patrick Breyer proti Bundesrepublik Deutschland;
18) SDEÚ,C-101/01- Lindqvist;
19) SDEÚ,C-212/13-Ryneš;
20) SDEÚ,C-131/12-Google Spain and Google alebo C-230/14-Weltimmo;
21) SDEÚ,C-585/08 - Pammer a Hotel Alpenhof;

Iné zdroje

22) Article 29 Data Protection Working Party Opinion 03/2013 on purpose limitation;
23) Article 29 Data Protection Working Party Opinion 03/2010 on the principle of accountability;
24) Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108) regarding supervisory authorities and transborder data flows, Strasbourg, 8.11.2001;
25) European Court of Human Rights: Guide on Article 8 of the European Convention on Human Rights. Right to respect for private and family life, home and correspondence.

26) https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (dostupné 29.10.2019);
27) https://dataprotection.gov.sk/uoou/sk/content/kedy-nariadenie-kedy-zakon-o-ochrane-osobnych-udajov (dostupné 29.10.2019).

KAPITOLA 3 ELEKTRONICKÁ IDENTITA, IDENTIFIKÁCIA A AUTENTIFIKÁCIA

3.1 Základy elektronickej identity, identifikácie a autentifikácie

V tejto časti učebnice sa najskôr budeme venovať problematike identity vo všeobecnosti a následne upriamime našu pozornosť na elektronickú identitu. Taktiež ozrejmíme teoretické východiská pojmov ako identifikácia, autentifikácia, autorizácia a úrovne záruky. V kontexte identifikácie a autentifikácie taktiež dôjde k objasneniu problematiky elektronického podpisu a jeho vytvorenia, ako aj infraštruktúry verejného kľúča.

3.1.1 Identita[178]

Identita, ako koncept, bola predmetom skúmania viacerých vedných disciplín. V sociológii sa identita spája s členstvom v určitej skupine (napr. rodina, zamestnanie a i.).[179] Koncept identity sa taktiež objavuje vo filozofii. V porovnaní so sociologickým chápaním identity, sa môže identita z filozofického hľadiska týkať nielen jednotlivcov, ale aj objektov, resp. vecí.[180] Z psychologického hľadiska identita znamená spôsob, akým osoba vníma samú seba, ale taktiež ako je vnímaná a ako je zastúpená.[181] Nakoniec z právneho hľadiska je koncept identity spájaný najmä s problematikou občianstva, ochrany osobných údajov, súkromia, bezpečnosti a pod.

---

[178] Etymologicky má slovo identita pôvod v latinskom slove *idem*, čo znamená ten istý.

[179] Hlavní predstavitelia sociologických teórií identity sú George Herbert Mead, Erving Goffman, a Anthony Giddens. Bližšie pozri ROOSENDAAL, A.: *Digital personae and profiles in law: Protecting individuals' rights in online contexts.* Oisterwijk: Wolf Legal Publishers, 2013, s. 20 - 25.

[180] Vo filozofii existuje viacero teórií týkajúcich sa identity. Napr. francúzsky filozof Ricoeur rozlišuje medzi *ipse* identitou a *idem* identitou. *Ipse* identita hovorí o tom, kým osoba skutočne je. Nakoľko má dynamický charakter, je neurčitá a mení sa. *Idem* identita je skôr statická a vyznačuje sa jednotvárnosťou, hoci môže dôjsť k jej modifikácii. Takýto pohľad na identitu sa spája s identifikátorom, nakoľko sa v prípade *idem* identity pýtame na to, čo je nemenné (*idem*) v prípade konkrétnej osoby z perspektívy tretej strany. Na druhej strane, *ipse* identita sa týka identity v zmysle samého seba (z pohľadu samého seba). Bližšie pozri VAN DER HOF, S. a kol.: *Framing Citizen's Identities: The construction of personal identities in new modes of government in the Netherlands.* Nijmegen: Wolf Legal Publishers, 2010, s. 16.

[181] V psychológii vzniklo v súvislosti s problematikou identity viacero teórií. Napr. Andre Durand vo svojej knihe *Three Tiers of Identity* rozdelil identitu do troch kategórií, resp. stupňov. Prvý, najnižší stupeň, predstavuje osobná identita. Táto identita je tvorená atribútmi a znakmi, ktoré sú spojené s danou osobou a sú večne platné a nepodmienené. Taktiež platí, že osobná identita patrí a je kontrolovaná jedine danou osobou. Druhú úroveň predstavuje spoločná identita, ktorú tvoria atribúty, ktoré boli priradené osobe inými osobami. Táto identita sa týka konkrétneho vzťahu (napr. obchodný vzťah) a atribúty sú In dočasne priradené osobe. Napr. kreditná karta, knižničná karta obsahujú informácie o identite, ktoré sú priradené konkrétnej osobe. V prípade, ak vzťah, ktorý definuje identitu, zanikne (napr. vypršanie platnosti karty), atribúty nie sú ďalej použiteľné. Najvyššiu úroveň predstavuje abstraktná identita, ktorú tvoria skupiny identity a týka sa najmä marketingu. Napr. zákazník patrí do strednej vrstvy, stredného veku, má auto, hrá futbal a býva v jednom z miest na západnom pobreží. Všetky tieto skupiny identifikujú osobu, ale abstraktne. Bližšie pozri WINDLEY, P. J.: *Digital Identity: Unmasking Identity Management Architecture (IMA).* California: O'Reilly Media, Inc., 2005, s. 12-13. Taktiež pozri RANNENBERG, K. a kol.: *The future of Identity in the Information Society. Challenges and Opportunities.* Springer: London Heidelberg New York Dordrecht, 2009, s. 40-41.

Problematika identity je taktiež predmetom manažmentu informačnej bezpečnosti. V súvislosti s pojmom identita platí, že každá entita[182] sa vyznačuje charakteristickými znakmi, tzv. atribútmi. Napríklad fyzická osoba je charakterizovaná výškou, vekom, výzorom, váhou, DNA, dátumom a miestom narodenia, bydliskom alebo zamestnaním. Súbor týchto atribútov danej entity, ktorý nám umožňuje odlíšiť jednu entitu od druhej, sa nazýva úplná identita.[183] Niektoré atribúty majú statický charakter, čiže sa nemenia (napr. miesto narodenia, DNA a i.), iné majú zas dynamický charakter a časom sa môžu meniť (napr. farba vlasov, trvalý pobyt a i.).

V praktických situáciách nepotrebujeme odlišovať entity rovnakého typu, ale len tie, ktoré by sme si mohli zameniť (napr. fyzické osoby). Z uvedeného dôvodu definujeme oblasť pôsobnosti identity a požiadavku na rozlišovanie akýchkoľvek entít (toho istého druhu). Aby sme mohli entity od seba odlíšiť, bez toho aby sme poznali všetky atribúty, čo nie je ani možné, umelo vytvárame **identifikátory**.[184] Identifikátor by sme mohli definovať ako atribút alebo súbor atribútov entity, ktoré jednoznačne identifikujú entitu v rámci konkrétnej oblasti pôsobnosti.[185] Roosendaal charakterizoval identifikátor ako: *„súbor atribútov ktorý odlišuje jednotlivca v rámci skupiny."*[186] Príkladom takýchto identifikátorov pri fyzických osobách je rodné číslo a v komplexnejšom ponímaní verejné listiny ako občiansky preukaz, alebo rodný list.[187]

McLoughlin chápe identitu ako výsledok spojenia viacerých atribútov, ktorými sa osoby prejavujú vo fyzickom svete, ktoré môžu byť zaznamenané (napr. miesto a čas narodenia, pohlavie, podpis a i.) a zároveň sú spojené s konkrétnou osobou. V tomto zmysle možno identitu chápať ako prostriedok, prostredníctvom ktorého sú jednotlivci rozpoznaní alebo odlíšení od iných jednotlivcov pre transakčné alebo podobné účely.[188]

---

[182] Entitou môže byť čokoľvek, človek, zviera, vec, organizácia, dokument, ale aj nehmotný objekt ako myšlienka. Pre potreby učebnice sa zameriavame na fyzické osoby, fyzické osoby podnikateľov a právnické osoby. V súvislosti s využívaním elektronických služieb verejnej správy sa venujeme najmä fyzickým osobám.

[183] Pfitzmann a Hansen definujú aj čiastkovú identitu (*partial identity*). Táto identita predstavuje podmnožinu atribútov úplnej identity. Na základe týchto atribútov nemusí dôjsť k jednoznačnej identifikácii danej osoby. Bližšie pozri PFITZMANN, A. a HANSEN, M.: *Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology,* 2005. Dostupné na: https://www.freehaven.net/anonbib/cache/terminology.pdf.

[184] Všetky atribúty tvoriace úplnú identitu osoby pozná len samotná osoba.

[185] GRAUX, H. a kol.: *Eid interoperability for pegs—update of country profiles—analysis and assessment report.* 2009, s. 7. Dostupné na: http://ec.europa.eu/idabc/servlets/Doc2ba1.pdf?id=32521.

[186] ROOSENDAAL, A.: *Digital personae and profiles in law: Protecting individuals' rights in online contexts.* Oisterwijk: Wolf Legal Publishers, 2013, s. 19.

[187] OLEJÁR, D. a kol.: *Manažment informačnej bezpečnosti a základy PKI.* Bratislava, 2015. s. 13. Dostupné na: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html.

[188] MCLOUGHLIN, I. a kol.: *Digital Government at Work. A social Informarics Perspective.* Oxford: Oxford University Press, 2013, s. 93.

Z vyššie uvedeného je zrejmé, že koncept identity sa líši v závislosti od oblasti, ktorej sa týka. Pre potreby učebnice vychádzame najmä z pohľadu manažmentu informačnej bezpečnosti, nakoľko mnohé pojmy z tejto oblasti boli prevzaté do legislatívy týkajúcej sa identity a inštitútov s ňou súvisiacou.

Je však otázne ako sa prejavuje identita danej osoby v interakciách s inými subjektmi vo virtuálnom priestore. Pôjde o tú istú identitu alebo možno povedať, že fyzická osoba má viacero identít? Odpoveď na tieto otázky nám dáva pojem elektronická identita.

3.1.2 Elektronická identita

Vo fyzickom svete vystupuje osoba pod jednou identitou, resp. môže vystupovať anonymne. Vo virtuálnom priestore je situácia iná, nakoľko možno hovoriť o viacerých identitách tej istej osoby. Problematika elektronickej identity v akademickom prostredí predstavuje najmä debatu o pôvode ľudskej identity a jej premenách v informačnej spoločnosti. Z právneho hľadiska je problematika elektronickej identity spájaná najmä s otázkami týkajúcimi sa zodpovednosti, ochrany súkromia, ochrany osobných údajov, etiky a morálky. Taktiež sú veľmi dôležité otázky týkajúce sa anonymity a súkromia, kedy právo dovoľuje anonymitu vo virtuálnom priestore, kedy ju prikazuje a kedy zas vyžaduje identifikáciu a autentifikáciu. Na tomto mieste je potrebné uviesť, že konanie rôznych entít, ako sú fyzické osoby, fyzické osoby podnikatelia alebo právnické osoby vo virtuálnom priestore, môže mať právne následky aj vo fyzickom svete. V tejto súvislosti je vo vzťahu k elektronickým službám verejnej správy potrebné, aby poskytovateľ elektronickej služby verejnej správy mal istotu, s kým komunikuje.

Vo väčšine prípadov, ak neberieme do úvahy elektronické služby, kde je dovolený aj anonymný prístup, existuje podmienka identifikovať sa, aby daná osoba mala prístup a mohla využívať konkrétnu službu.

Odkedy sa Internet, konkrétne jeho služba WWW začala používať ako prostriedok komunikácie v oblasti obchodu, neskôr aj vo verejnej správe, vznikli úvahy o identite a jej podobe vo virtuálnom priestore. V odbornej literatúre sa môžeme okrem pojmu elektronická identita stretnúť aj s jeho synonymami, konkrétne digitálnou identitou a virtuálnou identitou.

Van Der Hof definuje digitálnu identitu ako: *„súbor atribútov predstavujúcich entitu v digitálnom prostredí, ktorá má odlišnú a nezávislú existenciu."*[189]

Podľa Laurenta a Bozefrana predstavuje digitálna identita súbor digitálnych údajov, ktoré reprezentujú entitu vo virtuálnom svete (Internet, informačné systémy a pod.). Títo autori zastávajú názor, že fyzická osoba si môže vytvárať viacero digitálnych identít, ktoré s ňou korešpondujú, tak aby mohla rozčleniť svoje aktivity v rôznych oblastiach (napr. člen rodiny, zákazník, predávajúci, zamestnanec a pod.). Laurent a Bozefrane chápu digitálne údaje, ktoré tvoria digitálnu identitu ako atribúty. Tie atribúty, ktoré možno použiť pre jednoznačnú identifikáciu, nazývajú identifikátory.[190]

Cameron definuje digitálnu identitu ako: *„súbor tvrdení urobených digitálnym subjektom o ňom samom alebo o inom digitálnom subjekte."*[191]

Podľa Sullivanovej, ktorá zastáva anglo-americký pohľad na koncepciu identity, predstavuje otázka digitálnej identity právny koncept, podľa ktorého je digitálna identita identitou jednotlivca a tvoria ju informácie, ktoré sú uchovávané a prenášané v digitálnej forme."[192] Inými slovami možno povedať, že digitálna identita predstavuje všetky informácie, ktoré sú digitálne zaznamenané o konkrétnej osobe.[193]

Andrade pri definovaní elektronickej identity využíva analógiu s identitou vo fyzickom svete, ktorá je tvorená atribútmi ako meno, váha, dátum narodenia a i. Podstatné je, že tieto atribúty sú spojené s konkrétnou osobou. Elektronická identita je identitou len vtedy, keď je uznaná verejným sektorom alebo súkromným sektorom ako dostačujúca náhrada za (fyzickú) identitu. Takáto situácia je zrejmá, ak sa jedna strana (napr. verejná

---

[189] VAN DER HOF, S. a kol.: *Framing Citizen's Identities: The construction of personal identities in new modes of government in the Netherlands*. Nijmegen: Wolf Legal Publishers, 2010, s. 21.

[190] LAURENT, M. a BOUZEFRANE, S.: *Digital Identity Management*. London: ISTE Press Ltd., 2015, s. 33.

[191] CAMERON, K.: *The laws of identity*. Microsoft Corporation, 2005, s. 4. Dostupné na: http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.

[192] SULLIVAN, C.: *Protecting digital identity in the cloud: Regulating cross border data disclosure*. *In* Computer Law & Security Review, 2014, roč. 30, č. 2, s. 139.

[193] Sullivan skúma digitálnu identitu v transakčnom kontexte, kedy aj v rámci elektronickej verejnej správy dochádza k transakciám medzi osobami a verejnou správou. Sullivan v rámci informácií, ktoré tvoria digitálnu identitu, rozlišuje medzi tzv. transakčnými informáciami, a tými ostatnými. Transakčné informácie sú skôr statické a týkajú sa informácií, ktoré vznikli narodením. Ide, napr. o meno, pohlavie, dátum narodenia, miesto narodenia. Tieto informácie tvoria tzv. transakčnú identitu. Ostatné informácie predstavujú väčšiu množinu informácií v rámci digitálnej identity. Sú viac dynamické, nakoľko časom dochádza k ich zmene. Taktiež platí, že ostatné informácie predstavujú osobné informácie, ktoré sú spojené s osobou prostredníctvom transakčnej identity. Transakčná identita spája digitálnu identitu s osobou prostredníctvom identifikačných údajov, ktoré môžu byť aj číselnými identifikátormi, vlastnoručným podpisom alebo fotografiou tváre. Bližšie pozri SULLIVAN, C.: *Digital identity and mistake*. *In* International Journal of Law and Information Technology, 2012, roč. 20, č. 3, s. 225-226.

správa) snaží overiť prostredníctvom dostupných atribútov, či realizuje transakciu s danou osobou a nie s niekým iným.[194]

V odbornej literatúra sa taktiež spomína koncept digitálnej osoby (*digital personae*). V zmysle tohto konceptu, ktorý založil Roger Clarke, digitálna osoba reprezentuje jednotlivca a je tvorená údajmi, ktorými možno tohto jednotlivca identifikovať. Vytváranie a uchovávanie digitálnej osoby je založené na transakciách, ktoré môžu mať podobu akejkoľvek interakcie medzi jedincom a osobami či technickými zariadeniami.[195] Údaje, ktoré tvoria digitálnu osobu, môžu slúžiť na reprezentovanie čiastkovej identity jednotlivca. V tomto prípade predstavuje čiastková identita podmnožinu atribútov úplnej identity. V súvislosti s čiastkovou identitou je potrebné uviesť, že jednotlivci zverejňujú len informácie, ktoré sú vhodné pre konkrétnu oblasť pôsobnosti.

Z vyššie uvedených definícií je zrejmé, že pohľady na identitu vo virtuálnom priestore sa rôznia. Ako sme mohli vidieť, v odbornej literatúre neexistuje jednotný názor na samotný pojem, ktorý by sa týkal identity vo virtuálnom priestore, ani na jeho význam. Pre účely učebnice budeme používať pojem elektronická identita, ktorý by sme mohli definovať ako: *„súbor atribútov, ktoré sú uchovávané a prenášané v elektronickej forme a jednoznačne odlišujú osobu od iných osôb."* Taktiež musíme poznamenať, že ak hovoríme o atribútoch, máme na mysli atribúty, ktoré sú uznané a rozpoznávané verejnou správou.

Inými slovami možno povedať, že elektronická identita predstavuje prostriedok, prostredníctvom ktorého osoby preukazujú vo virtuálnom priestore, že sú naozaj tou

---

[194] DE ANDRADE, N. N. G. a kol.: *Electronic identity*, *SpringerBriefs in Cybercecurity*. Springer: London Heidelberg New York Dordrecht, 2014, s. 4.
Norberto Nuno Gomes de Andrade v súvislosti s elektronickou identitou poznamenal, že identifikátory majú digitálnu formu a možno ich rozdeliť do dvoch kategórií. Prvú kategóriu tvoria identifikátory, ktoré sú priamo spojené s osobou (napr. meno, adresa, mobilné číslo alebo elektronický podpis.) Druhú kategóriu tvoria identifikátory, ktoré nie sú priamo spojené s osobou (napr. IP adresa). Bližšie pozri DE ANDRADE, N. N. G. a kol.: *Electronic identity*, *SpringerBriefs in Cybercecurity*. Springer: London Heidelberg New York Dordrecht, 2014.

[195] Clarke rozlišuje medzi premietnutou digitálnou osobou a vnútenou digitálnou osobou. Skôr spomenutá digitálna osoba predstavuje obraz danej osoby, ktorý jedinec vyjadruje voči ostatným prostredníctvom údajov (napr. vytvorením si profilu na sociálnej sieti). Takáto digitálna osoba je kontrolovaná osobou, s ktorou je spojená. V prípade neskôr spomenutej digitálnej osoby, je identita osoby prenesená na osobu prostredníctvom údajov z rôznych inštitúcií súkromného alebo verejného sektora. V tomto prípade je digitálna osoba kontrolovaná niekým iným ako osobou, s ktorou je spojená (napr. záznam v registri dlžníkov). Existujú taktiež kombinácie vyššie uvedených kategórií digitálnych osôb. Napr. v prípade elektronických záznamov pacienta, kedy pacient poskytuje údaje o sebe, ale zdravotnícke zariadenie analyzuje údaje o stave pacienta, robí diagnózy a pod. Bližšie pozri CLARKE, R.: *The Digital Persona Concept, Two Decades Later*. 2013. Dostupné na: http://www.rogerclarke.com/ID/DP12.html.
Roosendal vychádzajúc z Clarkovej koncepcie digitálnej osoby definoval digitálnu osobu ako: *„digitálne zastúpenie jednotlivca z fyzického sveta, ktoré môže byť spojené s týmto jednotlivcom z fyzického sveta a obsahuje dostatočné množstvo (relevantných) údajov, v rámci oblasti pôsobnosti a pre účel použitia ako zástupcu jednotlivca."* Bližšie pozri ROOSENDAAL, A.: *Digital personae and profiles in law: Protecting individuals' rights in online contexts*. Oisterwijk: Wolf Legal Publishers, 2013, s. 39-41.

osobou, ktorou tvrdia, že sú. Navyše, elektronická identita umožní osobám odlíšiť sa od iných osôb.[196]

3.1.3 Identifikácia a autentifikácia

Problematika identifikácie a autentifikácie je stará ako ľudstvo samé. Pôvodne fyzické osoby preukazovali svoju totožnosť geografickým názvom svojho miesta narodenia, ako napr. Herakleitos z Efezu. Takáto identifikácia osôb v neskorších dobách, kedy vznikali prvé moderné štáty samozrejme nepostačovala. V dôsledku nárastu obyvateľstva, ako aj migračných tendencií, bolo potrebné identifikovať osoby oficiálnou cestou. K identifikácii všetkých občanov bez výnimky došlo, napr. vo Francúzsku po skončení Francúzskej revolúcie (1799), kedy tamojšie legislatívne orgány mali stanoviť, akým spôsobom sa bude overovať narodenie, uzavretie manželstva a smrť, ako aj ktorý orgán bude o týchto skutočnostiach vydávať príslušné dokumenty a tie aj uchovávať.[197]

Tradičné spôsoby preukazovania identity ako vyslovenie svojho mena a priezviska a preukázanie sa (fyzickým) preukazom totožnosti pred zamestnancom verejnej správy, predkladanie dokumentov, ktoré sú vlastnoručne podpísané alebo opatrené odtlačkom pečiatky, nie sú využiteľné vo virtuálnom priestore.

Vo virtuálnom priestore sa pracuje s informáciou, ktorá nie je viazaná na materiálny nosič (informácia v elektronickej forme) a spracovávanie informácie prebieha do značnej miery automatizovane, kedy fyzické osoby komunikujú navzájom a s verejnou správou na diaľku. V takýchto prípadoch si zamestnanec verejnej správy nemôže porovnať fotografiu v občianskom preukaze s výzorom človeka. Navyše hrozí, že dôjde k vytvoreniu alebo úprave dokumentu, ktorý sa v elektronickej forme nedá odlíšiť od pravého.

Identifikácia a autentifikácia vo fyzickom svete využíva predpoklady, ako fyzická prítomnosť, materiálny subjekt, papierový dokument, svedectvo dôveryhodnej tretej osoby. Avšak tieto predpoklady nie sú splnené vo virtuálnom priestore.

Z uvedeného dôvodu bolo potrebné, s príchodom elektronickej verejnej správy a poskytovaním elektronických služieb verejnej správy, prispôsobiť identifikáciu

[196] Hlavným dôvodom, prečo sa prikláňame k pojmu elektronická identita a nie k pojmu digitálna identita či virtuálna identita, je skutočnosť, že v právnom poriadku Slovenskej republiky, ako aj aktoch EÚ, sa používa pojem elektronická identita.

[197] NOIRIEL, G.: *The identification of the citizen: the birth of republican civil status in France. In* Documenting individual identity, the development of state practices in the modern world. Princeton and Oxford: Princeton University Press, 2001, s. 28.

a autentifikáciu osôb, ale aj manažment identity, tak aby bolo možné spoľahlivo overiť identitu osoby elektronicky a taktiež, aby bolo možné spravovať elektronické identity.

V tejto časti učebnice definujeme základné pojmy problematiky identifikácie a autentifikácie, ktorými sú identifikácia, autentifikácia, úrovne záruky, autorizácia a manažment identity.

3.1.3.1 Identifikácia

Identifikácia osôb má v porovnaní s konceptom identity praktický rozmer. Človek sa počas svojej existencie dostáva do situácií, kedy sa musí identifikovať, aby mohol realizovať rôzne transakcie. Z pohľadu verejnej správy je dôležité, aby poskytovatelia elektronických služieb verejnej správy, čiže orgány verejnej správy vedeli, s kým komunikujú. V porovnaní s fyzickým svetom, kde osoby pri interakcii so zamestnancami verejnej správy preukazujú svoju identitu na základe preukazov totožnosti, je vo virtuálnom priestore situácia iná, nakoľko osoba, ktorá chce využívať konkrétnu elektronickú službu verejnej správy, preukazuje svoju identitu neživým objektom, akými sú informačné systémy.

Clarke definuje identifikáciu ako: *„proces, v rámci ktorého sú spojené údaje s konkrétnou identitou osoby existujúcou vo fyzickom svete, čo je možné zabezpečiť prostredníctvom získania identifikátora."*[198] Inými slovami možno povedať, že identifikácia predstavuje hľadanie údajov, ktoré zodpovedajú konkrétnej identite.

V rámci identifikácie osoba deklaruje svoju identitu. Inými slovami možno povedať, že osoba, ktorá chce, napr. využívať konkrétnu elektronickú službu verejnej správy, realizuje vyhlásenie o identite (*identity claim)*. Takéto vyhlásenie predstavuje deklaratórny akt osoby, ktorá tvrdí, že: *„Ja som ja a tu sú potrebné atribúty a identifikátory, ktoré sú nevyhnutné na overenie, že som, kto tvrdím, že som."*

V praxi môže nastať situácia, že osoba bude tvrdiť, že je danou osobou, avšak takéto vyhlásenie môže byť falošné. Takéto aktivity môžu smerovať ku krádeži identity alebo neoprávnenému prístupu k informačnému systému verejnej správy alebo elektronickej komunikácii. Aby sme mohli overiť takéto vyhlásenie o identite, musí sa osoba preukázať preukazom identity a následne musí dôjsť k autentifikácii.

---

[198] CLARKE, R.: *Identification and Authentication Fundamentals.* 2004. Dostupné na: http://www.rogerclarke.com/DV/IdAuthFundas.html.

3.1.3.2 Autentifikácia

Dlhé obdobie boli postupy autentifikácie pri využívaní a poskytovaní verejných služieb založené na papierovej forme. Prostriedky autentifikácie ako občiansky preukaz, cestovný pas, vodičský preukaz či rodný list boli používané ako oficiálne potvrdenie deklarovanej identity jednotlivca. Tieto dokumenty podliehali fyzickej kontrole. Avšak príchodom nových IKT a poskytovaním elektronických služieb verejnej správy bolo potrebné vytvoriť nové spôsoby autentifikácie, ktoré by bolo možné použiť v situáciách, kedy je potrebné identifikovať a autentifikovať jednotlivca na diaľku.

Aby sme aj vo virtuálnom priestore v rámci rôznych online interakcií dosiahli určitú úroveň záruky, že osoba, ktorá urobila vyhlásenie o identite je naozaj tou osobou, vyžaduje sa od nej, aby sa preukázala preukazom identity[199]. Príkladmi preukazu identity vo fyzickom svete je, napr. občiansky preukaz, cestovný pas alebo vodičský preukaz. Na základe týchto preukazov identity, ktoré boli vydané dôveryhodnou treťou stranou, ktorou je štát, môže osoba urobiť vyhlásenie o identite na základe overených atribútov (napr. vek, adresa trvalého pobytu a i.), ktoré sa v preukaze identity nachádzajú. Preukaz identity by sme mohli vo všeobecnosti definovať ako údaje, ktoré sa používajú na autentifikáciu deklarovanej identity alebo atribútov danej osoby. Inými slovami možno povedať, že preukaz identity predstavuje autentifikátor, prostredníctvom ktorého sa osoby môžu v rámci rôznych transakcií autentifikovať.

Vo virtuálnom priestore, kde dochádza k rôznym interakciám medzi osobami a rôznymi organizáciami, je situácia v porovnaní s fyzickým svetom podobná. Osoba, ktorá uskutočnila vyhlásenie o identite, musí disponovať **preukazom elektronickej identity[200]**, ktorý bude obsahovať údaje o tom, že osoba, ktorá urobila vyhlásenie o identite, je naozaj tou osobou. Príkladom takýchto preukazov elektronickej identity je, napr. heslo, PIN[201], elektronický podpis, digitálny certifikát a i.[202]

---

[199] Z technologického hľadiska možno povedať, že operačný systém alebo aplikácie budú vyžadovať od osoby (užívateľa) dôkaz o tom, že je naozaj tou osobou, ktorou tvrdí, že je. Takýmto dôkazom je preukaz identity. Pojem preukaz identity je prekladom anglického pojmu *credential*.

[200] Ak sa v texte učebnice používa pojem preukaz identity v kontexte poskytovania a využívania elektronických služieb verejnej správy, má sa za to, že ide o preukaz elektronickej identity.

[201] PIN (*Personal Identification Number*) predstavuje osobné identifikačné číslo, ktoré pozostáva z číselného kódu.

[202] Preukazy elektronickej identity môžu byť integrované do autentifikačného tokenu (napr. čipová karta), ale taktiež nemusia (napr. heslo alebo certifikát).

V rámci autentifikačného postupu musí osoba, ktorá deklarovala svoju identitu, dokázať, že skutočne je tou osobou, ktorej identitu deklarovala. Inými slovami ide o potvrdenie deklarovanej identity.

Osoba sa môže autentifikovať rôznymi spôsobmi. V odbornej literatúre možno hovoriť o troch základných prístupoch, ktoré sú založené na tom:

a) čo človek vie (PIN, heslo, rodné priezvisko mamy),

b) čo človek má (certifikát, čipová karta),

c) čo človek je (biometrické charakteristiky[203] ako odtlačok prstov, obraz sietnice, hlas, obraz dúhovky). [204]

Samozrejme, môže dôjsť aj ku kombinácii rôznych spôsobov autentifikácie, napr. elektronický občiansky preukaz v sebe môže obsahovať biometrickú charakteristiku ako obraz tváre, ale aj elektronický čip. Ďalším príkladom je autentifikácia prostredníctvom čipovej karty a následným zadaním PIN kódu. V takýchto prípadoch sa hovorí o viacfaktorovej autentifikácii.[205]

3.1.3.3 Úrovne záruky

Konečný výsledok autentifikácie je binárny, a teda deklarovaná identita bola potvrdená alebo zamietnutá. Avšak v závislosti od sily prostriedkov, ktoré sa používali na overovanie identity, má spoliehajúca sa strana (napr. poskytovateľ elektronických služieb verejnej správy) rôznu mieru istoty, že skutočne ide o tú osobu, ktorá sa identifikovala. Aj slabšie metódy autentifikácie postačujú na bežné účely. Je potrebné, aby sa pri identifikácii a autentifikácii používali metódy primerané účelu, na ktorý sa výsledok identifikácie a autentifikácie použije. Tento koncept je formalizovaný **úrovňou záruky**.

Stanovenie potrebnej úrovne záruky závisí od úrovne rizika, ktoré môže vzniknúť pri interakcii medzi stranami (napr. fyzická osoba – verejná správa). Ak je úroveň záruky nižšia ako úroveň rizika, nedôjde k interakcii medzi stranami. Analogicky, vo fyzickom svete taktiež

---

[203] Použitie biometrie ako prostriedku identifikácie a autentifikácie osôb siaha až do 3. storočia pred Kr. V starovekej Číne boli objavené tabuľky, kde sa popri mene jednotlivcov nachádzal aj odtlačok prstov. Bližšie pozri SUTROP, M. a LAAS-MIKKO, K.: *From Identity Verification to Behaviour Prediction: Ethical Implications to Second Generation Biometrics. In* Review of Policy research, 2012, roč. 29, č. 1, s. 21-22.

[204] OLEJÁR, D. a kol.: *Manažment informačnej bezpečnosti a základy PKI.* Bratislava, 2015. s. 14. Dostupné na: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html.

[205] TODOROV, D.: *Mechanics of Users Identification and Authentication. Fundamentals of Identity Management.* USA: Auerbach Publications, 2007, s. 6.

musíme preukázať svoju identitu alebo niektorý z atribútov, ak je to odôvodnené úrovňou rizika vyplývajúcej z konkrétnej interakcie.

Autentifikačný proces poskytuje určitú úroveň záruky, že osoba je naozaj tou osobou, ktorej identitu deklarovala. Úroveň záruky a vyžadovanie konkrétneho preukazu identity závisí od úrovne rizika spojeného s transakciou alebo interakciou.

Je potrebné podotknúť, že nie všetky interakcie si vyžadujú rovnakú úroveň autentifikácie. Dokonca, pri niektorých interakciách nie je identifikácia a autentifikácia potrebná.

3.1.3.4 Autorizácia

Úspešná identifikácia a autentifikácia je predpokladom autorizácie. Autorizácia predstavuje povolenie konať v súlade s oprávneniami, ktoré danej osobe prislúchajú.[206]

Clarke definoval autorizáciu ako proces pridelenia povolení a privilégií pre vstup do zdrojov a služieb danej organizácie.[207]

Inými slovami možno povedať, že osoba po úspešnej identifikácii a autentifikácii je autorizovaná na prístup ku konkrétnym službám, informáciám alebo môže vykonávať konkrétne transakcie. O tom, aké úkony môže autentifikovaná osoba vykonávať, najčastejšie rozhoduje spoliehajúca sa strana (napr. poskytovateľ elektronickej služby verejnej správy).

3.1.4 Základy elektronického podpisu a PKI

Vznik informačnej spoločnosti a otázka jej úpravy bola spojená s prístupom, ktorý zastával názor, že čo je vo fyzickom svete, malo by byť aj vo virtuálnom priestore. Inými slovami, normy, ktoré sa aplikujú vo fyzickom svete, by sa mali aplikovať aj vo virtuálnom priestore. V súvislosti s týmto prístupom sa namiesto vlastnoručného podpisu začal používať elektronický podpis, ktorý je jeho ekvivalentom vo virtuálnom priestore.

V tejto časti učebnice ozrejmíme problematiku elektronického podpisu a jeho vytvorenia, ako aj infraštruktúru verejného kľúča.

---

[206] OLEJÁR, D. a kol.: *Manažment informačnej bezpečnosti a základy PKI.* Bratislava, 2015. s. 14. Dostupné na: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html.

[207] Vo fyzickom svete by šlo, napr. o situáciu, kedy by zamestnanec mal povolenie na vstup len do konkrétnej budovy z viacerých budov. V kontexte virtuálneho prostredia má osoba, ktorá bola identifikovaná a autentifikovaná, prístup ku konkrétnym údajom a môže vykonávať konkrétne úkony, na ktoré má povolenie. CLARKE, R.: *A Sufficiently Rich Model of (Id)entity, Authentication and Authorisation.* 2010. Dostupné na: http://www.rogerclarke.com/ID/IdModel-1002.html#MAs.

3.1.4.1 Vlastnoručný podpis

Vlastnoručný podpis vytvára vo fyzickom svete človek (fyzická osoba). Z právneho hľadiska ide o prejav vôle a vyjadrenie súhlasu s obsahom podpísaného dokumentu.[208] Z bezpečnostného hľadiska plní vlastnoručný podpis nasledujúce bezpečnostné požiadavky:

a) identifikuje osobu, ktorá dokument podpísala,
b) zaručuje autentickosť (originalitu) dokumentu, aby nedošlo k modifikácii dokumentu po podpise,
c) vyjadruje súhlas podpisovateľa s obsahom dokumentu,
d) nemožno ho preniesť na iný dokument,
e) je nesfalšovateľný, nakoľko vytvoriť ho vie len podpisovateľ a overiť ho dokáže každý.[209]

Ako však zabezpečiť, aby vyššie uvedené bezpečnostné požiadavky vlastnoručného podpisu boli naplnené aj vo virtuálnom priestore v situáciách, kedy sa vyžaduje podpísanie elektronického dokumentu? Odpoveď na túto otázku nám dáva elektronický podpis.

3.1.4.2 Elektronický podpis alebo digitálny podpis?

V odbornej literatúre a technických normách sa možno stretnúť s pojmami elektronický podpis a digitálny podpis. Na tomto mieste by sme radi poukázali na skutočnosť, že nejde o synonymické pojmy a radi by sme ozrejmili ich význam.

Elektronický podpis má viacero foriem. V praxi sa môžeme stretnúť s napísaním mena do elektronického dokumentu, naskenovaním vlastnoručného podpisu a vložením ho do elektronického dokumentu, elektronickým podpisom vytvoreným na podpisový tablet alebo s digitálnym podpisom, ktorý je založený na kryptografii verejného kľúča. V takomto ponímaní predstavuje digitálny podpis špeciálny druh elektronického podpisu. Digitálny podpis je vytvorený súkromným kľúčom za podpory certifikátu verejného kľúča vydaným certifikačnou autoritou (ďalej len „CA").[210]

---

[208] Písomnú formu právneho úkonu tvoria dva pojmové náležitosti. Prvou je písomnosť, ktorá spočíva v tom, že obsah prejavu vôle je zachytený v texte listiny. Druhou pojmovou náležitosťou je podpis konajúcej osoby. Popisom fyzickej osoby je napísanie mena fyzickej osoby jej vlastnou rukou. Z podpísania vlastnou rukou existujú aj výnimky, napr. pomoc pri podpisovaní z dôvodu úrazu, choroby a pod. Podpisom sa završuje písomný právny úkon, a tým vyvoláva zamýšľané právne následky. Podpis danej osoby sa musí javiť ako podpis konkrétnej osoby, nakoľko je potrebné z podpisu identifikovať podpisujúceho.

[209] OLEJÁR, D. a kol.: *Manažment informačnej bezpečnosti a základy PKI*. Bratislava, 2015, s. 108. Dostupné na: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html.

[210] MASON, S.: *Electronic Signatures in Law*. UK: LexisNexis, 2003, s. 78-82.

Avšak v právnych predpisoch národného alebo medzinárodného charakteru sa začal používať pojem elektronický podpis, ktorý predstavuje ekvivalent vlastnoručného podpisu vo virtuálnom priestore. Pre účely učebnice budeme používať pojem elektronický podpis a budeme ho chápať ako právny pojem pre označenie úkonu podpísania a ako ekvivalent vlastnoručného podpisu vo virtuálnom priestore. V prípade, že budeme chcieť poukázať na elektronický podpis založený na kryptografii verejného kľúča, uvedieme v učebnici pojem digitálny podpis.

3.1.4.3 Vytvorenie elektronického podpisu a PKI

Postup vytvorenia elektronického podpisu budeme ilustrovať na nasledujúcom príklade, kde vystupujú dve fyzické osoby, konkrétne Alžbeta a Bernard. Nakoľko ide o postup technického charakteru, založený na asymetrickej kryptografii, nebudeme zachádzať do detailov a pokúsime sa opísať postup vytvorenia elektronického podpisu, čo najjednoduchšie.[211]

Alžbeta by chcela poslať Bernardovi elektronicky podpísaný elektronický dokument[212]. Alžbeta a Bernard majú každý svoju dvojicu kryptografických kľúčov (súkromný kľúč a verejný kľúč). Súkromný kľúč slúži na vytvorenie elektronického podpisu (tzv. podpisový kľúč) a verejný kľúč slúži na overenie správnosti elektronického podpisu (tzv. overovací kľúč). Alžbetin aj Bernardov verejný kľúč sú zverejnené.

Alžbeta pomocou hašovacej funkcie[213] vypočíta hašovaciu hodnotu elektronického dokumentu (tzv. vypočítaná hašovacia hodnota[214]), ktorú zašifruje pomocou svojho súkromného kľúča. Táto hodnota tvorí Alžbetin elektronický podpis dokumentu. Elektronický dokument spolu s pripojeným elektronickým podpisom pošle Alžbeta Bernardovi. Bernard rozšifruje zašifrovanú hašovaciu hodnotu Alžbetiným verejným kľúčom a sám vypočíta hašovaciu hodnotu zaslaného elektronického dokumentu (nepodpísaného).

---

[211] Kryptografia je veda, ktorá sa zaoberá šifrovacími systémami. V modernej kryptografii nastal zlom v roku 1975, kedy Diffie a Hellman použili namiesto jedného kľúča na šifrovanie aj dešifrovanie, dva rôzne kľúče (jeden na šifrovanie, druhý na dešifrovanie). Kľúče mali tú vlastnosť, že jeden z druhého sa nedal jednoducho odvodiť. K histórii kryptografie bližšie pozri DOOLEY, J. F.: *A Brief History of Cryptology and Cryptographic Algorithms*. SpringerBriefs in Computer Science. Springer Science & Business Media, 2013, 99 s. DAVIES, D.: *A Brief History of Cryptography*. *In* Information Security Technical Report, 1997, roč. 2, č. 2, s. 14-17.

[212] Elektronický dokument môžeme vo všeobecnosti definovať ako digitálny objekt, ktorý nie je len ekvivalentom papierového dokumentu vo virtuálnom prostredí, nakoľko môže existovať v rôznych formách ako graf, audio nahrávka, video a pod.

[213] Hašovacia funkcia slúži na prevod vstupného reťazca údajov na krátky výstupný reťazec.

[214] Hašovacia hodnota taktiež známa pod označením digitálny odtlačok (*hash*).

Ak sa obe hašovacie hodnoty zhodujú, považujeme Allžbetin podpis za overený. Ale ako vieme zistiť, že Alžbeta naozaj poslala daný elektronický dokument a aj ho podpísala?

Naša dôvera, že elektronický podpis vytvorila Alžbeta sa zakladá na tom, že z nejakého zdroja máme Alžbetin verejný kľúč. Z uvedeného dôvodu je potrebné spojiť Alžbetin verejný kľúč s jej identitou. Alžbeta vyhľadá dôveryhodnú tretiu osobu, konkrétne CA a požiada ju o vydanie certifikátu verejného kľúča (ďalej len „certifikát"). CA si overí Alžbetinu identitu na základe predložených dokladov, overí si či má k verejnému kľúču aj súkromný kľúč. Následne CA vydá Alžbete potvrdenie, tzv. certifikát, ktorý obsahuje Alžbetino meno a priezvisko, verejný kľúč, dobu platnosti certifikátu a zopár technických údajov a všetky tieto informácie podpíše CA svojím súkromným kľúčom.

Teraz, keď sme už spojili identitu verejného kľúča s jej majiteľom, prebehne vytvorenie elektronického podpisu ako v predchádzajúcom prípade (Alžbeta vypočíta hašovaciu hodnotu elektronického dokumentu, túto hodnotu súkromným kľúčom zašifruje), s tým rozdielom, že k elektronickému dokumentu a elektronickému podpisu pripojí aj certifikát verejného kľúča a celé to pošle Bernardovi. Bernard následne overí podpis CA na certifikáte, overí platnosť certifikátu a potom z neho vyberie Alžbetin verejný kľúč, ktorý použije na overenie jej elektronického podpisu.[215]

Dôveryhodnosť vyššie popísaného postupu je založená na predpokladoch, že CA je spoľahlivá, iba Alžbeta má svoj súkromný kľúč a ten sa nedá odvodiť z verejného kľúča. Z toho vyplýva, že Alžbeta musí chrániť svoj súkromný kľúč a ak by sa ho niekto zmocnil, musí požiadať CA o zrušenie platnosti certifikátu.[216] CA musí viesť zoznam zrušených certifikátov a taktiež vedieť označiť elektronický dokument elektronickou pečiatkou. Elektronická pečiatka predstavuje časový údaj, ktorý dokazuje, že daný elektronický dokument v danom čase existoval.

Takto popísaný systém, ktorý umožňuje automaticky spravovať certifikáty verejných kľúčov sa nazýva infraštruktúra verejného kľúča (ďalej len „PKI").[217] PKI vytvára rámec pre

[215] Súkromný kľúč môže byť uložený, napr. v čipe, kde sa dá aktivovať a používať na podpisovanie, ale nedá sa vybrať z čipu. Verejný kľúč sa môže vybrať z čipu a na čip sa dokonca môže uložiť aj certifikát verejného kľúča.

[216] Súkromný kľúč môže byť uložený v rôznych technických zariadeniach, ako napr. čipová karta alebo USB token. Čipová karta predstavuje plastovú kartu, ktorá ma vo svojom tele elektronický čip. Čipové karty sa delia na kontaktné čipové karty, procesorové čipové karty a bezkontaktné čipové karty. Podskupinou procesorových čipových kariet sú PKI čipové karty, ktoré okrem kryptografických operácií (napr. vytvorenie súkromného a verejného kľúča) vedia vypočítať aj hašovaciu hodnotu. Čipová karta sa k počítaču pripája prostredníctvom čítačky čipovej karty (tzv. terminál).USB token (mini kľúč) sa pripája k počítaču prostredníctvom USB portu. DOSTÁLEK, L. a kol.: *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. 2. aktualizované vydání.* Brno: Computer Press, a. s., 2009, s. 40-49.

[217] Infraštruktúra verejného kľúča z anglického názvu *Public Key Infrastructure.*

vytváranie, uchovávanie, podpisovanie, potvrdenie a zrušenie certifikátov. Vo všeobecnosti možno povedať, že PKI tvorí:

a) **CA**[218] - je dôveryhodná tretia strana, ktorá vydáva, podpisuje a spravuje certifikáty,

b) **registračná autorita** (ďalej len „RA") - je v spojení s CA, overuje identitu žiadateľa o certifikát pred tým ako je vydaný CA,

c) iné subjekty poskytujúce certifikačné služby (napr. vydavateľ časovej pečiatky).[219]

3.1.4.4 Certifikát

Certifikát (verejného kľúča) predstavuje preukaz elektronickej identity, ktorý zakladá identitu osoby (žiadateľa o certifikát) vo virtuálnom priestore. Vo všeobecnosti by sme mohli certifikát definovať ako elektronický dokument, ktorým vydavateľ certifikátu potvrdzuje, že v certifikáte uvedený verejný kľúč patrí osobe, ktorej bol vydaný.[220]

Formát certifikátu je presne definovaný štandardom X.509. V zmysle tohto štandardu sa certifikát skladá z troch častí. Prvou časťou je telo certifikátu, ktoré obsahuje informácie ako identifikátor osoby, ktorej bol certifikát vydaný, verejný kľúč osoby, informácie o dobe platnosti certifikátu, technické údaje potrebné na spracovanie certifikátu a údaje, ktoré upravujú jeho použitie. Druhá časť certifikátu je tvorená identifikátorom algoritmu, ktorý CA ako vydavateľ certifikátu používa na vytvorenie podpisu tela certifikátu. Poslednou časťou je samotný elektronický podpis CA, ktorá certifikát vydala. Tento podpis zabezpečuje autentickosť informácií, ktoré sú v tele certifikátu. V súvislosti s platnosťou certifikátov platí, že certifikáty majú obmedzenú platnosť.[221]

V praxi môže nastať situácia, kedy informácie nachádzajúce sa v certifikáte nebudú aktuálne (napr. smrť osoby, ktorej bol vydaný certifikát) alebo dôjde k odcudzeniu súkromného kľúča. V takýchto prípadoch je potrebné zrušiť platnosť certifikátu, nakoľko môže dôjsť k zneužitiu elektronického podpisu. O tejto skutočnosti upozorní CA ostatné osoby zverejnením zoznamu zrušených certifikátov.[222]

---

[218] Vo všeobecnosti platí, že CA má jedno alebo viac úložísk certifikátov a systém na správu certifikátov (vydávanie, rušenie platnosti).
[219] KHOSROW-POU, M.: *Dictionary of Information Science and Technology*. USA: Idea Group Reference, 2007, s. 77 a 553.
[220] Tamtiež, s. 176.
[221] VACCA, J. R.: *Computer and Information Security Handbook*. USA: Morgan Kaufmann Publishers, 2009, s. 436.
[222] Tamtiež, s. 440.

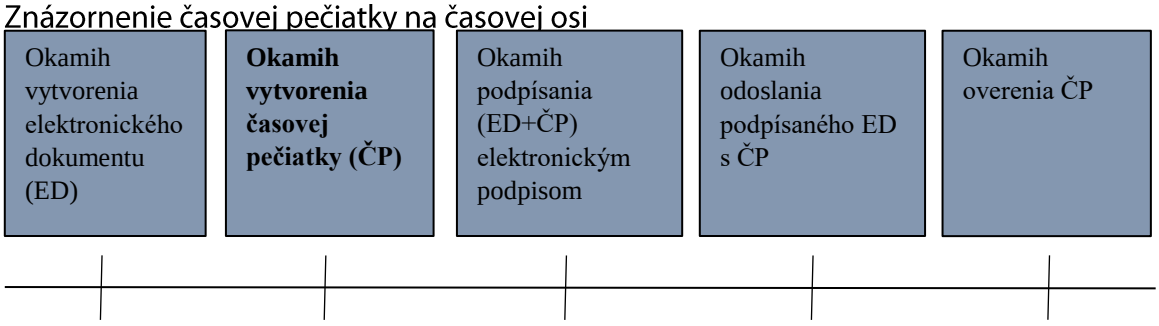
3.1.4.5 Elektronická pečať a elektronická pečiatka

Elektronická pečať z technického hľadiska predstavuje digitálny podpis, avšak plní iný účel ako elektronický podpis. Nakoľko v praxi nastali problémy s uznávaním elektronických podpisov právnických osôb, bola vytvorená obdoba elektronických podpisov s tým rozdielom, že namiesto podpisovateľa sa zaviedol inštitút pôvodcu pečate, ktorým je právnická osoba alebo orgán verejnej moci a je držiteľom súkromného kľúča. Prostredníctvom tohto kľúča je schopný vyhotoviť elektronickú pečať elektronického dokumentu. Používanie elektronickej pečate našlo využitie aj súvislosti s hromadným podpisovaním dokumentov, napr. diplomov, faktúr a i.

Účelom **časovej pečiatky** je dokázanie existencie konkrétneho elektronického dokumentu v konkrétnom čase. Ak sa k elektronickému podpisu pripojila časová pečiatka, tak mohlo byť zabezpečené dôveryhodné určenie času podpísania konkrétneho elektronického dokumentu. Je potrebné uviesť, že časová pečiatka nedokazuje moment vzniku elektronického dokumentu, ale dokazuje jeho existenciu v čase vytvorenia časovej pečiatky. [223]

Časová pečiatka vzniká nasledovne. V prvom rade vznikne elektronický dokument, následne sa k nemu pripojí časový údaj (časová pečiatka). Neskôr sa elektronický dokument spolu s časovým údajom podpíše elektronickým podpisom.

Znázornenie časovej pečiatky na časovej osi



Časová os
Zdroj: Vlastné spracovanie

[223] Význam použitia časovej pečiatky na elektronické dokumenty môžeme demonštrovať na situácii, kedy by sme chceli, napr. určiť existenciu vedeckého objavu publikovaného v článku. Určenie priority nášho objavu by nám zaručovala časová pečiatka, ktorá by dokazovala existenciu článku v čase vyhotovenia časovej pečiatky.

3.2 Právna úprava identifikácie a autentifikácie osôb - národná úroveň

3.2.1 Elektronická identita

Orgány verejnej správy pri poskytovaní elektronických služieb musia s určitosťou vedieť, kto žiada o prístup do ich informačných systémov a kto chce využívať elektronickú úradnú komunikáciu. Nakoľko sa v rámci elektronického výkonu verejnej moci koná a rozhoduje o právach, právom chránených záujmoch alebo povinnostiach konkrétnej osoby, je nevyhnutné spoľahlivo zistiť, či identita, ktorú konkrétna osoba deklaruje pri prístupe do informačných systémov verejnej správy alebo pri elektronickej úradnej komunikácii, je skutočne identitou danej osoby.[224]

Problematika **elektronickej identity** osoby je upravená v zákona č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) (ďalej len „Zákon o e-Governmente). V zmysle ustanovenia § 19 ods. 1 Zákona o e-Governmente je elektronickou identitou osoby: *„súbor atribútov, ktoré sú zaznamenateľné v elektronickej podobe a ktoré jednoznačne odlišujú jednu osobu od inej osoby najmä na účely prístupu k informačnému systému alebo na účely elektronickej komunikácie..*" Taktiež platí, že sa elektronická identita deklaruje identifikáciou osoby a overuje sa autentifikáciou osoby.

3.2.2 Identifikácia

Určenie identity konkrétnej osoby možno v zmysle Zákona o e-Governmente rozdeliť do dvoch fáz. Prvou fázou určenia identity osoby je identifikácia. Podstatou identifikácie je, že osoba deklaruje svoju identitu. V zmysle § 3 písm. m) Zákona o e-Governmente možno za identifikáciu považovať*: „deklarovanie identity objektu vrátane osoby, a to najmä pri prístupe k informačnému systému verejnej správy alebo pri elektronickej komunikácii."* Inými slovami možno povedať, že konkrétna osoba deklaruje svoju identitu najmä z dôvodu prístupu k informačnému systému verejnej správy alebo elektronickej komunikácie.

Preukazovanie identity je zabezpečené pomocou **identifikátora osoby**. Pre účely identifikácie využívajú konkrétne osoby rôzne identifikátory.[225] V prípade fyzickej osoby je

[224] Problematika informačných systémov verejnej správy bola upravená zákonom č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov. Predmetný zákon bol zrušený zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov, ktorý nadobudol účinnosť 5. mája 2019.

[225] Pre identifikátory pre orgány verejnej moci a iné osoby pozri § 3 písm. m) Zákona o eGovernmente.

jej identifikátorom rodné číslo[226] v spojení s menom a priezviskom alebo aj iný identifikátor, ak tak ustanoví osobitný predpis.[227] Zavedenie aj iného identifikátora ako je rodné číslo v spojení s menom a priezviskom reflektuje pripravované zmeny týkajúce sa novej koncepcie identifikátorov fyzických osôb.

V súvislosti s identifikátormi fyzickej osoby Zákon o e-Governmente stanovil pre medzisystémovú identifikáciu[228] identifikátor osoby, ktorým je sada atribútov, ak tak ustanoví osobitný predpis.[229]

3.2.3 Autentifikácia

Druhou fázou určenia identity je autentifikácia. V tejto fáze musí osoba, ktorá deklarovala svoju identitu, dokázať, že skutočne je tou osobou, ktorej identitu deklarovala. Inými slovami ide o potvrdenie deklarovanej identity.

Zákon o e-Governmente definuje **autentifikáciu** ako: *„preukazovanie identity identifikovaného objektu, spravidla prostredníctvom autentifikátora..“*[230] V súvislosti so spôsobom autentifikácie, Zákon o e-Governmente stanovil, že na autentifikáciu sa môže použiť len:

a) úradný autentifikátor, ktorým sú občiansky preukaz s elektronickým čipom a bezpečnostný osobný kód alebo doklad o pobyte s elektronickým čipom a bezpečnostný osobný kód,

b) alternatívny autentifikátor, ktorý ustanoví všeobecne záväzný právny predpis,

c) autentifikačný certifikát, ak ide o autentifikáciu pri prístupe k informačnému systému alebo pri elektronickej komunikácii, ktoré súvisia s výkonom verejnej moci, alebo na účely prístupu do elektronickej schránky alebo disponovania s elektronickou schránkou, a to automatizovaným spôsobom, s použitím technického prostriedku alebo programového prostriedku, alebo

---

[226] § 2 zákona Národnej rady Slovenskej republiky č. 301/1995 Z. z. o rodnom čísle.

[227] Ak ide o zahraničnú fyzickú osobu, za jej identifikátor sa považuje číslo, ktoré je obdobné rodnému číslu alebo identifikátor, ktorý je zahraničnej fyzickej osobe pridelený alebo určený na účely jednoznačnej identifikácie v zmysle právneho poriadku štátu, ktorého je štátnym občanom. Takéto obdobné číslo alebo identifikátor zahraničnej osoby musí byť v spojení s jej menom a priezviskom.

[228] O medzisystémovú identifikáciu ide v prípade, ak je potrebné identifikovať osobu, ktorá sa nenachádza vo vnútornom systéme (Slovenskej republiky). Ide o prípady, kedy je potrebné identifikovať, napr. cudzinca, na základe sady atribútov, ktoré obsahuje systém štátu jeho trvalého pobytu.

[229] § 3 ods. písm. n) Zákona o e-Governmente.

[230] § 3 písm. p) Zákona o e-Governmente.

d) prostriedok elektronickej identifikácie vydaný v rámci schémy elektronickej identifikácie, ktorý je uvedený v zozname podľa osobitného predpisu, ak sú splnené podmienky podľa osobitného predpisu.[231]

V prípade úradného autentifikátora a alternatívneho autentifikátora zabezpečuje vykonanie autentifikácie pri prístupe osoby do informačného systému verejnej správy prostredníctvom prístupového miesta autentifikačný modul, a to overením správnosti a platnosti identifikátora osoby a použitého autentifikátora.[232]

Pri autentifikačných certifikátoch a prostriedku elektronickej identifikácii zodpovedá za vykonanie autentifikácie pri prístupe osoby do informačného systému verejnej správy prostredníctvom prístupového miesta správca komunikačnej časti autentifikačného modulu.[233]

Na základe úspešnej autentifikácie, kedy osoba spoľahlivo potvrdila deklarovanú identitu, má táto osoba v zmysle § 19 ods. 8 Zákona o eGovernmente prístup k:

a) elektronickej úradnej komunikácii a
b) prostriedkom a údajom informačného systému prostredníctvom prístupového miesta.[234]

3.2.4 Úradný autentifikátor

Vo všeobecnosti možno povedať, že v podmienkach Slovenskej republiky bola problematika správy elektronických identít vyriešená prenesením tohto procesu na dôveryhodnú tretiu stranu. Takouto dôveryhodnou treťou stranou je Ministerstvo vnútra Slovenskej republiky, ktoré zodpovedá za vydávanie a správu občianskych preukazov s elektronickým čipom a bezpečnostným osobným kódom, tzv. elektronická identifikačná karta (ďalej len „eID karta“). Právny rámec pre eID kartu je tvorený zákonom č. 395/2019 Z. z. o občianskych preukazoch a o zmene a doplnení niektorých zákonov (ďalej len „Zákon o občianskych preukazoch“).

eID karta vznikla implementáciou elektronického čipu do občianskeho preukazu formátu EÚ, ktoré boli vydávané v Slovenskej republike od júla 2008. V Slovenskej republike

[231] K prostriedku elektronickej identifikácii bližšie pozri prechádzajúce state učebnice.
[232] § 19 ods. 5 písm. a) Zákona o eGovernmente.
[233] § 19 ods. 5 písm. a) Zákona o eGovernmente.
[234] Za prostriedok možno považovať, napr. program, prostredníctvom ktorého je možné získať prístup k údajom.

sa eID karta vydáva od decembra 2013 a Ministerstvo vnútra Slovenskej republiky vydalo už viac ako 2 milióny kusov eID karty.[235]

Postup vydávania eID karty je upravený v § 6 a nasl. Zákona o občianskych preukazoch. Okrem možnosti požiadať o vydanie eID karty osobne na okresnom riaditeľstve Policajného zboru, Zákon o občianskych preukazoch umožňuje požiadať o vydanie eID karty aj prostredníctvom portálu Ministerstva vnútra Slovenskej republiky. Táto žiadosť sa vzťahuje len na vydanie občianskeho preukazu z dôvodu uplynutia platnosti občianskeho preukazu alebo po zmene trvalého pobytu na území Slovenskej republiky.[236] Personalizácia eID karty (zápis údajov na eID kartu) sa vykonáva centrálne v Národnom personalizačnom centre Ministerstva vnútra Slovenskej republiky (ďalej len „NPC MV SR").[237]

Elektronický čip, ktorý sa nachádza na zadnej strane eID karty obsahuje údaje, ktoré sú zapísané, alebo ich možno zapísať do občianskeho preukazu okrem údajov v zmysle a § 3 ods. 1 písm. h) a i) Zákona o občianskych preukazoch (podoba tváre občana a podpis občana). Okrem toho, môže elektronický čip eID karty obsahovať až tri druhy certifikátov[238]:

- **kvalifikovaný certifikát** (ACA) – slúži na podpisovanie kvalifikovaným elektronickým podpisom[239],
- **certifikát na podpisovanie** (PCA) – slúži na autorizáciu vybraných procesov formou elektronického podpisu pri komunikácii v rámci poskytovaných elektronických služieb verejnej správy[240],
- **certifikát na šifrovanie** (SCA) – slúži na šifrovanie údajov pre jeho držiteľa v rámci poskytovaných elektronických služieb verejnej správy.

V elektronickom čipe sa môže nachádzať aj súkromný kľúč a verejný kľúč (kryptografické kľúče), ktoré sú nevyhnutné pre vytvorenie, resp. overenie kvalifikovaného elektronického podpisu.

---

[235]Dostupné na: http://www.parlamentnelisty.sk/politika/politici-volicom/Ministerstvo-vnutra-Odovzdavanie-2-milionteho-obcianskeho-preukazu-284090.

[236] § 8b ods. 1 Zákona o občianskych preukazoch.

[237] V NPC MV SR sa realizuje personalizácia dokladov laserovým gravírovaním a atramentovou tlačou, vstupná a výstupná kontrola dokladov, príprava personalizovaných dokladov na distribúciu na jednotné pracoviská v Slovenskej republike, ako aj skladovanie dodaných čistopisov jednotlivých druhov dokladov. NPC MV SR personalizuje okrem občianskych preukazov aj vodičské preukazy a cestovné doklady. Bližšie pozri: MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY: *Informácia o projekte zavádzania dokladov európskeho formátu v SR a zavádzania prvkov biometrie, vrátane vývoja príjmov a výdavkov podľa jednotlivých prvkov realizácie projektu minimálne do roku 2008.* Bratislava, 2006.

[238] DISIG: *Certifikačná politika pre vydávanie certifikátov na eID*, Bratislava, 2016, s. 13. Dostupné na: https://www.slovensko.sk/_img/CMS4/eid/Certifikacna_politika_pre_vydavanie_certifikatov_na_eID.pdf.

[239] Kvalifikovaný certifikát pre elektronický podpis v zmysle čl. 3 bod 15 Nariadenia eIDAS.

[240] Certifikát pre elektronický podpis v zmysle čl. 3 bod 14 Nariadenia eIDAS.

Taktiež platí, že elektronický čip musí spĺňať požiadavky na kvalifikované elektronické zariadenie na vytvorenie elektronického podpisu v zmysle nariadenia EP a Rady 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (ďalej len „Nariadenie eIDAS"), aby ho bolo možné použiť na uchovanie kvalifikovaného certifikátu a vytváranie kvalifikovaného elektronického podpisu.

V súčasnosti na vytvorenie kvalifikovaného elektronického podpisu prostredníctvom eID karty potrebujete:

- elektronický dokument,
- eID kartu,
- súkromný kľúč,
- čítačku čipových kariet kompatibilnú s eID kartou,
- softvér pre prácu s eID kartou,
- aplikáciu pre vytváranie kvalifikovaného elektronického podpisu[241],
- poznať svoj bezpečnostný osobný kód,
- poznať svoj PIN kód pre kvalifikovaný elektronický podpis.

Údaje na elektronickom čipe eID karty je technicky možné prečítať len so súhlasom jej držiteľa zadaním bezpečnostného osobného kódu (ďalej len „BOK") a súčasným priložením eID karty k čítaciemu zariadeniu kariet.[242] Len oprávnení poskytovatelia elektronických služieb (spoliehajúca sa strana) budú môcť požiadať o prečítanie údajov z eID karty. Ktoré z údajov budú z eID karty prečítané a odovzdané poskytovateľovi elektronických služieb je určené a zabezpečené príslušným certifikátom.[243]

V zmysle § 5 ods. 2 Zákona o občianskych preukazoch BOK predstavuje kombináciu 6 číslic. Občan starší ako 15 rokov je povinný zvoliť si BOK pri podaní žiadosti o vydanie občianskeho preukazu. V prípade občanov starších ako 65 rokov platí, že si BOK môžu zvoliť

[241] Takouto aplikáciou je, napr. *D.Signer/XAdES*, ktorá predstavuje certifikovanú aplikácia určenú na vytváranie kvalifikovaného elektronického podpisu vo formáte *XAdES*, ktorý slúži na autorizáciu elektronických podaní a elektronických úradných dokumentov. Aplikácia *D.Signer/XAdES* je certifikovaná NBÚ. Bližšie pozri Aplikácie pre kvalifikovaný elektronický podpis. Dostupné na: https://www.slovensko.sk/sk/na-stiahnutie.

[242] Pre bezpečnosť je veľmi podstatné, aby čítanie kariet bolo kontaktné. Pri bezkontaktnom čítaní je totiž možné prečítať údaje aj zo vzdialenosti niekoľkých metrov (závisí od technológie), a tak by protivník vybavený čítacím zariadením mohol odchytiť údaje, ktoré by občan poskytoval, napr. úradníkovi pri fyzickej návšteve.

[243] Popri BOK zabezpečujú ochranu údajov zapísaných v elektronickom čipe eID karty aj bezpečnostné mechanizmy. Prvým z nich je pasívna autentifikácia, ktorá chráni autenticitu a integritu údajov v čipe. Tento mechanizmus využíva elektronický podpis generovaný vo fáze personalizácie (zápisu údajov) čipu. Druhým bezpečnostným mechanizmom je aktívna autentifikácia, ktorá predstavuje ochranu pred klonovaním čipu (kópia čipu, do ktorej mohol falšovateľ zapísať nezmenené údaje spolu s digitálnym podpisom vyčítaným z eID karty). Dostupné na: http://www.plaut.sk/technologie-a-systemova-integracia/bezpecnost-a-sukromie/bezpecnostne-mechanizmy/m533.

aj neskôr na príslušnom útvare.[244] BOK spolu s eID slúži na potvrdenie totožnosti držiteľa občianskeho preukazu pri elektronickej komunikácii s informačnými systémami orgánov verejnej správy alebo s inými fyzickými osobami alebo právnickými osobami.

S ohľadom na vyššie uvedené skutočnosti možno konštatovať, že nový typ občianskeho preukazu sa spolu s BOK stáva dôveryhodným prostriedkom pre identifikáciu a autentifikáciu osoby vo virtuálnom priestore, a to pomocou osobných údajov, ktoré sú uložené v elektronickom čipe. Táto funkcia je nevyhnutná pri využívaní elektronických služieb, či už v oblasti verejnej správy alebo v súkromnom sektore.

Napriek skutočnosti, že eID karta predstavuje identifikačný a autentifikačný prostriedok pre využívanie elektronických služieb verejnej správy, stále predstavuje aj fyzický doklad totožnosti.

3.2.5 Alternatívny autentifikátor

V zmysle § 22 Zákona o e-Governmente **alternatívny autentifikátor** vydáva a zneplatňuje Ministerstvo vnútra Slovenskej republiky. Alternatívny autentifikátor je možné použiť pre jednotlivé úrovne autentifikácie (úrovne záruky). Detaily o alternatívnom autentifikátore má stanoviť všeobecne záväzný právny predpis.

K 1. marcu 2017 nadobudla účinnosť vyhláška Ministerstva vnútra Slovenskej republiky č. 29/2017 Z. z., ktorou sa ustanovujú podrobnosti o alternatívnom autentifikátore (ďalej len „Vyhláška o alternatívnom autentifikátore“). V zmysle tejto vyhlášky má alternatívny autentifikátor formu karty s elektronickým čipom spolu s bezpečnostným osobným kódom. Alternatívny autentifikátor je určený fyzickým osobám, ktoré nemajú povolený pobyt na území Slovenskej republiky, teda nespĺňajú podmienky vydania elektronického občianskeho preukazu s čipom alebo dokladu o pobyte cudzinca s čipom. Platnosť alternatívneho autentifikátora je obmedzená na 3 roky. O vydanie alternatívneho autentifikátora môže požiadať fyzická osoba, ktorá je:

- štatutárnym orgánom, členom štatutárneho orgánu právnickej osoby so sídlom na území Slovenskej republiky zapísanej v obchodnom registri alebo
- vedúcim jej organizačnej zložky zapísanej v obchodnom registri.

[244] § 5 ods. 1 a 2 Zákona o občianskych preukazoch.

Vyššie uvedeným fyzickým osobám môže byť vydaný alternatívny autentifikátor len v prípade ak nie sú držiteľmi úradného autentifikátora v zmysle § 21 ods. 1 písm. a) Zákona o eGovernemnte.

O vydanie alternatívneho autentifikátora môže v zmysle § 1 ods. 3 Vyhlášky o alternatívnom autentifikátore požiadať aj advokát, hosťujúci euroadvokát a usadený euroadvokát, a to za podmienky, že nie sú držiteľmi autentifikačného prostriedku podľa § 21 Zákona o eGovernmente .

V súvislosti s účelom alternatívneho autentifikátora musíme poznamenať, že v predmetnej vyhláške, ktorá zavádza alternatívny autentifikátor absentuje zmienka o účele jeho použitia. V návrhu tejto vyhlášky bolo jasne stanovené, že alternatívny autentifikátor (vtedy nazývaný ešte dočasný alternatívny autentifikátor) slúži výlučne na prístup a disponovanie s elektronickou schránkou právnickej osoby, ktorej bola zriadená. Takéto ustanovenie v prijatej vyhláške absentuje. Avšak z rôznych zdrojov je zrejmé[245], že účelom zavedenia alternatívneho autentifikátora je vytvoriť podmienky zahraničným štatutárom a po novele Vyhlášky o alternatívnom autentifikátore[246] aj advokátom pre vstup a disponovanie s elektronickou schránkou.

3.2.6 Autentifikačný certifikát[247]

Autentifikačný certifikát je v zmysle § 22a ods. 1 Zákona o e-Governmente definovaný ako: *„elektronický dokument, ktorý preukazuje elektronickú identitu toho, komu bol vydaný.“* Autentifikačný certifikát sa používa na účely identifikácie a autentifikácie, ktoré súvisia s výkonom verejnej moci pri automatizovanom prístupe:

a) k informačnému systému,

b) k elektronickej komunikácii alebo

Taktiež sa využíva na účely automatizovaného prístupu do elektronickej schránky alebo disponovanie s elektronickou schránkou.

---

[245] Pozri, napr. https://www.nases.gov.sk/alternativne-autentifikatory-umoznia-pristup-k-e-schranke-statutarom-bez-pobytu-na-uzemi-slovenska/index.html alebo https://www.slovensko.sk/sk/oznamy/detail/_alternativny-autentifikator-pr.

[246] Vyhláška Ministerstva vnútra Slovenskej republiky č. 239/2019 Z. z. ktorou sa mení a dopĺňa vyhláška Ministerstva vnútra Slovenskej republiky č. 29/2017 Z. z., ktorou sa ustanovujú podrobnosti o alternatívnom autentifikátore.

[247] Problematika autentifikačného certifikátu bola niekedy predmetom Zákona o EP. Zákonom č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov bol inštitút autentifikačného certifikátu integrovaný do Zákona o e-Governmente.

Na účely zabezpečenia identifikácie a autentifikácie s použitím autentifikačného certifikátu vedie správca komunikačnej časti autentifikačného modulu register autentifikačných certifikátov, ktorý je informačným systémom verejnej správy.[248]

Pre účely automatizovaného prístupu a spracúvania, napr. doručených elektronických správ, je pre orgány verejnej moci, ale aj právnické osoby a fyzické osoby podnikateľov vhodné, aby bolo možné na účely autentifikácie osoby použiť aj certifikát, ktorý je vydaný pre informačný systém tejto osoby. Autentifikačný certifikát by mal v praxi uľahčiť identifikáciu a autentifikáciu, ktorá sa vyžaduje, napr. pri prístupe zamestnancov orgánu verejnej moci do informačných systémov verejnej správy na účely plnenia pracovných úloh.

3.2.7 Iný spôsob autentifikácie alebo žiadna autentifikácia

Orgány verejnej moci sú oprávnené zaviesť a používať pre špecializované portály, ktoré spravujú, aj **iný spôsob autentifikácie** osoby ako je autentifikácia prostredníctvom úradného autentifikátora a alternatívneho autentifikátora. V praxi pôjde o prípady, keď sa osoba bude autentifikovať na základe hesla alebo GRID karty[249]. V prípade, ak sa iný pôsob autentifikácie osoby zavedie, je potrebné zabezpečiť možnosť autentifikácie osoby prostredníctvom autentifikátora podľa § 21 ods. 1 Zákona o e-Governmente pre príslušnú alebo vyššiu úroveň záruky v súlade so štandardom elektronických služieb verejnej správy pre úrovne záruky podľa výnosu Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy.[250] V praxi by teda mohla nastať situácia, že zahraničný štatutár sa môže autentifikovať na špecializovaný portál prostredníctvom alternatívneho autentifikátora. Avšak tento alternatívny autentifikátor je určený len na vstup a disponovanie s elektronickou schránkou.

Pri prístupe osoby do informačného systému verejnej správy prostredníctvom prístupového miesta zabezpečuje overením správnosti a platnosti identifikátora osoby a použitého autentifikátora vykonanie autentifikácie správca špecializovaného portálu ak ide o autentifikáciu podľa § 21 ods. 6 Zákona o e-Governmente. Elektronické prostriedky tohto

[248] Správca komunikačnej časti autentifikačného modulu eviduje v registri autentifikačných certifikátov o autentifikačnom certifikáte údaje v zmysle § 22a ods. 3 Zákona o eGovernmente.
[249] GRID karta má rozmery platobnej karty a jednu jej stranu tvorí matica s x stĺpcami a y riadkami obsahujúca číselné kódy v poli matice (tzv. tabuľka kódov). Riadky môžu byť označené napríklad číslicami, stĺpce písmenami. Využívateľ danej služby môže byť pri autentifikácii vyzvaný, aby zadal konkrétny kód z GRID karty, definovaný jeho pozíciou na konkrétnom riadku a stĺpci (napr. kód C3, čiže kód zo stĺpca C a riadku 3).
[250] § 21 ods. 7 Zákona o e-Governmente.

portálu musia zabezpečovať najmenej ten istý rozsah a kvalitu funkcií ako autentifikačný modul.[251]

V zmysle § 19 ods. 8 zákona o e-Governmente je možné vykonávať elektronickú úradnú komunikáciu prostredníctvom prístupového miesta aj **bez autentifikácie** ak to osobitný predpis ustanoví. Taktiež platí, že osoba o ktorej právach, právom chránených záujmoch a povinnostiach orgán verejnej moci pri výkone verejnej moci elektronicky koná alebo vo vzťahu ku ktorým verejnú moc vykonáva, môže mať prístup k prostriedkom a údajom informačného systému prostredníctvom prístupového miesta, aj bez autentifikácie ak to osobitný predpis ustanoví alebo správca informačného systému určí.

3.2.8 Autorizácia

Úspešná identifikácia a autentifikácia je predpokladom autorizácie. Ako už bolo v prvej kapitole spomenuté, autorizácia predstavuje povolenie konať v súlade s oprávneniami, ktoré danej osobe prislúchajú. Avšak v Zákone o e-Governmente sa autorizácia chápe v užšom zmysle, nakoľko sa spája len s autorizáciou úkonu. V zmysle § 3 písm. o) Zákona o e-Governmente sa za autorizáciu úkonu považuje: *„vyjadrenie súhlasu s obsahom právneho úkonu a s vykonaním tohto právneho úkonu."*

V zmysle § 23 ods. 1 Zákona o e-Governmente vykonáva orgán verejnej moci autorizáciu elektronického podania alebo elektronického úradného dokumentu:

a) kvalifikovaným elektronickým podpisom a mandátnym certifikátom[252] s pripojenou kvalifikovanou elektronickou časovou pečiatkou alebo
b) kvalifikovanou elektronickou pečaťou s pripojenou kvalifikovanou elektronickou časovou pečiatkou.[253]

Praktická situácia, kedy môže dôjsť k autorizácii orgánom verejnej moci je vyhotovenie elektronického úradného dokumentu, napr. rozhodnutia. Ak Zákon o e-Governmente alebo osobitný predpis[254] ustanovuje len povinnosť autorizácie bez označenia konkrétnej osoby alebo osoby v konkrétnom postavení, alebo autorizujúcu osobu označuje len všeobecne ako oprávnenú osobu, orgán verejnej moci na autorizáciu

[251] § 19 ods. 5 písm. c) Zákona o eGovernmente.
[252] Problematika mandátnych certifikátov je upravená v zákone zákona č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov. Mandátny certifikát dokazuje, že osoba vykonávajúca autorizáciu koná za alebo v mene orgánu verejnej moci alebo inej osoby, sama je orgánom verejnej moci (notár, súdny exekútor) alebo zastáva funkciu v orgáne verejnej moci (sudca, prokurátor).
[253] § 23 ods. 1 Zákona o e-Governmente.
[254] Napríklad § 47 ods. 5 zákona č. 71/1967 Zb. o správnom konaní (správny poriadok) v znení neskorších predpisov.

použije kvalifikovaný elektronický podpis vyhotovený s použitím mandátneho certifikátu alebo kvalifikovanú elektronickú pečať, ku ktorým sa pripojí kvalifikovaná elektronická časová pečiatka.[255]

Ak zákon o e-Governmente alebo osobitný predpis[256] vyžaduje autorizáciu konkrétnou osobou alebo osobou v konkrétnom postavení, orgán verejnej moci na autorizáciu použije kvalifikovaný elektronický podpis vyhotovený s použitím mandátneho certifikátu, ku ktorému sa pripojí kvalifikovaná elektronická časová pečiatka.[257]

Zákon o e-Governmente upravuje aj situáciu, keď orgán verejnej moci vydáva elektronický úradný dokument, o ktorom vie, že je určený na použitie do zahraničia, alebo ak o to z dôvodu použitia v zahraničí požiada osoba, ktorej sa takýto dokument vydáva. V takýchto prípadoch orgán verejnej moci na autorizáciu použije kvalifikovaný elektronický podpis vyhotovený s použitím mandátneho certifikátu, ku ktorému sa pripojí kvalifikovaná elektronická pečať a kvalifikovaná elektronická časová pečiatka.[258] Predmetné ustanovenie je výsledkom toho, že v zmysle Nariadenia eIDAS má rovnocenné účinky s vlastnoručným podpisom len kvalifikovaný elektronický podpis. V prípade, ak by orgány verejnej moci autorizovali elektronické dokumenty kvalifikovanou elektronickou pečaťou, je pravdepodobné, že by vznikli problémy s uznaním jej právnych účinkov v členských štátoch Európskej únie.

Osoba, ktorá nie je orgánom verejnej moci, vykoná autorizáciu elektronického podania ak sa podľa Zákona o e-Governmente podáva v elektronickej podobe a zákon neustanovuje iný spôsob autorizácie alebo ak je podľa osobitného predpisu náležitosťou podania vlastnoručný podpis:

a) kvalifikovaným elektronickým podpisom alebo kvalifikovanou elektronickou pečaťou,[259]
b) použitím na to určenej funkcie informačného systému prístupového miesta,
c) uznaným spôsobom autorizácie.

V prípade použitia na to určenej funkcie informačného systému prístupového miesta platí, že úroveň záruky musí zodpovedať minimálne úrovni pokročilá v zmysle Nariadenia

[255] § 23 ods. 3 Zákona o e-Governmente.
[256] Napríklad § 222 Civilného sporového poriadku.
[257] § 23 ods. 3 Zákona o e-Governmente.
[258] § 23 ods. 3 Zákona o e-Governmente.
[259] V súvislosti s realizovaním podania v zmysle § 19 ods. 1 Správneho poriadku je stanovené, že v prípade podaní, ktoré boli urobené elektronickými prostriedkami, musí byť takéto podanie podpísané kvalifikovaným elektronickým podpisom, čím je vylúčené použitie kvalifikovanej elektronickej pečate.

eIDAS pri splnení nasledujúcich podmienok v zmysle § 23 ods. 1 písm. b) Zákona o e-Governmente :

- ak sa zabezpečí uvedenie tejto osoby ako odosielateľa elektronickej správy,
- ak sa zabezpečí nemennosť obsahu autorizovaného dokumentu do momentu uloženia v elektronickej schránke adresáta,
- ak sa zabezpečí spojenie autorizovaného dokumentu s identifikátorom osoby odosielateľa a zachovanie väzby medzi nimi,
- ak to osobitný predpis nezakazuje.

Uznané spôsoby autorizácie ustanoví Ministerstvo vnútra Slovenskej republiky všeobecne záväzným právnym predpisom.

V súvislosti s autorizáciou úkonu Zákon o e-Governmente upravuje v § 23 ods. 4 aj **oprávnenie osoby konať za inú osobu alebo v mene inej osoby**. Ak nie je preukázaný opak, na účely elektronickej komunikácie je oprávnenie osoby konať za inú osobu alebo v mene inej osoby preukázané vždy, ak nasledujúcimi spôsobmi[260]:

a) konajúca osoba použije na autorizáciu platný mandátny certifikát, z ktorého vyplýva oprávnenie konať za túto osobu alebo v jej mene a rozsah tohto oprávnenia alebo
b) konajúca osoba použije na autorizáciu prostriedok, ktorý zodpovedá najmenej úrovni záruky vysoká podľa Nariadenia eIDAS a obsahuje identifikátor osoby a z referenčného údaja vyplýva oprávnenie tejto osoby konať za inú osobu alebo v jej mene.

Okrem vyššie uvedených spôsobov sa oprávnenie konať v mene inej osoby, na účely elektronickej komunikácie, preukazuje v zmysle § 23 ods. 5 Zákona o e-Governmente aj:

a) elektronickým dokumentom obsahujúcim jednoznačnú identifikáciu konajúcej osoby, osoby, v mene ktorej je oprávnená konať, a rozsah oprávnenia konať v mene tejto osoby, pričom tento elektronický dokument musí byť autorizovaný:
    1. splnomocniteľom, ak oprávnenie konať vzniká udelením splnomocnenia, alebo
    2. príslušným orgánom verejnej moci, ak oprávnenie konať vzniká rozhodnutím orgánu verejnej moci,

[260] Zatiaľ čo oprávnenie osoby konať za inú osobu predstavuje tzv. nepriame zastúpenie (napríklad v prípade, ak splnomocnenec na základe udelenej plnej moci koná za splnomocniteľa), tak oprávnenie osoby konať v mene inej osoby predstavuje tzv. priame zastúpenie (napríklad v situácii, kedy štatutárny orgán obchodnej spoločnosti koná v rámci výkonu svojej funkcie ako jej štatutárny orgán priamo v mene tejto obchodnej spoločnosti). Bližšie pozri: SMALIK,M. In MAMOJKA, M. Obchodný zákonník 2. zv. : veľký komentár. - Žilina : Eurokódex, 2016, s. 416-443.

b) elektronickým odpisom z informačného systému verejnej správy nie starším ako jeden mesiac, ak sa oprávnenie konať zapisuje podľa Zákona o e-Governmente do informačného systému verejnej správy,

c) identifikátorom osoby, v mene ktorej sa koná, ak konajúca osoba je zákonným zástupcom osoby, v mene ktorej sa koná.

Orgán verejnej moci je povinný zabezpečiť aktuálnu evidenciu údajov preukazujúcich oprávnenie konať v mene inej osoby, o ktorých sa dozvie pri svojej činnosti alebo v súvislosti s ňou, a to spôsobom, ktorý zodpovedá platnému skutkovému a právnemu stavu a ktorý umožní preukázať toto oprávnenie na základe autentifikácie osoby. Evidenciu vedie orgán verejnej moci prostredníctvom centrálneho registra elektronických plnomocenstiev podľa § 23a Zákona o e-Governmente. Takáto evidencia slúži najmä na to, aby nebolo potrebné opätovne preukazovať oprávnenie ku konaniu. V prípade, ak sú tieto oprávnenia hodnotou referenčného údaja alebo vyplývajú z hodnôt referenčných údajov, orgán verejnej moci ich referencuje.[261]

V prípade, ak orgán verejnej moci takéto oprávnenia vo svojom informačnom systéme eviduje[262], nie je oprávnený požadovať od konajúcej osoby preukázanie tohto oprávnenia, ak nemá dôvodnú pochybnosť o tom, či oprávnenie trvá alebo nemá odôvodnenú pochybnosť o jeho rozsahu. Oprávnenie osoby konať v mene inej osoby môže byť aj hodnotou referenčného údaja alebo môže vyplývať z hodnôt referenčných údajov vedených v iných informačných systémoch verejnej správy.[263]

3.2.9 Autentifikačný modul

Osoba, o ktorej právach, právom chránených záujmoch koná orgán verejnej moci elektronickou formou alebo vo vzťahu ku ktorým vykonáva verejnú moc, sa musí pri prístupe k niektorému z **prístupových miest** alebo **spoločného modulu** identifikovať, čiže deklarovať svoju identitu prostredníctvom identifikátora osoby.[264]

[261] § 23 ods. 6 Zákona o e-Governmente.
[262] Oprávnenie osoby konať v mene inej osoby môže byť aj hodnotou referenčného údaja alebo môže vyplývať z hodnôt referenčných údajov vedených v iných informačných systémoch verejnej správy.
[263] § 23 ods. 5 Zákona o e-Governmente.
[264] § 19 ods. 2 Zákona o e-Governmente.

Prístupové miesta[265] a spoločné moduly tvoria spolu s agendovými systémami[266] základnú koncepčnú architektúru informačných systémov pre elektronický výkon verejnej moci. Všetky komponenty architektúry informačných systémov pre elektronický výkon verejnej moci musia byť budované tak, aby prostredníctvom nich bolo možné vykonávať verejnú moc výhradne elektronicky, bez potreby ďalšej listinnej komunikácie, pokiaľ osobitný právny predpis listinnú komunikáciu vyslovene neustanovuje.

Spoločné moduly predstavujú jeden z komponentom architektúry informačných systémov pre elektronický výkon verejnej moci.[267] Je potrebné uviesť, že aj pri prístupe k spoločnému modulu sa osoba, o ktorej právach, právom chránených záujmoch a povinnostiach orgán verejnej moci pri výkone verejnej moci elektronicky koná alebo vo vzťahu, ku ktorým verejnú moc vykonáva, musí identifikovať prostredníctvom identifikátora osoby.

Spoločné moduly predstavujú informačné systémy verejnej správy a zabezpečujú základné funkcie potrebné pri elektronickom výkone verejnej moci. Tieto základné funkcie sú opakovane využívané orgánmi verejnej moci a inými osobami pri vzájomnej elektronickej komunikácii na účely výkonu verejnej moci elektronicky. Medzi takéto funkcie patrí, napr. autentifikácia používateľa, ktorý chce využiť elektronickú službu poskytovanú konkrétnym orgánom verejnej správy alebo funkcia umožňujúca realizáciu elektronickej platby. Nakoľko by nebolo efektívne, aby v každom informačnom systém verejnej správy bola takáto funkcia implementovaná, je vhodnejšie vytvoriť centrálne riešenia, ktoré budú ostatným

[265] K prístupovým miestam pozri prvú kapitolu tejto učebnice.

[266] V zmysle § 4 ods. 4 Zákona o e-Governmente agendové systémy predstavujú informačné systémy verejnej správy v správe orgánov verejnej moci a slúžia na zabezpečenie výkonu verejnej moci v rozsahu pôsobnosti a oprávnení orgánov verejnej moci podľa osobitných predpisov. Inými slovami možno povedať, že zabezpečujú informačnú podporu vlastnému výkonu agend podľa kompetenčného členenia. Sú využívané nielen na podporu elektronického výkonu verejnej moci, ale aj na podporu existujúceho listinného spôsobu výkonu verejnej moci.

[267] V zmysle § 10 ods. 3 Zákona o e-Governmente sú spoločnými modulmi:
„a) modul elektronických schránok,
b) autentifikačný modul,
c) platobný modul,
d) modul centrálnej elektronickej podateľne,
e) modul elektronických formulárov,
f) modul elektronického doručovania,
g) notifikačný modul,
h) modul úradnej komunikácie a
i) modul dlhodobého uchovávania."
Na účely zabezpečenia elektronickej komunikácie cez špecializovaný portál a na prístup a plnenie funkcií jeho agendového systému môžu orgány verejnej moci v zmysle § 10 ods. 13 Zákona o e-Governmente využívať aj ďalšie spoločné moduly, alebo vytvoriť informačné systémy verejnej správy s obdobnou funkcionalitou ako spoločné moduly, samozrejme s výnimkou tých, ktoré sú povinné využívať.

informačným systémom poskytovať tieto funkcie. V prípade, ak sa spoločné moduly delia na časti, sú informačnými systémami verejnej správy aj ich časti.[268]

V súvislosti s identifikáciou a autentifikáciou osôb má osobitné postavenie **autentifikačný modul**, známy taktiež pod označením **modul IAM** (*Identity Access Management*). Tento modul na základe identifikátora osoby a autentifikátora zabezpečuje:

a) autentifikáciu osôb na účely elektronickej komunikácie,
b) využitie elektronickej identity osoby pre všetky prístupové miesta na účely elektronickej komunikácie a
c) prenos informácie o overenej identite.[269]

Autentifikačný modul sa skladá z dvoch častí, ktoré uvádzame v nasledujúcej tabuľke.[270]

Časti autentifikačného modulu

Časť autentifikačného modulu	**Popis**	**Správca časti autentifikačného modulu**
Autentifikačná časť	Určená na autentifikáciu	Ministerstvo vnútra Slovenskej republiky
Komunikačná časť	Určená na prenos informácie o overenej identite	Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu

Zdroj: Vlastné spracovanie

Tento modul predstavuje centralizované riešenie správy identít, ktorý funguje na princípe jedného prihlásenia *(Single Sign-On)*, čo znamená, že používateľ sa po autentifikácii k informačnému systému verejnej správy (napr. portál verejnej správy) nemusí znova autentifikovať pri prístupe k inému informačnému systému verejnej správy. Autentifikačný modul ako jediný vykonáva overenie identity používateľov, čiže ho možno označiť za poskytovateľa identity. Všetky ostatné informačné systémy verejnej správy sú v pozícii poskytovateľov služieb.

Ďalším významným spoločným modulom je **modul elektronických schránok,** ktorý je určený pre správu elektronických schránok a zabezpečenie fungovania elektronických

[268] § 4 ods. 3 Zákona o e-Governmente.
[269] § 10 ods. 5 Zákona o e-Governmente.
[270] § 10 ods. 5 Zákona o e-Governmente.

schránok. Jeho súčasťou je register elektronických schránok. Správcom modulu elektronických schránok je *Úrad vlády Slovenskej republiky*.[271]

Na tomto mieste je potrebné poznamenať, že orgány verejnej moci sú pri výkone verejnej moci elektronicky na zabezpečenie činností, ktoré predmetné moduly zabezpečujú, povinné používať:

- modul elektronických schránok,
- autentifikačný modul,
- modul elektronických formulárov a
- modul elektronického doručovania.[272]

3.3 Právna úprava identifikácie a autentifikácie osôb – úroveň EÚ

3.3.1 Uznávanie elektronických podpisov, elektronických pečatí a elektronických časových pečiatok

Nariadenie eIDAS predstavuje v porovnaní so Smernicou o EP rozsiahlejší akt EÚ. Zatiaľ, čo Smernica o EP upravovala len problematiku elektronického podpisu a certifikačných služieb s ním spojených, Nariadenie eIDAS zachováva prínos Smernice o EP a vytvára rámec upravujúci širší okruh **služieb dôvery**. V zmysle čl. 3 ods. 16 Nariadenia eIDAS ide o elektronické služby, ktoré sa spravidla poskytujú za odplatu a spočívajú:

„a) vo vyhotovovaní, overovaní a validácii elektronických podpisov, elektronických pečatí alebo elektronických časových pečiatok, elektronických doručovacích služieb pre registrované zásielky a certifikátov, ktoré s týmito službami súvisia, alebo

b) vo vyhotovovaní, overovaní a validácii certifikátov pre autentifikáciu webových sídiel, alebo

c) v uchovávaní elektronických podpisov, pečatí alebo certifikátov, ktoré s týmito službami súvisia."[273]

Vytvorenie právneho rámca pre elektronické podpisy, elektronické pečate, elektronické časové pečiatky, elektronické dokumenty[274], elektronické doručovacie služby pre registrované zásielky a certifikačné služby pre autentifikáciu webových sídiel má uľahčiť

[271] § 10 ods. 4 Zákona o e-Governmente.
[272] § 10 ods. 2 Zákona o e-Governmente.
[273] Je potrebné uviesť, že požiadavky Nariadenia eIDAS by mali spĺňať len služby dôvery, ktoré sú poskytované verejnosti a majú vplyv na tretie strany.
[274] Nariadenie eIDAS upravuje problematiku elektronických dokumentov len okrajovo. V zmysle čl. 3 bod 35 Nariadenia eIDAS predstavuje elektronický dokument: *„akýkoľvek obsah uložený v elektronickej forme, najmä text alebo zvukový, obrazový či audiovizuálny záznam."*

jednak fungovania vnútorného trhu, ako aj zabezpečenie dostatočnej úrovne bezpečnosti prostriedkov elektronickej identifikácie a služieb dôvery.[275]

3.3.1.1 Elektronický podpis

Nariadenie eIDAS definuje tri druhy elektronických podpisov podľa úrovne bezpečnosti[276]. Najnižšiu úroveň predstavuje tzv. **obyčajný elektronický podpis**, ktorý je definovaný ako: *„údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným údajom v elektronickej forme a ktoré podpisovateľ používa na podpisovanie."*[277] Za obyčajný elektronický podpis možno považovať v zásade čokoľvek, čo vieme zdigitalizovať (napr. heslo, PIN, obrázok a pod.) a pripojiť k iným údajom (podpisovanému dokumentu).[278]

V súvislosti s vytvorením elektronického podpisu platí, že údaje pre vytváranie elektronického podpisu predstavujú *„jedinečné údaje, ktoré podpisujúca osoba používa na vytvorenie elektronického podpisu."* [279] Pri použití asymetrického šifrovania môžeme za takéto údaje považovať súkromný kľúč.

Vyššiu úroveň bezpečnosti predstavuje **zdokonalený elektronický podpis**. V zmysle Nariadenia eIDAS ide o elektronický podpis, ktorý spĺňa požiadavky podľa článku 26 Nariadenia eIDAS. Prvou požiadavkou je jedinečnosť spojenia zdokonaleného elektronického podpisu s fyzickou osobou, ktorá vyhotovuje elektronický podpis, čiže podpisovateľom.[280] Ďalšou požiadavkou na zdokonalený elektronický podpis je určenie totožnosti podpisovateľa. Zdokonalený elektronický podpis musí taktiež spĺňať požiadavku, aby bol vyhotovený pomocou údajov na vyhotovenie elektronického podpisu, ktoré môže podpisovateľ s vysokou mierou dôveryhodnosti používať pod svojou výlučnou kontrolou. Poslednou požiadavkou je, aby zdokonalený elektronický podpis bol prepojený s údajmi, ktoré sa ním podpisujú, takým spôsobom, že každú dodatočnú zmenu údajov možno zistiť.[281]

Najvyššiu úroveň bezpečnosti predstavuje **kvalifikovaný elektronický podpis.** Tak ako v prípade zdokonaleného elektronického podpisu aj kvalifikovaný elektronický podpis

[275] Čl. 1 Nariadenia eIDAS.
[276] Resp. záruk, ktoré dané riešenie elektronického podpisu poskytuje.
[277] Čl. 3 bod. 10 Nariadenia eIDAS.
[278] Za obyčajný elektronický podpis by sme mohli považovať aj (zdigitalizovaný) hlas. Bližšie pozri: SMEJKAL, V. a KODL, J. a UŘIČAŘ, M..: *Elektronický podpis podle nařízení eIDAS. In* Revue pro právo a technologie, 2015, č. 11, s. 218-219, 228.
[279] Čl. 3 bod 13 Nariadenia eIDAS.
[280] Čl. 3 bod. 9 Nariadenia eIDAS.
[281] Tieto požiadavky sú typické pre elektronické podpisy, ktoré sú všeobecne známe pod názvom digitálne podpisy.

je jedinečne spojený s podpisovateľom. Popri požiadavkách, ktoré musí spĺňať zdokonalený elektronický podpis, musí byť kvalifikovaný elektronický podpis navyše vyhotovený s použitím kvalifikovaného zariadenia na vyhotovenie elektronického podpisu (napr. čipová karta, USB token) a musí byť založený na kvalifikovanom certifikáte pre elektronické podpisy, ktorý vydáva kvalifikovaný poskytovateľ služieb dôvery. Kvalifikovaný elektronický podpis ako najvyššia úroveň elektronického podpisu ponúka najvyššiu mieru záruky v autentickosť elektronického podpisu, čo znamená, že bol vytvorený osobou, ktorej bol vydaný kvalifikovaný certifikát pre elektronický podpis. Bezpečnosť kvalifikovaného elektronického podpisu je zabezpečená prostredníctvom kvalifikovaného zariadenia na vyhotovenie elektronického podpisu.[282]

Pre lepšie pochopenie tohto pojmu je potrebné ozrejmiť pojmy kvalifikované zariadenie na vyhotovenie elektronického podpisu a kvalifikovaný certifikát pre elektronický podpis.

Kvalifikované zariadenie na vyhotovenie elektronického podpisu predstavuje konfigurované programové vybavenie alebo technické zariadenie pre vytváranie elektronických podpisov, ktoré zároveň spĺňa požiadavky, aby:

„a) v primeranej miere bola zaručená dôvernosť údajov na vyhotovenie elektronického podpisu použitých na vyhotovenie elektronického podpisu;

b) sa údaje na vyhotovenie elektronického podpisu použité na vyhotovenie elektronického podpisu mohli v praxi objaviť iba raz;

c) údaje na vyhotovenie elektronického podpisu použité na vyhotovenie elektronického podpisu nebolo možné s primeranou úrovňou zabezpečenia odvodiť a elektronický podpis bol spoľahlivo chránený proti falšovaniu pomocou aktuálne dostupných technológií;

d) oprávnený podpisovateľ mohol údaje na vyhotovenie elektronického podpisu použité na vyhotovenie elektronického podpisu spoľahlivo chrániť pred použitím inými osobami."[283]

---

[282] Obyčajný elektronický podpis a zdokonalený elektronický podpis sú v podstate technologicky neutrálne, čo znamená, že takýmto podpisom by mohol byť napr. aj biometrický podpis. Kvalifikovaný elektronický podpis predstavuje elektronický podpis, ktorý je založený na kvalifikovanom certifikáte verejného kľúča a je vyhotovený pomocou kvalifikovaného zariadenia. Nariadenie eIDAS taktiež počíta s vytvorením kvalifikovaného elektronického podpisu na diaľku, nakoľko v bode 51 preambuly uvádza: *„Podpisovateľ by mal mať možnosť zveriť kvalifikované zariadenia na vyhotovenie elektronického podpisu do starostlivosti tretej strany za predpokladu, že sa zavedú vhodné mechanizmy a postupy, ktorými sa zabezpečí, že podpisovateľ bude mať výlučnú kontrolu nad používaním svojich údajov na vyhotovenie elektronického podpisu a že pri používaní zariadenia budú splnené požiadavky na kvalifikovaný elektronický podpis."* Bližšie o vyhotovovaní elektronického podpisu na diaľku pozri BATĚK, Ľ. a IMRICH, J.: *Vyhotovovanie elektronických podpisov na diaľku. In* Zborník príspevkov z konferencie Informačná bezpečnosť 2017. SASIB, 2017, s. 73-77.

[283] Príloha II Nariadenia eIDAS.

Kvalifikované zariadenie na vyhotovenie elektronického podpisu nesmie meniť údaje, ktoré sa majú podpísať a taktiež nesmie brániť tomu, aby tieto údaje boli podpisovateľovi zobrazené pred podpísaním. Ďalšou podmienkou pre takéto zariadenie je, aby údaje pre vytváranie elektronických podpisov mohli byť v mene podpisovateľa vytvorené alebo spravované len kvalifikovaným poskytovateľom služieb dôvery. Posledná podmienka umožní pri výrobe elektronického preukazu s čipom vytvoriť kvalifikované elektronické podpisy na kvalifikovaných elektronických certifikátoch držiteľa občianskeho preukazu.[284]

Nariadenie eIDAS sa v rámci problematiky kvalifikovaných zariadení na vyhotovenie elektronických podpisov obmedzuje len na hardvér a systémový softvér, ktorý sa používa na správu a ochranu údajov na vyhotovenie elektronických podpisov, ktoré sa tvoria, uchovávajú alebo spracúvajú v zariadení na vyhotovenie podpisov.

Na tomto mieste je potrebné uviesť, že v súvislosti s kvalifikovaným zariadením ide najmä o ochranu súkromných kľúčov, ktoré je možné ľahšie chrániť v špecializovanom technickom zariadení, ako v univerzálnom počítači, kde je reálna hrozba napadnutia, odchytávania údajov z klávesnice, podstrčenia iného dokumentu, ako toho, ktorý človek podpisuje a pod.

V súvislosti s **kvalifikovaným certifikátom pre elektronický podpis** je v prvom rade potrebné ozrejmiť pojem certifikát pre elektronický podpis. V zmysle Nariadenia eIDAS je certifikát definovaný ako *„elektronické osvedčenie, ktoré spája údaje na validáciu elektronického podpisu s fyzickou osobou a potvrdzuje aspoň jej meno alebo pseudonym."*[285]

Kvalifikovaný certifikát pre elektronický podpis musí spĺňať nasledujúce podmienky:

a) musí ísť o certifikát, ktorý vydáva kvalifikovaný poskytovateľ služieb dôvery a

b) musí spĺňať požiadavky stanovené v Nariadení eIDAS.[286]

Ad a) **Kvalifikovaným poskytovateľom služieb dôvery** je fyzická osoba alebo právnická osoba, ktorá poskytuje jednu alebo viacero kvalifikovaných služieb dôvery a ktorému bol udelený kvalifikovaný štatút orgánom dohľadu.[287] Tento štatút udeľuje v podmienkach

[284] Tamtiež.
[285] Čl. 3 bod 14 Nariadenia eIDAS.
[286] Čl. 3 bod 15 Nariadenia eIDAS.
[287] Čl. 3 bod. 19 a 20 Nariadenia eIDAS.

Slovenskej republiky Národný bezpečnostný úrad (ďalej len „NBÚ"), ktorý je orgánom dohľadu v zmysle Nariadenia eIDAS.

Ad b) **Požiadavky na kvalifikovaný certifikát pre elektronický podpis** sú stanovené v prílohe I Nariadenia eIDAS a platí, že musia byť splnené kumulatívne. V prvom rade musia kvalifikované certifikáty obsahovať označenie, aspoň vo formáte, ktorý je vhodný na automatizované spracovanie, že sa certifikát vydáva ako kvalifikovaný certifikát pre elektronický podpis. Ďalšími údajmi, ktoré musí kvalifikovaný certifikát obsahovať, sú údaje, ktoré jednoznačne identifikujú kvalifikovaného poskytovateľa služieb dôvery. Za takýto údaj možno považovať údaj aspoň o členskom štáte EÚ, v ktorom je tento poskytovateľ usadený a ak ide o právnickú osobu, tak aj názov prípadne registračné číslo. V prípade fyzickej osoby sa vyžaduje meno osoby. Kvalifikovaný certifikát musí taktiež obsahovať meno podpisovateľa alebo jeho pseudonym. Použitie pseudonymu musí byť jasne uvedené.

Každý kvalifikovaný certifikát musí taktiež obsahovať údaj o začiatku a konci obdobia jeho platnosti, ako aj identifikačný kód certifikátu, ktorý je jedinečný pre kvalifikovaného poskytovateľa služieb dôvery.

Kvalifikované certifikáty by nemali podliehať žiadnym povinným požiadavkám nad rámec Nariadenia eIDAS, nakoľko uznávanie kvalifikovaných certifikátov spolu s cezhraničnou interoperabilitou predstavujú predpoklady pre cezhraničné uznávanie kvalifikovaných elektronických podpisov. Členským štátom EÚ sa ponechala možnosť začlenenia konkrétnych atribútov do kvalifikovaných certifikátov, akými sú napríklad jedinečné identifikátory[288]. Avšak tieto jedinečné identifikátory nesmú byť prekážkou pre cezhraničnú interoperabilitu ani uznávanie kvalifikovaných certifikátov a elektronických podpisov.[289]

Elektronickému podpisu nesmú byť odopierané **právne účinky** a nesmie byť odmietaný ako **dôkaz v súdnom konaní** iba z toho dôvodu, že má elektronickú podobu, alebo že nespĺňa požiadavky na kvalifikované elektronické podpisy.[290] V tejto súvislosti je potrebné uviesť, že Nariadenie eIDAS spomína len súdne konanie. Vzhľadom na skutočnosť, že elektronický podpis sa používa aj v správnom konaní, zastávame názor, že nemožnosť odmietnutia právnych účinkov elektronického podpisu a jeho prípustnosti ako dôkazu sa

[288] Napr. rodné číslo.
[289] Bod 54 preambuly Nariadenia eIDAS.
[290] Čl. 25 Nariadenia eIDAS. Nemožnosť odoprenia právnych účinkov, ako aj dôkazu pred súdmi z dôvodu elektronickej formy, sa vzťahuje aj na elektronické dokumenty.

vzťahuje aj na konania, kde správny orgán rozhoduje o právach, právom chránených záujmoch a povinnostiach účastníkov správneho konania.[291]

Na tomto mieste je potrebné uviesť, že len **kvalifikovaný elektronický podpis** má **právny účinok rovnocenný s vlastnoručným podpisom**. V zmysle ustanovení Nariadenia eIDAS, ktoré upravujú uznávanie služieb dôvery v rámci celej EÚ, ako aj ich právnych účinkov, možno konštatovať, že vo všetkých členských štátoch EÚ sú s použitím kvalifikovaných elektronických podpisov spájané rovnaké právne účinky, za podmienky, že sú založené na kvalifikovanom certifikáte vydanom kvalifikovaným poskytovateľom služieb dôvery, ktorý sa nachádza v EÚ. Vytvorenie, čo najvhodnejších podmienok pre vzájomné uznávanie predstavuje významný faktor ovplyvňujúci vytvorenie jednotného digitálneho trhu v rámci EÚ.[292]

3.3.1.2 Elektronická pečať

Elektronická pečať je z technického hľadiska digitálny podpis a v porovnaní s elektronickým podpisom plní iný účel. Pri vyhotovení elektronickej pečate neidentifikuje konkrétnu fyzickú osobu, tak ako pri elektronickom podpise. Z uvedeného dôvodu ani vo forme kvalifikovanej elektronickej pečate nemá právne účinky vlastnoručného podpisu ako je to v prípade kvalifikovaného elektronického podpisu.

V zmysle Nariadenia eIDAS je **elektronická pečať** definovaná ako: *„údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným údajom v elektronickej forme s cieľom zabezpečiť pôvod a integritu týchto pridružených údajov.“*[293]

Právnická osoba môže elektronickú pečať použiť okrem autentifikácie dokumentu, ktorý vydala, aj na autentifikáciu akéhokoľvek jej digitálneho majetku, napríklad softvérového kódu alebo serverov.[294]

Podobne ako pri elektronickom podpise, aj v prípade elektronickej pečate Nariadenie eIDAS definuje niekoľko úrovní. Základnú úroveň predstavuje elektronická pečať. Vyššou úrovňou je **zdokonalená elektronická pečať**, ktorá musí spĺňať konkrétne

[291] V zmysle § 19 ods. 1 zákona č. 71/1967 o správnom konaní (správny poriadok) je stanovené, že v prípade podaní, ktoré boli urobené elektronickými prostriedkami, musí byť takéto podanie podpísané kvalifikovaným elektronickým podpisom. Online služby poskytované subjektmi verejného sektora v zmysle Nariadenia eIDAS podľa nášho názoru pokrývajú aj elektronické služby verejnej správy, kde sa v rámci správneho konania môže podanie urobiť elektronicky a podpísať kvalifikovaným elektronickým podpisom. V českom preklade Nariadenia eIDAS sa okrem súdneho konania spomína aj správne konanie. Dostupné na: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32014R0910&from=EN.
[292] Čl. 25 ods. 1-3 Nariadenia eIDAS.
[293] Čl. 3 bod 25 Nariadenia eIDAS.
[294] Bod 65 preambuly Nariadenia eIDAS.

požiadavky stanovené v Nariadení eIDAS. Prvou požiadavkou je, aby bola zdokonalená pečať jedinečne spojená s právnickou osobou, ktorá vyhotovila elektronickú pečať, čiže pôvodcom pečate. Ďalšou podmienkou je určenie totožnosti pôvodcu pečate na základe zdokonalenej elektronickej pečate. Zdokonalená elektronická pečať musí byť vyhotovená pomocou údajov na vyhotovenie elektronickej pečate. Tieto údaje môže pôvodca pečate s vysokou mierou dôveryhodnosti pod jeho kontrolou používať na vyhotovenie elektronickej pečate. Poslednou požiadavkou na zdokonalenú elektronickú pečať, je jej prepojenie s údajmi, na ktoré sa vzťahuje, takým spôsobom, že každú dodatočnú zmenu údajov možno zistiť.[295] Najvyššiu úroveň elektronickej pečate predstavuje **kvalifikovaná elektronická pečať**, ktorá musí spĺňať rovnaké požiadavky ako zdokonalená elektronická pečať a zároveň musí byť vyhotovená pomocou kvalifikovaného zariadenia na vyhotovenie elektronickej pečate a založená na kvalifikovanom certifikáte pre elektronickú pečať.[296]

V súvislosti s **právnymi účinkami** elektronickej pečate, ako aj s jej prípustnosťou ako dôkazu v súdnom konaní platia rovnaké podmienky ako v prípade elektronických podpisov. Taktiež platia rovnaké požiadavky na uznávanie kvalifikovanej elektronickej pečate v iných členských štátoch EÚ ako v prípade kvalifikovaného elektronického podpisu.

Je nutné podotknúť, že v prípade, ak sa pri transakcii vyžaduje kvalifikovaná elektronická pečať právnickej osoby, rovnako akceptovateľný by mal byť aj kvalifikovaný elektronický podpis splnomocneného zástupcu právnickej osoby.[297]

Na tomto mieste je potrebné poznamenať, že elektronická pečať neidentifikuje konkrétnu fyzickú osobu, ktorá ju vytvorila, ale iba právnickú osobu. V tejto súvislosti zastávame názor, že elektronická pečať nemôže mať ani v najvyššej úrovni, a teda kvalifikovanej elektronickej pečati, rovnaké právne účinky ako vlastnoručný podpis, ako to je v prípade kvalifikovaného elektronického podpisu. V nadväznosti na vyššie uvedenú skutočnosť musíme konštatovať, že súčasná právna úprava upravujúca právne účinky kvalifikovanej elektronickej pečate na národnej úrovni je v rozpore s ustanoveniami Nariadenia eIDAS, nakoľko § 40 ods. 4 Občianskeho zákonníka priznáva kvalifikovanej elektronickej pečati rovnaké právne účinky ako kvalifikovanému elektronickému podpisu.

[295] Čl. 36 Nariadenia eIDAS.
[296] Čl. 3 bod 27 Nariadenia eIDAS. Požiadavky na kvalifikovaný certifikát pre elektronické pečate možno nájsť v prílohe č. III Nariadenia eIDAS. V prípade kvalifikovaných zariadení na vyhotovenie elektronických pečatí sa uplatňujú požiadavky na kvalifikované zariadenia na vyhotovenie elektronických pečatí.
[297] Bod 58 preambuly Nariadenia eIDAS.

3.3.1.3 Elektronická časová pečiatka

Elektronická časová pečiatka je v zmysle Nariadenia eIDAS definovaná ako: *„údaje v elektronickej forme, ktoré viažu iné údaje v elektronickej forme s konkrétnym časom, čím tvoria dôkaz o existencii týchto iných údajov v danom čase."*[298] Iné údaje v elektronickej forme predstavujú konkrétny dokument, u ktorého sa zaznamenáva okamih času. Predmetné spojenie elektronickej časovej pečiatky s inými údajmi dokazujú, že tieto iné údaje existovali v konkrétnom momente.

V porovnaní s elektronickým podpisom a elektronickou pečaťou plní elektronická časová pečiatka iný účel, nakoľko dôveryhodným spôsobom určuje čas existencie konkrétnych údajov.

Nariadenie eIDAS rozpoznáva dve úrovne elektronickej časovej pečiatky. Popri základnej úrovni, čiže elektronickej časovej pečiatke definuje aj **kvalifikovanú elektronickú časovú pečiatku**, ktorá musí spĺňať požiadavky stanovené v čl. 42 Nariadenia eIDAS. Prvou požiadavkou je, aby kvalifikovaná elektronická časová pečiatka spájala dátum a čas s údajmi spôsobom, ktorý v rozumnej miere zamedzuje možnosť nezistiteľnej zmeny údajov. Ďalšou podmienkou je, aby kvalifikovaná elektronická časová pečiatka bola založená na presnom zdroji času s koordinovaným svetovým časom. Poslednou požiadavkou na kvalifikovanú elektronickú časovú pečiatku je, aby bola podpísaná zdokonaleným elektronickým podpisom alebo zapečatená zdokonalenou elektronickou pečaťou kvalifikovaného poskytovateľa služieb dôvery alebo rovnocennou metódou.[299]

Odopretie právnych účinkov elektronickej časovej pečiatky alebo jej prípustnosť ako dôkazu v súdnom konaní, výlučne z toho dôvodu, že ide o elektronickú formu alebo že nespĺňa požiadavky kvalifikovanej elektronickej časovej pečiatky, sa zakazuje. Taktiež platí, že na najvyššiu úroveň elektronickej časovej pečiatky, čiže kvalifikovanú elektronickú časovú pečiatku sa viaže domnienka správnosti dátumu a času, ktorý uvádza, ako aj domnienka integrity údajov, s ktorými je dátum a čas spojený. V prípade, ak je kvalifikovaná elektronická časová pečiatka vydaná v jednom členskom štáte EÚ, uznáva sa ako kvalifikovaná elektronická časová pečiatka vo všetkých členských štátoch EÚ.[300]

[298] Čl. 3 bod 33 Nariadenia eIDAS.
[299] Čl. 42 ods. 1 Nariadenia eIDAS.
[300] Čl. 41 Nariadenia eIDAS.

3.3.1.4 Elektronický podpis a elektronická pečať vo verejných službách[301]

Nariadenie eIDAS osobitne upravuje problematiku týkajúcu sa použitia elektronických podpisov a elektronických pečatí vo verejných službách. Predmetné ustanovenia sa týkajú využívania online služieb, ktoré poskytujú subjekty verejného sektora, alebo ktoré sú ponúkané v jeho mene. V zmysle čl. 3 ods. 7 Nariadenia eIDAS možno medzi subjekty verejného sektora zaradiť: *„ústredný, regionálny alebo miestny orgán, verejnoprávny subjekt[302] alebo združenie tvorené jedným alebo viacerými takýmito orgánmi alebo jedným či viacerými takýmito verejnoprávnymi subjektmi, alebo súkromný subjekt, ktorý aspoň jeden z takýchto orgánov, subjektov alebo združení poveril poskytovaním verejných služieb, keď koná na základe takéhoto poverenia."*

V týchto osobitných prípadoch pôjde už o realizáciu elektronických podaní alebo iných právnych úkonov vo vzťahu k verejnej správe, kde sa vyžaduje autorizácia, čiže pôjde o využitie elektronického podpisu alebo elektronickej pečate. V zmysle Nariadenia eIDAS platí, ak členský štát EÚ vyžaduje v prípade použitia online služby, ktorú poskytuje subjekt verejného sektora alebo v jeho mene, použitie elektronického podpisu alebo elektronickej pečate konkrétnej úrovne, tento členský štát má povinnosť uznať elektronický podpis alebo elektronickú pečať z iných členských štátov, ak sú rovnakej alebo vyššej úrovne. Vyslovene sa zakazuje, aby členský štát EÚ pre online službu vyžadoval elektronický podpis alebo elektronickú pečať vyššej úrovne bezpečnosti ako kvalifikovanú úroveň.[303]

Pre prehľadnejšie znázornenie terminologických zmien, ktoré nastali po prijatí Nariadenia eIDAS, v nasledujúcej tabuľke uvádzame ich ekvivalenty, ktoré boli obsiahnuté v zákone č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov (ďalej ako „Zákone o EP").

---

[301] Nariadenie eIDAS nedefinuje verejné služby a ani neodkazuje na iný legislatívny akt.

[302] Nariadenie eIDAS v prípade pojmu verejnoprávny subjekt odkazuje na pojem verejnoprávne inštitúcie upravený v čl. 2 ods. 1 bod 4 *Smernice Európskeho parlamentu a Rady 2014/24/EÚ z 26. februára 2014 o verejnom obstarávaní a o zrušení smernice 2004/18/ES.* V zmysle vyššie uvedeného ustanovenia sa za verejnoprávne inštitúcie považujú inštitúcie, ktoré majú všetky nasledujúce charakteristické znaky:
"a) sú zriadené na osobitný účel uspokojovania potrieb vo všeobecnom záujme, pričom nemajú priemyselnú ani komerčnú povahu;
b) majú právnu subjektivitu a
c) sú z väčšej časti financované štátnymi, regionálnymi alebo miestnymi orgánmi alebo inými verejnoprávnymi inštitúciami; alebo ich riadenie podlieha dohľadu týchto orgánov alebo inštitúcií; alebo majú správnu, riadiacu alebo dozornú radu, v ktorej viac ako polovicu členov menujú štátne, regionálne alebo miestne orgány alebo iné verejnoprávne inštitúcie."

[303] Čl. 27 a 37 Nariadenia eIDAS.

Porovnanie – Zákon o EP a Nariadenie eIDAS

Zákon o EP	**Nariadenie eIDAS**	**Poznámka**
Elektronický podpis	Zdokonalený elektronický podpis	Obyčajný elektronický podpis upravený v Nariadení eIDAS sa v Zákone o EP nepoužíval.
Zaručený elektronický podpis	Kvalifikovaný elektronický podpis	
Elektronická pečať	Zdokonalená elektronická pečať	V zmysle Nariadenia eIDAS nemá kvalifikovaná elektronická pečať účinky vlastnoručného podpisu.
Zaručená elektronická pečať	Kvalifikovaná elektronická pečať	
Časová pečiatka	Kvalifikovaná elektronická časová pečiatka	Nariadenie eIDAS upravuje aj obyčajnú elektronickú časovú pečiatku, ktorú Zákon o EP nepoznal.
Certifikát	Certifikát pre elektronický podpis	Tak ako Zákon o EP aj Nariadenie eIDAS upravuje aj ich kvalifikovanú formu.
Systémový certifikát	Certifikát pre elektronickú pečať	
Certifikačná autorita	Poskytovateľ služieb dôvery	V zmysle Nariadenia eIDAS zodpovedajú za škody spôsobené neplnením si povinností všetci poskytovatelia služieb dôvery.
Akreditovaná certifikačná autorita	Kvalifikovaný poskytovateľ služieb dôvery	
Certifikačná služba	Služba dôvery	Okruh služieb dôvery je širší v porovnaní s certifikačnými službami.
Akreditovaná certifikačná služba	Kvalifikovaná služba dôvery	
Bezpečné zariadenie na vyhotovenie elektronického podpisu	Kvalifikované zariadenie na vyhotovenie elektronického podpisu	Zákon o EP upravoval aj bezpečné zariadenie na vyhotovenie časovej

		pečiatky. V Nariadení eIDAS absentuje úprava zariadenia na vytvorenie elektronickej časovej pečiatky.
Bezpečné zariadenie na vyhotovenie elektronickej pečate	Kvalifikované zariadenie na vyhotovenie elektronickej pečate	

Zdroj: Vlastné spracovanie

3.3.2 Vzájomné uznávanie prostriedkov elektronickej identifikácie

Problematika **vzájomného uznávania prostriedkov elektronickej identifikácie**[304] je na úrovní práva Európskej únie (ďalej len „EÚ“)[305] predmetom Nariadenia eIDAS[306]. Cieľom predmetnej úpravy je zabezpečiť, aby sa prostriedky elektronickej identifikácie jedného členského štátu EÚ dali použiť na identifikáciu a autentifikáciu pri prístupe k online službám, ktoré sú poskytované subjektmi verejného sektora iného členského štátu EÚ.

Ustanovenia týkajúce sa zásady vzájomného uznávania sa dotkli nielen fyzických osôb, fyzických osôb podnikateľov a právnických osôb, ktorí primárne využívajú online služby, ale najmä subjektov verejného sektora, ktoré tieto služby poskytujú. Je potrebné podotknúť, že od 1. júla 2016 sa aplikuje Nariadenie eIDAS len v rozsahu upravujúcom služby dôvery. Povinnosť vzájomne uznávať prostriedky elektronickej identifikácie vznikla členským štátom EÚ 29. septembra 2018.

Vo väčšine členských štátov EÚ boli zavedené rôzne schémy elektronickej identifikácie, ktoré sa v mnohých aspektoch líšili. Doteraz neexistoval spoločný právny rámec, ktorý by vyžadoval, aby každý členský štát EÚ pri prístupe k online službám uznával a prijímal prostriedky elektronickej identifikácie vydávané v inom členskom štáte EÚ. Možno povedať, že cieľom tejto úpravy je zabezpečiť, aby sa prostriedky elektronickej identifikácie jedného

[304] Prostriedkom elektronickej identifikácie je v zmysle čl. 3 ods. 2 Nariadenia eIDAS: *„hmotná jednotka a/alebo nehmotná jednotka obsahujúca osobné identifikačné údaje, ktorá sa používa na autentifikáciu pre online služby.“* Inými slovami, prostriedky elektronickej identifikácie (napr. elektronické údaje z osobných a cestovných dokladov, digitálne certifikáty, zoznamy zrušených certifikátov a pod.), ktoré budú musieť členské štáty EÚ povinne uznávať, slúžia na elektronickú autentifikáciu, čiže overenie deklarovanej identity osoby, ktorá chce využiť online službu v inom členskom štáte EÚ. Na tomto mieste je potrebné uviesť, že cieľom Nariadenia eIDAS nie je uznávanie elektronického občianskeho preukazu, ale uznanie elektronickej identity, ktorá je obsiahnutá v ňom.

[305] V právnom poriadku Slovenskej republiky sú úrovne záruky upravené vo výnose Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy.

[306] Nariadenie EP a Rady 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES.

členského štátu EÚ dali použiť na identifikáciu a autentifikáciu pri využívaní online služieb, ktoré sú poskytované subjektmi verejného sektora iného členského štátu EÚ.
Praktický dopad vzájomného uznávania prostriedkov elektronickej identifikácie je zrejmý najmä v situácii, kedy by občan Slovenskej republiky (ďalej len „SR“) chcel využiť online služby, poskytované subjektmi verejného sektora iného členského štátu EÚ. V takejto situácii by si občan SR nemusel vybavovať elektronický prostriedok identifikácie danej krajiny, ale na cezhraničnú autentifikáciu by mu postačoval národný prostriedok elektronickej identifikácie.

3.3.2.1 Základné pojmy

Pre pochopenie konceptu a procesu vzájomného uznávania prostriedkov elektronickej identifikácie je potrebné objasniť základné pojmy ako schéma elektronickej identifikácie, prostriedky elektronickej identifikácie, elektronická identifikácia, osobné identifikačné údaje, autentifikácia a spoliehajúca strana.

V zmysle čl. 3 bodu 4 Nariadenia eIDAS je **schéma elektronickej identifikácie** definovaná ako: *„systém na elektronickú identifikáciu, v rámci ktorého sa fyzickým osobám alebo právnickým osobám alebo fyzickým osobám zastupujúcim právnické osoby vydávajú prostriedky elektronickej identifikácie“*. Podmienky, ktoré musí spĺňať schéma elektronickej identifikácie sú stanovené v čl. 6 ods. 1 Nariadenia eIDAS. Schéma elektronickej identifikácie úzko súvisí s prostriedkom elektronickej identifikácie, avšak tento pojem je potrebné vnímať v širšom kontexte. Schéma elektronickej identifikácie poskytuje dve služby, ktorými sú:

a) vydávanie prostriedkov elektronickej identifikácie,
b) zabezpečenie procesu autentifikácie.

Prostriedok elektronickej identifikácie je v zmysle čl.3 bodu 2 Nariadenia eIDAS definovaný ako: *„hmotná jednotka a/alebo nehmotná jednotka obsahujúca osobné identifikačné údaje, ktorá sa používa na autentifikáciu pre online služby“*. Slúži na elektronickú autentifikáciu, čiže overenie deklarovanej identity osoby, ktorá chce využiť online službu v inom členskom štáte EÚ. Ide napr. o elektronické údaje z osobných a cestovných dokladov, certifikáty, zoznamy zrušených certifikátov a pod. V najvšeobecnejšej rovine ide o elektronický občiansky preukaz. Avšak, cieľom Nariadenia eIDAS nie je uznávanie elektronického občianskeho preukazu ako takého, ale uznanie elektronickej identity, ktorá je obsiahnutá v ňom.

Elektronická identifikácia je v zmysle čl. 3 bodu 1 Nariadenia eIDAS definovaná ako: *„proces používania osobných identifikačných údajov v elektronickej forme, ktoré jedinečne reprezentujú fyzickú osobu alebo právnickú osobu alebo fyzickú osobu zastupujúcu právnickú osobu“*. Z tejto definície je zrejmé, že podľa Nariadenia eIDAS je možné identifikovať:

- fyzické osoby,
- fyzické osoby zastupujúce právnickú osobu alebo
- právnickú osobu.

Osobné identifikačné údaje predstavujú v zmysle čl. 3 bodu 3 Nariadenia eIDAS *„súbor údajov, ktorý umožňuje určiť identity fyzickej osoby alebo právnickej osoby alebo fyzickej osoby zastupujúcej právnickú osobu“*. Minimálny súbor osobných identifikačných údajov[307] pre **fyzické osoby** musí v zmysle vykonávacieho nariadenia Komisie (EÚ) 2015/1501 z 8. septembra 2015 o rámci interoperability obsahovať všetky nasledujúce atribúty:

a) súčasné priezvisko(á),
b) súčasné meno(á),
c) dátum narodenia,
d) jedinečný identifikátor vytvorený odosielajúcim členským štátom EÚ v súlade s technickými špecifikáciami na účely cezhraničnej identifikácie a pokiaľ možno následne nemenený.

Popri vyššie uvedených atribútoch, musí minimálny súbor údajov obsahovať jeden alebo viacero z nasledujúcich atribútov:

a) meno(á) a priezvisko(á) pri narodení,
b) miesto narodenia,
b) súčasná adresa,
c) pohlavie.

Nariadenie eIDAS taktiež definuje pojem **autentifikácia.** V zmysle Čl. 3 bodu 5 je autentifikácia: *„elektronický proces, ktorý umožňuje potvrdiť elektronickú identifikáciu fyzickej osoby alebo právnickej osoby alebo pôvod a integritu údajov v elektronickej forme.“* Takýmto spôsobom je zaručené, že v rámci preukazovania identity danej osoby a jej autentifikácie pre online služby sú používané neporušené údaje s potvrdenou integritou a že sú rovnaké

[307] Osobné identifikačné údaje predstavujú z pohľadu nariadenia Európskeho parlamentu a Rady (EÚ) 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, ďalej len „GDPR“) osobné údaje. Bližšie pozri: BERTHOTY, J., MESARČÍK, M., ZIMEN, O.: *Základné pojmy Nariadenia.* In Všeobecné nariadenie o ochrane osobných údajov. Praha : C.H. Beck, 2018, s. 123-186.

ako súbor údajov uložených na prostriedku elektronickej identifikácie. Inými slovami možno povedať, že tieto údaje v rámci prenosu prostredníctvom informačných systémov nikto nezmenil, nezamenil za iné a pod.

Spoliehajúca strana je v zmysle čl. 3 bodu 6 Nariadenia eIDAS definovaná ako: *„fyzická osoba alebo právnická osoba, ktorá sa spolieha na elektronickú identifikáciu alebo službu dôvery"*. Táto definícia je dôležitá pre rozdelenie práv a povinností jednotlivých strán. Spoliehajúcou stranou je napr. poskytovateľ online služby, do ktorej sa autentifikuje osoba prostredníctvom prostriedku elektronickej identifikácie (napr. elektronickým občianskym preukazom). Poskytovateľ takejto služby sa spolieha na schému elektronickej identifikácie, ktorú zabezpečuje v prípade elektronického občianskeho preukazu štát.

3.3.2.2 Podmienky pre vzájomné uznávanie prostriedkov elektronickej identifikácie

Pre vzájomné uznávanie prostriedkov elektronickej identifikácie musia byť v zmysle Nariadenia eIDAS splnené nasledujúce **tri podmienky**.

Prvou podmienkou pre vzájomné uznávanie prostriedku elektronickej identifikácie iným členským štátom EÚ je, aby bol prostriedok elektronickej identifikácie vydávaný v rámci schémy elektronickej identifikácie, ktorá je uvedená v zozname, ktorý zverejňuje Európska komisia podľa čl. 9 Nariadenie eIDAS. Inými slovami možno povedať, že musí ísť o oznámenú schému elektronickej identifikácie podľa Nariadenia eIDAS.

Časový rámec procesu oznámenia schémy elektronickej identifikácie

Časový rámec procesu oznámenia schémy elektronickej identifikácie	
Poskytnutie opisu schémy elektronickej identifikácie ostatným členským štátom EÚ Čl. 7, písm. g) Nariadenia eIDAS	min. 6 mesiacov pred oznámením
Partnerské hodnotenie	môže trvať max. 3 mesiace
Oznámenie národného systému elektronickej identifikácie Európskej komisii Čl. 9 Nariadenia eIDAS	do 2 mesiacov od oznámenia sa zverejní v Úradnom vestníku EÚ

Zverejnenie systému elektronickej identifikácie v Úradnom vestníku EÚ Čl. 9 ods. 3 Nariadenia eIDAS	vzájomné uznávanie sa začne do 12 mesiacov od zverejnenia
Povinnosť vzájomne uznávať systémy elektronickej identifikácie	

Zdroj: Vlastné spracovanie

Druhou podmienkou pre vzájomné uznávanie prostriedku elektronickej identifikácie iným členským štátom EÚ je zaistenie úrovne záruky prostriedku elektronickej identifikácie vyššej alebo rovnakej ako tá, ktorú vyžaduje príslušný subjekt verejného sektora pre prístup k online službe za predpokladu, že úroveň záruky daných prostriedkov elektronickej identifikácie zodpovedá úrovni záruky pokročilá alebo vysoká.

Treťou podmienkou vzájomného uznávania prostriedku elektronickej identifikácie je, aby príslušný subjekt verejného sektora používal vo vzťahu k prístupu k danej online službe úroveň záruky pokročilá alebo vysoká.[308] V prípade, ak prostriedok elektronickej identifikácie má nižšiu úroveň záruky, členský štát ho môže, ale nemusí uznať pre potreby identifikácie pre online služby, ktoré poskytuje.[309]

Nariadenie eIDAS rozlišuje **tri úrovne záruky**, konkrétne nízka, pokročilá a vysoká. Pri definovaní týchto úrovní záruky Nariadenie eIDAS vychádzalo z výsledkov rozsiahleho pilotného projektu financovaného prostriedkami EÚ a normalizačných a medzinárodných činností, ktoré obsahujú rôzne technické vymedzenia a opisy úrovní záruky. Konkrétne ide o projekt STORK 1.0[310] a medzinárodnú normu Štandard o úrovniach záruky[311], kde Nariadenie eIDAS odkazuje na úrovne 2, 3 a 4 stanovené v projekte STORK 1.0 a Štandarde o úrovniach záruky. V nasledujúcej tabuľke uvádzame prehľad úrovní záruky.

[308] Tamtiež, čl. 6 písm. b) c).
[309] Tamtiež, bod 13 preambuly..
[310] Projekt STORK (*Secure idenTity acrOss boRders linKed*) bol realizovaný v rokoch 2008-2011 a zaoberal problematikou identifikácie a autentifikácie v kontexte cezhraničného využívania verejných služieb.
[311] ISO/IEC 29115:2013 Entity authentication assurance framework.

Porovnanie úrovní záruky Nariadenia eIDAS, STORK 1.0 a Štandardu o úrovniach záruky

Úrovne záruky podľa Nariadenia eIDAS	**Úrovne záruky podľa STORK 1.0**	**Úrovne záruky podľa Štandardu o úrovniach záruky**
Nízka	QAA úroveň 2	Úroveň záruky 2 - stredná
Pokročilá	QAA úroveň 3	Úroveň záruky 3 - vysoká
Vysoká	QAA úroveň 4	Úroveň záruky 4 – veľmi vysoká

Zdroj: Vlastné spracovanie

Úrovne záruky upravené v Nariadení eIDAS boli vypracované na základe prístupu, ktorý je založený na výsledkoch *(outcome based approach)*, čo znamená, že každý členský štát EÚ môže splniť požadovanú úroveň záruky rôznymi špecifickými spôsobmi, ktoré sú upravené na národnej úrovni. Inými slovami, Nariadenie eIDAS nezrušuje národné riešenia pre stanovenie úrovní záruky, ale oznámeným prostriedkom elektronickej identifikácie bude musieť byť pridelená konkrétna úroveň záruky v zmysle Nariadenia eIDAS.

Jednotlivé úrovne záruky predstavujú v zmysle Nariadenia eIDAS hierarchický systém. Tieto úrovne sú charakterizované pomocou súvisiacich technických špecifikácií, noriem a postupov, vrátane technických kontrol, ktorých účelom je znížiť riziko zneužitia alebo zmeny totožnosti. Podrobnosti o minimálnych technických špecifikáciách, normách a postupoch, pomocou ktorých sa stanovujú úrovne záruky sú upravené vo vykonávacom nariadení Komisie (EÚ) 2015/1502 z 8. septembra 2015 (ďalej len „Vykonávacie nariadenie").[312]

3.3.3 Ako funguje cezhraničná autentifikácia?

Nariadenie eIDAS vytvorilo systém **cezhraničnej autentifikácie**, ktorý je založený na **uzloch** (kontaktných bodoch).[313] Uzol je miesto pripojenia, ktoré je súčasťou architektúry interoperability elektronickej identifikácie a je zapojené do cezhraničnej autentifikácie osôb. Uzol je schopný rozoznať a spracovať alebo prenášať prenosy údajov alebo ich prenášať na

[312] Vykonávacie nariadenie Komisie (EÚ) 2015/1502 z 8. septembra 2015, ktorým sa stanovujú minimálne technické špecifikácie a postupy pre úrovne zabezpečenia prostriedkov elektronickej identifikácie podľa článku 8 ods. 3 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu.

[313] Tzv. brány – pred tým nazývané PEPS (*Pan-European Proxy Services*). Architektúra prepojených národných bodov. Výsledok projektu STORK 1 a STORK 2. PEPS = eIDAS uzol.

iné uzly tým, že umožňuje prepojenie vnútroštátnej infraštruktúry elektronickej identifikácie jedného členského štátu EÚ s vnútroštátnymi infraštruktúrami elektronickej identifikácie ostatných členských štátov EÚ.[314] Nariadenie eIDAS nevylučuje, aby takýchto uzlov bolo viacero.

Proces cezhraničnej autentifikácie by sme mohli opísať v nasledujúcich krokoch:

a) občan požaduje on-line službu v členskom štáte,

b) občan je požiadaný autentifikovať sa prostredníctvom on-line služby,

c) vo fáze autentifikácie je zrejmé, že občan má prostriedok elektronickej identifikácie z iného členského štátu,

d) žiadosť o autentifikáciu je odoslaná do krajiny občana na overenie totožnosti prostredníctvom riešenia eIDAS poskytovateľovi identity občana (*Identity Provider*), v ktorom sa uskutočňuje autentifikácia,

e) výsledok autentifikácie sa vráti poskytovateľovi služieb,

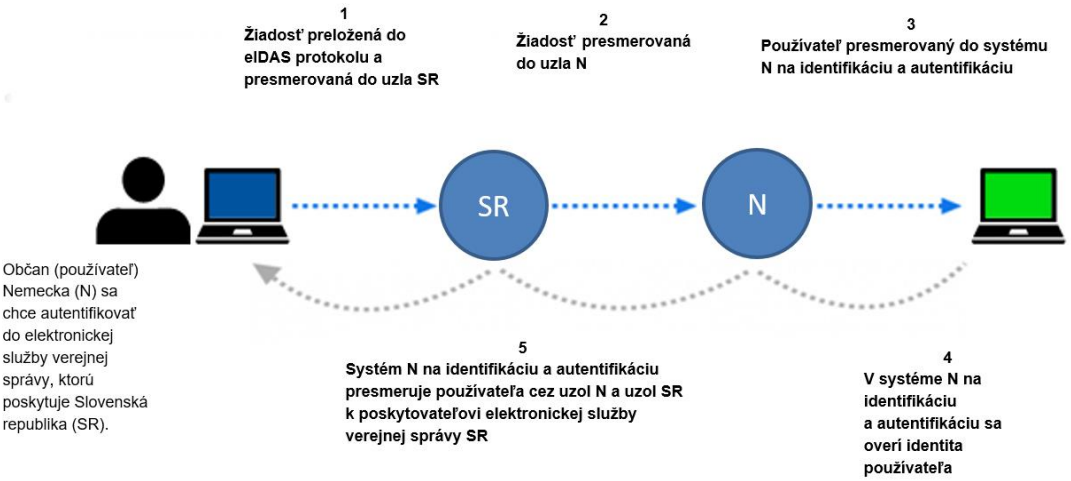
f) výsledok autentifikácie je dokončený a v prípade pozitívneho výsledku občan môže pokračovať v prístupe k službe.

Riešenie eIDAS robí rôzne národné protokoly prostriedkov elektronickej identifikácie interoperabilné. Riešenie využíva **protokol eIDAS** na preklad národných identifikačných údajov do spoločného formátu, ktorému členské štáty rozumejú a používajú.[315]

V nižšie uvedenom obrázku je znázornený postup cezhraničnej autentifikácie, kde SR žiada o autentifikáciu (*receiving memeber state*) a Nemecko poskytuje autentifikáciu (*sending member state*).

[314] Čl. 2 ods. 1 vykonávacieho nariadenia Komisie (EÚ) 2015/1501 z 8. septembra 2015 o rámci interoperability.
[315] Dostupné na: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/How+does+it+work+-+eIDAS+solution.

Cezhraničná autentifikácia



Zdroj: Vlastné spracovanie

3.4.2 Vzájomné uznávanie prostriedkov elektronickej identifikácie a cezhraničná autentifikácia v SR

Je potrebné uviesť, že v zmysle Nariadenia eIDAS je na rozhodnutí členských štátov EÚ, či oznámia Európskej komisii všetky, niektoré alebo neoznámia žiadne schémy elektronickej identifikácie, ktoré sa používajú na vnútroštátnej úrovni na prístup aspoň k verejným online službám alebo ku konkrétnym službám.[316] V kontexte oznámenia, resp. neoznámenia schémy elektronickej identifikácie je potrebné poznamenať, že členským štátom EÚ vznikla v septembri 2018 povinnosť vzájomne uznávať prostriedky elektronickej identifikácie, ktoré boli oznámené v súlade s Nariadením eIDAS. Inými slovami, ak napr. občan Českej republiky bude chcieť využiť online službu poskytovanú orgánom verejnej správy Slovenskej republiky a Česká republika v súlade s Nariedením eIDAS oznámila schému elektronickej identifikácie, tak občan Českej republiky má právo sa autentifikovať pre využitie takejto služby.

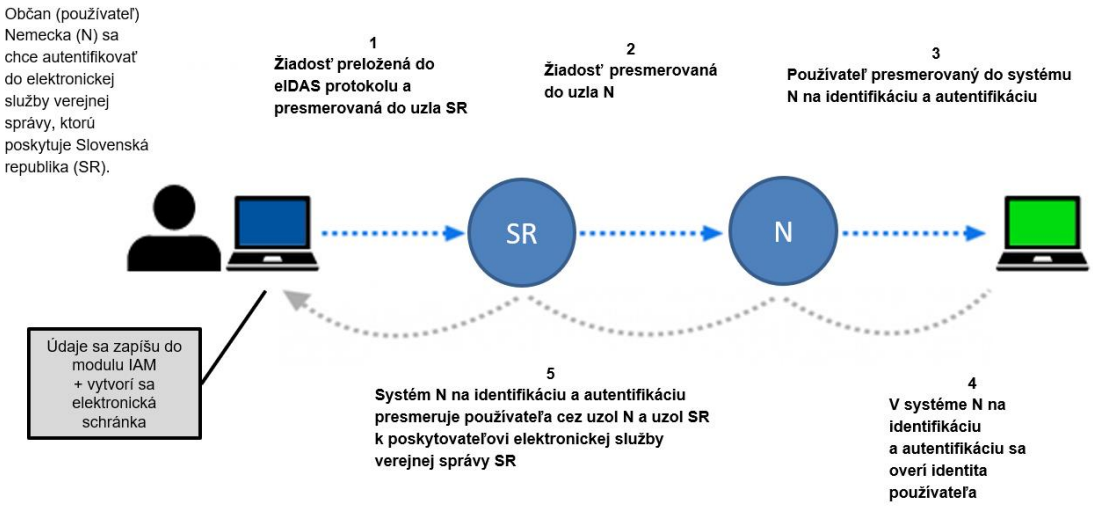
K decembru 2019 bolo oznámených 12 schém elektronickej identifikácie 11 členskými štátmi.[317] Slovenská republika poskytla opis schémy elektronickej identifikácie ostatným členským štátom EÚ 18. apríla 2019. Slovenskej schéme elektronickej identifikácie, oficiálne nazvanej *National identity scheme of the Slovak Republic* je v opise priradená úroveň záruky vysoká. Predmetná schéma je tvorená z nasledujúcich častí:

[316] Bod 13 preambuly Nariadenia eIDAS.
[317] Zoznam dostupný na: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS.

- elektronické občianske preukazy vydané Slovenskou republikou. Existujú dva typy elektronických občianskych preukazov – elektronický občiansky preukaz vydávaný občanom Slovenskej republiky starším ako 15 rokov a doklad o pobyte s elektronickým čipom vydávaný cudzincom, ktorí majú pobyt na území Slovenskej republiky,
- eID autentifikačný server,
- IAM (*Identity Access Management*) modul,
- uzol eIDAS.[318]

Pri prvom prihlásení osoby z iného členského štátu do online služby poskytovanou subjektom verejného sektora SR sa zapíšu z eIDAS uzla do **modulu IAM**[319] údaje o danej osobe a zároveň sa mu vytvorí elektronická schránka v zmysle Zákona o e-Governmente. Občan iného členského štátu pre doručovanie do elektronickej schránky musí vykonať jej aktiváciu.[320]

Cezhraničná autentifikácia v SR



Zdroj: Vlastné spracovanie

Výpočet údajov, ktoré sú zapísané do modulu IAM budú limitované, nakoľko minimálny súbor **osobných identifikačných údajov** pre fyzické osoby obsahuje **atribúty v zmysle**

[318] Opis slovenskej schémy elektronickej identifikácie dostupný na: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Slovakia+--+eID+Scheme.
[319] Bližšie k modulu IAM pozri predchádzajúce state učebnice.
[320] Často kladené otázky k elektronickej identifikácii na základe eIDAS (Nariadenie Európskeho parlamentu a Rady EÚ č. 910/2014). Dostupné na: https://www.slovensko.sk/_img/CMS4/eIDAS/FAQ%20-%20eIDAS_v2.pdf.

vykonávacieho nariadenia Komisie (EÚ) 2015/1501 z 8. septembra 2015 o rámci interoperability podľa čl. 12 ods. 8 Nariadenia eIDAS .

V zmysle dostupných informácií, sa v module IAM vytvorila od 28. septembra 2018 možnosť prihlasovať sa prostredníctvom eIDAS uzla pre zahraničné fyzické osoby s nemeckým občianskym preukazom alebo dokladom o pobyte cudzinca žijúceho v Nemecku. Tieto osoby sa budú môcť s vyššie uvedenými dokladmi identifikovať a autentifikovať do ústredného portálu verejnej správy (ďalej len „ÚPVS“), ako aj na všetky portály, ktoré prostredníctvom ÚPVS využívajú jednotné prihlásenie a technicky akceptujú tento typ autentifikačného prostriedku.[321]

V tejto súvislosti je potrebné podotknúť, že konečné poskytnutie konkrétnej elektronickej služby je spojené s právom na využívanie takýchto služieb na základe podmienok, ktoré sú stanovené vo vnútroštátnych právnych predpisoch.[322] Je potrebné selektovať online služby SR, ktoré môžu občania iných členských štátov EÚ reálne využiť. Inými slovami, v prípade služieb poskytovaných online subjektmi verejného sektora SR, kde sa vyžaduje identifikácia a autentifikácia a kde je stanovená oprávnená podmienka (trvalý pobyt, štátne občianstvo a pod.), nie je možné, aby došlo k faktickému poskytnutiu takejto služby. Za sprístupnenie faktického využitia konkrétnej online služby sú zodpovedné príslušné orgány verejnej moci, ktoré danú online službu poskytujú.[323]

V praxi môžu vzniknúť prípady duplicitnej identity, a to najmä z dôvodu, že členské štáty neposkytujú mechanizmus cezhraničného stotožňovania identít. Pôjde najmä o situácie ako:

a) občan iného členského štátu má vydaný prostriedok elektronickej identifikácie inej krajiny EÚ a zároveň mu bol v SR vydaný aj prostriedok, napríklad alternatívny autentifikátor.

b) občan iného členského štátu je zapísaný v registri fyzických osôb na základe fyzicky predloženého dokladu ako je pas alebo občiansky preukaz. Pri prihlasovaní cez eIDAS uzol sa však obvykle zasiela odlišný identifikátor, a preto nepríde k automatickému stotožneniu

[321] Často kladené otázky k elektronickej identifikácii na základe eIDAS (Nariadenie Európskeho parlamentu a Rady EÚ č. 910/2014). Dostupné na: https://www.slovensko.sk/_img/CMS4/eIDAS/FAQ%20-%20eIDAS_v2.pdf, s. 7.
[322] Bod 14 preambuly Nariadenia eIDAS.
[323] Často kladené otázky k elektronickej identifikácii na základe eIDAS (Nariadenie Európskeho parlamentu a Rady EÚ č. 910/2014). Dostupné na: https://www.slovensko.sk/_img/CMS4/eIDAS/FAQ%20-%20eIDAS_v2.pdf, s. 3.

c) krajina vydávajúca identifikátor vytvára pre každý prostriedok identifikácie nový identifikátor. V prípade Nemecka pri každom novom vydanom eID (napríklad po jeho strate alebo vypršaní) pre rovnakú osobu vzniká nový identifikátor a teda aj nová identita v IAM.

d) krajina vydávajúca identifikátor môže poskytovať viacero prostriedkov elektronickej identifikácie pre jednu osobu a tým aj viaceré jedinečné identifikátory.[324]

Pri vytváraní duplicitných identít dôjde k situácii, že pre rovnakú osobu (v jednom právnom postavení) budú vytvorené viaceré elektronické schránky.

ZOZNAM POUŽITEJ LITERATÚRY

Knižné publikácie

1) DE ANDRADE, Norberd Nuno Gomes a kol.: *Electronic identity*, *SpringerBriefs in Cybercecurity*. Springer: London Heidelberg New York Dordrecht, 2014, 90. s. ISBN 978-1-4471-6448-7
2) DOOLEY, John F.: *A Brief History of Cryptology and Cryptographic Algorithms*. SpringerBriefs in Computer Science. Springer Science & Business Media, 2013, 99 s. ISBN 978-3-319-01627-6
3) DOSTÁLEK, Libor a kol.: *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. 2. aktualizované vydání.* Brno: Computer Press, a. s., 2009, 544 s. ISBN 978-80-251-2619-6
4) DURAND, Andrae: *Three Tiers of Identity*. Digital Identity World, 2002.
5) KHOSROW-POU, Mehdi: *Dictionary of Information Science and Technology*. USA: Idea Group Reference, 2007, 761 s. ISBN 1-59904-385-8
6) LAURENT, Maryline a BOUZEFRANE, Samia: *Digital Identity Management*. London: ISTE Press Ltd., 2015, 250 s. ISBN 978-1-78548-004-1
7) MAMOJKA, Mojmír: *Obchodný zákonník 2. zv. : veľký komentár*. Žilina : Eurokódex, 2016, 1087 s.
8) MASON, Stephen: *Electronic Signatures in Law*. UK: LexisNexis, 2003, 591 s. ISBN: 0 406 97006 8
9) MCLOUGHLIN, Ian a kol.: *Digital Government at Work. A social Informarics Perspective*. Oxford: Oxford University Press, 2013, 208 s. ISBN 978-0-19-955772-1

[324] Tamtiež, s. 4-5.

10) OLEJÁR, Daniel a kol.: *Manažment informačnej bezpečnosti a základy PKI*. Bratislava, 2015, 175 s.
11) OLEJÁR, Daniel a kol.: *Informačná bezpečnosť*. Bratislava, 2013. 246 s.
12) RANNENBERG, Kai a kol.: *The future of Identity in the Information Society. Challenges and Opportunities*. Springer: London Heidelberg New York Dordrecht, 2009, 508 s. ISBN 978-3-540-88480-4
13) ROOSENDAAL, Arnold: *Digital personae and profiles in law: Protecting individuals' rights in online contexts*. Oisterwijk: Wolf Legal Publishers, 2013, 303 s. ISBN: 978-90-5850-989-5
14) TODOROV, Dobromir: *Mechanics of Users Identification and Authentication. Fundamentals of Identity Management*. USA: Auerbach Publications, 2007, 756 s. ISBN 978-1-4200-5219-0
15) VACCA, John R.: *Computer and Information Security Handbook*. USA: Morgan Kaufmann Publishers, 2009, 844 s. ISBN:978-0-12-374354-1
16) VAN DER HOF, Simone a kol.: *Framing Citizen's Identities: The construction of personal identities in new modes of government in the Netherlands*. Nijmegen: Wolf Legal Publishers, 2010, 258 s. ISBN 978-90-5850-610-8
17) WINDLEY, Philip J.: *Digital Identity: Unmasking Identity Management Architecture (IMA)*. California: O'Reilly Media, Inc., 2005, 256 s. ISBN 9780596553944

Periodiká a zborníky

18) BATĚK, Ľuboš a IMRICH, Jaroslav: *Vyhotovovanie elektronických podpisov na diaľku. In* Zborník príspevkov z konferencie Informačná bezpečnosť 2017. SASIB, 2017, s. 73-77
19) BOYER, K. a kol.: *Eservices: operating strategy—a case study and a method for analyzing operational benefits. In* Journal of Operations Management, 2002, roč., č. 2. s. 175-185
20) DAVIES, Donald: *A Brief History of Cryptography. In* Information Security Technical Report, 1997, roč. 2, č. 2, s. 14-17
21) NOIRIEL, Gérard: *The identification of the citizen: the birth of republican civil status in France. In* Documenting individual identity, the development of state practices in the modern world. Princeton and Oxford: Princeton University Press, 2001. s. 28-48. ISBN: 9780691009124

22) PFITZMANN, Andreas a HANSEN Martin: *Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology*. 2005, 43 s. Dostupné na: https://www.freehaven.net/anonbib/cache/terminology.pdf
23) SCUPOLA, Ada a kol.: *E-Services: Characteristics, Scope and Conceptual Strengths. In* International Journal of E-Services and Mobile Applications, 2009, roč. 1, č. 3, s. 1-16
24) SMEJKAL, Vladimír a KODL, Jindřich a UŘIČAŘ, Miroslav: *Elektronický podpis podle nařízení eIDAS*. *In* Revue pro právo a technologie, 2015, č. 11, s. 189-235
25) SULLIVAN, Clare: *Protecting digital identity in the cloud: Regulating cross border data disclosure*. *In* Computer Law & Security Review, 2014, roč. 30, č. 2, s. 137-152
26) SULLIVAN, Clare: *Digital identity and mistake*. *In* International Journal of Law and Information Technology, 2012, roč. 20, č. 3, s. 223-241
27) SUTROP, Margit a LAAS-MIKKO, Katrin: *From Identity Verification to Behaviour Prediction: Ethical Implications to Second Generation Biometrics. In* Review of Policy research, 2012, roč. 29, č. 1, s. 21-36

Právne predpisy Slovenskej republiky

28) Zákon č. 71/1967 o správnom konaní (Správny poriadok)
29) Zákon Národnej rady Slovenskej republiky č. 301/1995 Z. z. o rodnom čísle
30) Zákon č. 253/1998 Z. z. o hlásení pobytu občanov Slovenskej republiky a registri obyvateľov Slovenskej republiky v znení neskorších predpisov
31) Zákon č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov
32) Zákon č. 215/2002 Z. z o elektronickom podpise a doplnení niektorých zákonov
33) Zákon č. 395/2019 Z. z. o občianskych preukazoch a o zmene a doplnení niektorých zákonov
34) Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy
35) Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
36) Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente)

37) Zákon č. 272/2015 Z. z. o registri právnických osôb, podnikateľov a orgánov verejnej moci a o zmene a doplnení niektorých zákonov
38) Zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov
39) Vyhláška Ministerstva vnútra Slovenskej republiky č. 29/2017 Z. z., ktorou sa ustanovujú podrobnosti o alternatívnom autentifikátore
40) Vyhláška Ministerstva financií Slovenskej republiky č. 25/2014 Z. z. o integrovaných obslužných miestach a podmienkach ich zriaďovania, označovania, prevádzky a o sadzobníku úhrad
41) Výnos Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy

Dokumenty a právne predpisy zo zahraničia

42) Nariadenie EP a Rady 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES
43) Vykonávacie nariadenie Komisie (EÚ) 2015/1502 z 8. septembra 2015, ktorým sa stanovujú minimálne technické špecifikácie a postupy pre úrovne zabezpečenia prostriedkov elektronickej identifikácie podľa článku 8 ods. 3 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu
44) Smernica EP a Rady 1999/93/ES o rámci spoločenstva pre elektronické podpisy
45) Smernica Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov
46) Smernica 2006/123/ES z 12. decembra 2006 o službách na vnútornom trhu
47) ISO/IEC 29115:2013 *Entity authentication assurance framework*

Webové zdroje a navštívené webové stránky

48) CAMERON, Kim: *The laws of identity*. Microsoft Corporation, 2005, 12 s. Dostupné na: http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf
49) CLARKE, Roger: *Identification and Authentication Fundamentals*. 2004. Dostupné na: http://www.rogerclarke.com/DV/IdAuthFundas.html

50) CLARKE, Roger: *A Sufficiently Rich Model of (Id)entity, Authentication and Authorisation*. 2010. Dostupné na: http://www.rogerclarke.com/ID/IdModel-1002.html#MAs

51) CLARKE, Roger: *The Digital Persona Concept, Two Decades Later*. 2013. Dostupné na: http://www.rogerclarke.com/ID/DP12.html

52) DISIG: *Certifikačná politika pre vydávanie certifikátov na eID*. Bratislava, 2016, 52 s. Dostupné na: https://www.slovensko.sk/_img/CMS4/eid/Certifikacna_politika_pre_vydavanie_certifikatov_na_eID.pdf.

53) GRAUX, Hans a kol.: *Eid interoperability for pegs—update of country profiles—analysis and assessment report*. 2009, 228 s. Dostupné na: http://ec.europa.eu/idabc/servlets/Doc2ba1.pdf?id=32521

54) www.nases.gov.sk

ISBN: 978-80-7160-523-2