ELEKTRONINIO PARAŠO NAUDOJIMO VIDAUS RINKOJE PROBLEMOS

Mindaugas Civilka
Advokatas
Advokato M. Civilkos kontora
Ozo g. 25, LT-07150 Vilnius, Lietuva
Tel. (+370 5) 204 2200
Mob. +370 687 32714
Faks. +370 5 204 2203
El. paštas: mindaugas.civilka@vilniuslegalgroup.lt

Straipsnyje analizuojami probleminiai Elektroninio parašo direktyvos įgyvendinimo ir taikymo aspektai, siekiama nustatyti svarbiausias elektroninio parašo naudojimo peržengiant vienos valstybės narės ribas kliūtis, taip pat koncentruotai įvertinti Europos Komisijos siūlomo naujojo reguliavimo ypatumus.

This article analyses problematic aspects pertaining to implementation and application of E-Signature Directive and seeks to reveal the principal barriers for the cross border operation of electronic signatures, as well as evaluates in a nutshell the new regulation proposed by the European Commission.

Įvadas

Informacinės technologijos tapo vienu iš svarbiausių ekonominės plėtros Europos Sąjungoje (toliau – ES) veiksniu, o informacinės visuomenės narių nuotolinis dalyvavimas sudarant sandorius lėmė, kad tapatybės nustatymo ir elektroninių duomenų pasirašymo klausimai tapo bene plačiausiai nagrinėti doktrinoje. 1999 m. gruodžio 13 d. Europos Parlamento ir Tarybos direktyvos 1999/93/EB dėl Bendrijos elektroninių parašų reguliavimo sistemos [1] (toliau – Direktyva) rengėjai vylėsi sukurti ilgaamžį dokumentą, reaguojantį į kintamus rinkos, technologinius ir teisinius poreikius. Direktyvos 1 straipsnis įtvirtino dvejopą jos tikslą: palengvinti elektroninių parašų naudojimą ir teisinį pripažinimą bei nustatyti elektroninių parašų ir tam tikrų sertifikavimo paslaugų teisinio reguliavimo sistemą, užtikrinant vidaus rinkos funkcionavimą. Būta lūkesčių, kad Direktyva padės suklestėti elektroninių parašų rinkai [15] ir taps visoms technologijoms vienodai atviru harmonizavimo instrumentu.

Nepaisant minėtų tikslų, Direktyva virto neišsenkančios diskusijos šaltiniu, kurios aktualumas globaliems elektroninės komercijos procesams ilgainiui išsikvėpė, o itin mažas poveikis elektroninės komercijos realybei tapo vienu iš didžiausių jos „nuopelnų“ [47, p. 14]. Gausybė Europos Komisijos (toliau – Komisija) užsakytų studijų [pvz., 48; 64; 68; 69; 70; 73] siekė paaiškinti sąlygiškai ribotą Direktyvos poveikį elektroniniam parašui funkcionuoti, Direktyvos vertinimas nėra naujas mėginimas ir Lietuvos teisės doktrinoje [44].

Vis dėlto, 2012 m. birželio 4 d. Komisija pateikė pasiūlymą „Europos Parlamento ir Tarybos reglamentas dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje“ [10] (toliau – Pasiūlymas dėl Reglamento arba Siūlomas reglamentas), kuriuo *inter alia* siūloma panaikinti Direktyvą, todėl kaip tik dabar kyla neatidėliotinas poreikis dar kartą susisteminti ir įvertinti jos įgyvendinimo ir taikymo praktiką.

Šiame straipsnyje nagrinėjama tik viena iš elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų rūšių (Siūlomo reglamento 3 straipsnio 12 dalis) – elektroninis parašas. Straipsnyje siekiama atskleisti problemiškiausius Direktyvos įgyvendinimo vidaus rinkoje aspektus, identifikuoti svarbiausius Direktyvos ir jos įgyvendinimo trūkumus tose srityse, kurios turi reikšmingiausią įtaką tarpvalstybiniam elektroninio parašo veikimui (Direktyvos 4 straipsnio 2 dalis). Straipsnyje daugiausia dėmesio skiriama Direktyvos ir ją įgyvendinančių ES teisės aktų bei kitų dokumentų analizei, taip pat glaustai pateikiamas Pasiūlymo dėl Reglamento įvertinimas.

Direktyvos įgyvendinimo problematika pradėjo ryškėti nuo pat termino jai perkelti į valstybių narių teisę pabaigos (t. y. nuo 2001 m. liepos 19 d.). 2006 m. paskelbtoje Komisijos ataskaitoje apie Direktyvos veikimą [15] identifikuotos šios svarbesnės problemos: (a) valstybės narės pagal Direktyvos 3 straipsnį yra įgyvendinusios skirtingus sertifikavimo paslaugų tiekėjų priežiūros modelius; (b) saugus elektroninis parašas įsisavinamas labai lėtai, atsirado daug kitokių programų, kuriose naudojami paprastesni elektroniniai parašai; (c) techninės sąveikos trūkumas nacionaliniu ir tarptautiniu lygiu.

2010 m. elektroninio parašo tarpvalstybinio suderinimo studija [65] identifikavo iš esmės tas pačias problemas: (a) skirtingas valstybių požiūris į pamatines Direktyvos sąvokas, sukuriantis prielaidas vidaus rinkos segmentacijai (Direktyvos 4 straipsnis); (b) Direktyvos „*viešojo sektoriaus nuostatų*“ [1, 3 straipsnio 7 dalis] panaudojimas nustatant papildomus reikalavimus elektroniniams parašams viešajame sektoriuje (pvz., viešuosiuose pirkimuose ir pan.); (c) standartų sistema yra paini ir nebeatitinka rinkos dalyvių lūkesčių; (d) nacionalinės priežiūros režimai skiriasi valstybėse narėse [1, 2 straipsnio 13 dalis ir 3 straipsnio 3 dalis]. Komisijos užsakymu 2012 m. parengta Elektroninio identifikavimo, autentifikavimo ir parašo studija [63, p. 63–66], Direktyvos svarbiausias ydas identifikavo tose pačiose srityse. 2012 m. Komisijos pasiūlymo dėl reglamento poveikio vertinimo ataskaitoje [7] nurodomos dvi pagrindinės kliūtys teikiant tarpvalstybines patikimumo užtikrinimo paslaugas: (a) rinkos fragmentacija (paslaugų teikėjams taikomos skirtingos taisyklės, priklausiančios nuo to, kuriose valstybėse jie įsisteigę); ir (b) vartotojų pasitikėjimo stoka.

Rinkos fragmentacija ir kilmės valstybės principas

Direktyva kritikuojama tuo pagrindu, kad jos 4 straipsnyje įtvirtintas kilmės valstybės principas lėmė vidaus rinkos fragmentaciją [7]. Komisijos vertinimu, valstybės narės yra įgyvendinusios skirtingus kvalifikuotus sertifikatus išduodančių sertifikavimo paslaugų tiekėjų priežiūros modelius (Direktyvos 3 straipsnis), o šie skirtumai gali turėti įtakos teikiant tarptautines sertifikavimo paslaugas [7].

Visų pirma tokia Direktyvos kritika ne visada pagrįsta turint omenyje ribotą jos tikslą ir siaurą taikymo sritį. Direktyva nesiekta išspręsti absoliučiai visų elektroninio parašo veikimo aspektų, pvz., teisinių kliūčių sutartims sudaryti elektroniniu būdu panaikinimas reglamentuojamas Elektroninės komercijos direktyvos 9 straipsnyje [2]. Be to, pripažinta, kad šalia Direktyvos veikia ir šalių susitarimu nustatytos elektroninių parašų naudojimo sąlygos (Direktyvos preambulės 16 punktas).

Antra, tai, kad harmonizuotas elektroninio parašo sistemos veikimas vidaus rinkoje liko neįgyvendintas [žr.: 66, p. 3], daugiausia nulėmė netinkamas Direktyvos nuostatų perkėlimas nacionalinėje teisėje. Kilmės valstybės principas (angl. *countryoforigin*) nuosekliai lemia tai, kad sertifikavimo paslaugų teikėjai skirtingose valstybėse narėse susiduria su skirtingomis priežiūros (todėl ir veiklos) sąlygomis. Direktyva priskiriama toms ankstesnio tipo direktyvoms, kuriomis, siekiant minimalaus harmonizavimo, buvo nustatyti tam tikri minimalūs reikalavimai, privalomi visiems ES vidaus rinkoje veikiantiems subjektams [49, p. 12]. Kilmės valstybės koncepcija yra kompromisinis paslaugų judėjimo vidaus rinkoje reglamentavimo principas ir todėl vargu ar gali būti kritikuojama kaip savaime ribojanti elektroninio parašo sistemos veikimą peržengiant vienos valstybės ribas. Vis dėlto kilmės valstybės principas įvairiose valstybėse narėse įgyvendintas skirtingai, jose skiriasi užsienio teikėjų išduotų sertifikatų pripažinimo techninės ir teisinės sąlygos. Lietuvos Respublikos elektroninio parašo įstatymo [25] (toliau – Įstatymas) 5 straipsnio 1 dalyje numatomos užsienio valstybių sertifikavimo paslaugų teikėjų sudarytų kvalifikuotų sertifikatų pripažinimo Lietuvoje sąlygos (t. y. sertifikatai yra sudaryti paslaugų teikėjo, akredituoto Lietuvoje arba kitoje valstybėje, arba už sertifikatą laiduoja Lietuvos arba kitos ES valstybės kvalifikuotus sertifikatus išduodantis paslaugų teikėjas, atitinkantis Lietuvoje taikomus reikalavimus), kurie ne visai dera su Direktyvos 4 straipsniu. Nors Lietuvoje jau nuo 2006 m. naudojamasi užsienio valstybių sertifikavimo paslaugų teikėjų sudarytais kvalifikuotais sertifikatais [57][1], tačiau sunku įvertinti, kiek problemų ši Įstatymo nuostata sukėlė praktikoje. Kai kurios Lietuvos valstybės institucijos užsienio kvalifikuotų sertifikatų pripažinimą sprendžia individualiai (pvz., pačios patikrina sertifikavimo paslaugų teikėjus ir jų išduodamus sertifikatus ir įtraukia į savo sąrašus). Manytina, kad užsienio sertifikavimo paslaugų teikėjų identifikavimą, jų išduodamų sertifikatų patikrinimą ir pripažinimą turėtų gerokai palengvinti Komisijos sprendimo 2009/767/EB [6] (toliau – Komisijos sprendimas 2009/767/EB) 2 straipsnio 1 dalyje numatoma priemonė – valstybių narių sudaromi patikimi sąrašai (angl. *trusted services lists, TLS*) [plačiau žr.: 67], kuriuose pateikiama informacija apie tos valstybės narės prižiūrimus ir (arba) akredituotus sertifikavimo paslaugų teikėjus, išduodančius kvalifikuotus sertifikatus, įskaitant informaciją apie tai, ar parašas kuriamas naudojant saugią parašo formavimo įrangą (tai gali būti nurodyta ir pačiuose sertifikatuose, o jei ne – pateikta kaip atskira informacija sąraše). Iki šiol tokios galimybės patikrinti

[1] UAB „Omnitel“ mobiliųjų telefonų SIM kortelėse yra įrašiusi kvalifikuotų sertifikatų, iš kurių daugumą sudarė Estijos sertifikavimo paslaugų teikėjas AS „Sertifitseerimiskeskus“.

kitoje valstybėje narėje išduotus sertifikatus nebuvo dėl skirtingų nacionalinių techninių reikalavimų, įskaitant ir skirtingo sertifikatų formato. Lietuvos nacionalinės priežiūros institucijos – Ryšių reguliavimo tarnybos – tinklalapyje yra skelbiamas prižiūrimų ir (ar) akredituotų sertifikavimo paslaugų teikėjų patikimas sąrašas.

Trečia, priekaištai, kad valstybės narės yra įgyvendinusios skirtingus sertifikavimo paslaugų tiekėjų priežiūros modelius, tiesiogiai nepaaiškina, kodėl vidaus rinka iki šiol yra susiskaidžiusi į atskiras nacionalines rinkas. Vis dėlto tokią fragmentaciją gali paaiškinti tarp priežiūros režimų egzistuojantys skirtumai, kurių negalima pavadinti formaliais – nors daugelyje valstybių vykdomas periodinis paslaugų teikėjų patikrinimas, kai kuriose valstybėse apskritai nėra prieinamos informacijos apie tokius patikrinimus arba jie atliekami tik kilus pažeidimų grėsmei [7, taip pat žr.: 48, p. 101–103]. Sertifikavimo paslaugų teikėjams taikoma priežiūros tvarka turi tenkinti Direktyvos reikalavimus, išdėstytus 3 straipsnio 3 dalyje, 8 straipsnio 1 dalyje ir 11 straipsnyje, o Direktyvos II Priede yra įtvirtinti išsamūs reikalavimai sertifikavimo paslaugų teikėjams, tačiau pačioje Direktyvoje nėra jokių detalesnių nurodymų ar gairių valstybėms narėms. Direktyvos įgyvendinimas atskleidė, kad kilmės valstybės principas turėjo būti nuosekliai derinamas su išsamesniu minimalių reikalavimų sertifikavimo paslaugų teikėjams ir priežiūros tarnyboms sąrašu, taip pat su aktyvių pareigų valstybėms narėms įtvirtinimu pačioje Direktyvoje (vietoje kompromisinių reikalavimų Direktyvos 3 straipsnyje ir pan.). Komisija, įvertinusi Direktyvos įgyvendinimo praktiką, galėjo išleisti gaires ar rekomendacijas valstybėms narėms[2]. Gana pavėluotai, 2010 m. Komisijai CROBIES projekto rėmuose buvo pateiktas pasiūlymas dėl bendrojo kvalifikuotus sertifikatus išduodančių sertifikavimo paslaugų teikėjų priežiūros modelio [68].

Prie kilmės valstybės principo nulemiamo rinkos susiskaldymo priskirtinos ir Direktyvos „viešojo sektoriaus nuostatos“ (Direktyvos 3 straipsnio 7 dalis), kurios valstybėms narėms leidžia įtvirtinti papildomus reikalavimus viešajame sektoriuje. Šių nuostatų taikymas labiausiai paplitęs valstybėms narėms taikant skirtingus reikalavimus viešųjų elektroninių pirkimų elektroniniams parašams. Tiesa, ne visada tie reikalavimai yra susiję su kvalifikuotu parašu, pvz., Lietuvoje veikiančios perkančiosios organizacijos, vykdančios pirkimus esant elektroninio parašo reikalavimui, numato, kad elektroninėmis priemonėmis teikiami pasiūlymai ar paraiškos turi būti pateikti su **saugiu elektroniniu parašu** (t. y. formaliai nereikalaujama kvalifikuoto elektroninio parašo), atitinkančiu Įstatymo nustatytus reikalavimus ir CVP IS[3] naudojamus elektroninių parašų

[2] Tiesa, tokia teisinė schema yra kaip standartas – paslaugų teikėjai turi atitikti ETSI (TS 101 456) standarto [21] reikalavimus, kvalifikuotus sertifikatus sudarantiems paslaugų teikėjams. Atitiktį kvalifikuoto sertifikato politikai, kuria įgyvendinamas minėtas standartas, gali patvirtinti (a) tinkamai įgaliotas auditorius (gali būti vidinis, tačiau hierarchiškai nepavaldus sertifikavimo paslaugų teikėjui); (b) įvertinimas, atliktas kompetentingo nepriklausomo auditoriaus. Atitiktis turi būti tikrinama reguliariai, taip pat įvykus veiklos pokyčių.

[3] Centrinė viešųjų pirkimų informacinė sistema: https://pirkimai.eviesiejipirkimai.lt/login.asp?B=PPO&target=&timeout=. Tiesa, CVP IS nepalaiko „mobiliųjų“ elektroninių parašų (teisiniu požiūriu mobiliojo elektroninio parašo sąvoka nėra vartotina, nes ji pagrįsta tik parašo formavimo įrangos technologija, o ne teisinius padarinius lemiančiomis elektroninio parašo savybėmis), kurie paremti kvalifikuotais sertifikatais,

tipus. Prancūzijoje viešuosiuose pirkimuose taip pat leidžiama naudoti net ir nekvalifikuotus sertifikatus, tačiau teikėjui keliami reikalavimai būti akredituotam pagal Prancūzijoje galiojančias taisykles, taikomas vietiniams sertifikavimo paslaugų teikėjams [43, p. 20]. Kai kuriose valstybėse nustatyti reikalavimai dalyviams naudoti kvalifikuotą sertifikatą, patvirtintą sertifikatu išduotu akredituoto sertifikavimo paslaugų teikėjo [48, p. 99]. Direktyvos 3 straipsnio 7 dalyje įtvirtinta „viešojo sektoriaus“ išimtis gali būti taikoma tik esant objektyviems pagrindams, o patys reikalavimai turi būti proporcingi, skaidrūs ir nediskriminaciniai. Vis dėlto Komisija iš esmės netikrino, kaip valstybės narės laikosi šių principų – „viešojo sektoriaus“ išlygos, kurios imtos taikyti ankstyvuoju Direktyvos įgyvendinimo laikotarpiu, nulėmė nacionalinių elektroninio parašo salelių susiformavimą vidaus rinkoje.

Su kilmės valstybės principu glaudžiai susijusios ir Direktyvos nuostatos dėl sertifikavimo paslaugų teikėjų akreditavimo. Direktyvos 3 straipsnio 2 dalyje teigiama, kad valstybės narės gali įdiegti arba išlaikyti savanoriškos akreditacijos sistemas, kurių tikslas – geresnė sertifikavimo paslaugų teikimo kokybė. Direktyvos 2 straipsnio 13 dalyje savanoriška akreditacija apibrėžiama kaip leidimas, nustatantis su sertifikavimo paslaugų teikimu susijusias teises ir pareigas, kuriomis paslaugų teikėjas neturi teisės naudotis iki kompetentingos institucijos sprendimo jį išduoti.

Direktyvos rengėjai manė, kad savanoriška akreditacija bus naudinga rinkai, nes suteiks paslaugų teikėjams galimybę pademonstruoti savo paslaugų saugumo ir patikimumo lygį [8, p. 6]. Vis dėlto valstybėse narėse iki šiol skiriasi ne tik savanoriškos akreditacijos schemos įgyvendinimo procedūros, bet ir jos teisiniai padariniai ir reikšmė sertifikavimo paslaugų teikėjų veiklai. Akreditacijos schemos, taikytos kaip būtina sąlyga dalyvauti nacionaliniuose elektroninės vyriausybės projektuose, *de facto* tapo privalomais reikalavimais visiems paslaugų teikėjams, o tai aiškiai prieštarauja Direktyvai (pvz., reikalavimas Prancūzijoje sertifikavimo paslaugų teikėjui būti akredituotam pagal Prancūzijoje galiojančias taisykles). Taigi, vien tai vietiniams sertifikavimo paslaugų teikėjams, palyginti su užsienio teikėjais, sukuria palankesnes veiklos sąlygas ir iškreipia valstybės kilmės principo esmę. Privaloma akreditacija gali būti savaime aiškinama kaip diskriminacijos forma bent jau tų valstybių narių atžvilgiu, kuriose tokia schema apskritai neveikia [43, p. 21], todėl akreditaciją reikėjo orientuoti į regioninę, o ne į nacionalinę [48, p. 10]. Savanoriškos akreditacijos idėjos valstybės narės taip ir nesuprato (ar nebuvo suinteresuotos suprasti), o ja pasinaudojo kaip papildoma priemone apginti savo nacionalinę rinką (sertifikavimo paslaugų teikėjus).

2. Elektroninio parašo sąvoka ir teisinis statusas

Direktyvos 2 straipsnyje elektroninis parašas apibrėžiamas gana lakoniškai – tai elektronine forma pateikti duomenys, kurie yra prijungti ar logiškai susieti su kitais elektroniniais duomenimis ir gali būti naudojami kaip autentifikavimo priemonė. Ši sąvoka apima platų duomenų autentikavimo technologijų spektrą (Direktyvos preambulės 8 punktas). Kai kurie mokslininkai mano, kad elektroninio parašo

o tai sukelia praktinių apribojimų, stokojančių teisinio pagrįstumo.

sprendimai pagal Direktyvą turi apimti ir tokias priemones kaip PIN (angl. *personal identification number*) kodus, vardą ir pavardę elektroninio pranešimo gale, skenuotą parašą [61, p. 154], elektroninės bankininkystės priemones, ką jau kalbėti apie viešųjų raktų infrastruktūros (PKI) kriptografines ar biometrines priemones [59, p. 9].

Parašo koncepcija yra itin glaudžiai susijusi su popierinio dokumento samprata, todėl istoriškai elektroninio parašo funkcijas pradėta konstruoti būtent pagal tradicinio parašo atliekamas funkcijas, atsižvelgiant į elektroninio dokumento ypatumus [55, p. 26]. UNCITRAL Pavyzdinio elektroninio parašo įstatymo rengėjai visoms svarbiausioms tradicinio parašo funkcijoms surado ekvivalentes elektroninio parašo savybes (Direktyvos preambulės 8 punktas; [23, p. 10, 43]; [žr. plačiau: 22, p. 20]). Vis dėlto funkcinio ekvivalentiškumo koncepcija, kurią sukūrė ir pagrindė teisininkai, ilgainiui lėmė, kad elektroninio parašo koncepcija, kurią nuo pat pradžių iš esmės kūrė techninių mokslų atstovai, imta tapatinti su teisine parašo samprata, o tai sukėlė painiavą ir net teisinio ir technikos pasaulio atstovų nesusikalbėjimą.

Bendriausiu teisiniu požiūriu parašas įgyvendina dvi funkcijas: leidžia patikrinti pasirašančio asmens tapatybę ir užtikrinti, kad jis patvirtino pasirašytus duomenis (t. y. save susiejo su jais) [22, 7 straipsnis]. Vis dėlto Direktyvos rengėjai kaip esminę elektroninio parašo funkciją pasirinko būtent [duomenų] autentifikaciją. Autentifikaciją techniniu požiūriu galima apibrėžti kaip atributų, požymių rinkinio ar faktų patikrinimą tam tikru patikimumo lygiu [63, p. 9]. Teisės literatūroje „autentifikacija“ gali reikšti (a) asmens sutikimą, patvirtinimą, kad jis sutinka su pasirašytu turiniu, jį priima kaip savo pasirašytą [42, p. 142]; (b) oficialų patvirtinimą, kad dokumentas laikytinas priimtinu įrodymu [42, p. 142]; (c) padarymą autentiško, suteikiant autoritetą (galią) [75]. Reikia pripažinti, kad duomenų autentifikavimas, kaip kertinė elektroninio parašo funkcija, pabrėžtinai svetima tradicinei ir kartu teisinei parašo sampratai.

Taigi, teisiniu požiūriu pradėjo ryškėti takoskyra tarp duomenų autentifikavimo (pvz., duomenų vientisumo patvirtinimas) ir asmens autentifikavimo (pvz., asmens tapatybę nusakančių požymių patikrinimas ir patvirtinimas). Oficialiai pripažįstama, kad į Direktyvos apimtį patenka tik sprendimai, atliekantys duomenų autentifikavimo funkciją [48, p. 29]. Toks ribotas ir gana techninis elektroninio parašo apibrėžimas Direktyvoje lėmė įvairius nesusipratimus. Pirma, techninis sąvokos elementas (pagrįstas duomenų autentifikavimo) ir teisinis (pagrįstas tradicinio parašo funkcijomis ir asmens autentifikavimo) sąvokos elementas tapo nebesuderinami tarpusavyje – duomenų autentifikavimas, kaip skaitmeninio parašo funkcija, pati savaime niekaip neskirta išspręsti asmens identifikacijos (teisingiau, verifikacijos) klausimo. Teisiniu požiūriu, nors asmens susiejimas su tradiciniu parašu pasirašomu tekstu ir nėra tiesiogiai susijęs su jo tapatybės nustatymu (t. y. iš asmens parašo sutarties šalis gali spręsti tik apie parašą fiziškai uždėjusio asmens (pasirašytojo) sutikimą būti susietam su pasirašomo dokumento turiniu, tačiau asmens tapatybės patikrinimas vien tik pagal parašą neįmanomas), *pasirašytojo* tapatybės patvirtinimas pasirašant ant popieriaus yra neatskiriama nuo tradicinio parašo savasties. Antra, elek-

troninio parašo sąvoka imta tapatinti su technine sąvoka, kuri yra pagrįsta duomenų autentifikavimu PKI pagalba. Trečia, techninėje elektroninio parašo sąvokoje nėra asmens sutikimo būti susietam su pasirašomu dokumentu elemento – joje glūdi tik loginis ir techninis parašo duomenų susiejimas su pasirašomais duomenimis, o teisinis elementas pabrėžia būtent valinį ir sąmoningą asmens (t. y. ne tiek fizinio pasirašytojo, kiek sandorio šalies) susiejimą su dokumento turiniu per fizinį, aktyvų veiksmą – pasirašomą tekstą popieriuje ar kitoje laikmenoje (tiesa, elektroninio parašo sudėtyje gali būti papildomi elementai, leidžiantys išreikšti asmens ryšį su pasirašomu dokumentu). Neatsitiktinai pastaruoju metu imta siūlyti, kad europinė elektroninio parašo sąvoka turėtų labiau orientuotis į teisinę dimensiją – apimti ir pasirašančio asmens sutikimo išraišką [63, p. 10].

Su autentifikacija glaudžiai susijusi identifikacijos sąvoka. Identifikacija apibrėžtina kaip asmens tapatybės įrodymas [42, p. 761], tapatumo, atitikties nustatymas, atpažinimas [74, p. 394]. Įdomu, kad Direktyvoje asmens identifikavimas nėra išskiriamas kaip elektroninio parašo funkcija, o asmens tapatybės nustatymas nurodomas kaip viena iš saugaus parašo funkcijų (Direktyvos 2 straipsnio 2 dalies b) punktas). Teisiniu požiūriu svarbu atskirti asmens tapatybės nustatymą (identifikaciją *stricto sensu*) nuo asmens tapatybės patikrinimo (verifikacijos) [50, p. 252]. Identifikacija reiškia asmens tikrosios tapatybės nustatymą, o verifikacija tik patvirtina, kad du ar keli duomenys yra susiję ir atitinka tą patį asmenį (asmens tapatybė patikrinama pagal nuotrauką asmens tapatybės dokumente arba personalizuotomis priemonėmis (pvz., pagal ID numerį, PIN kodą, slaptažodį). Paprastai pirminį asmens identifikavimą vykdo tas, kuris išduoda asmeniui tapatybės dokumentus, o elektroninis parašas *stricto sensu* asmens identifikavimo funkcijos neatlieka – jis leidžia atlikti asmens autentifikavimą. Direktyva (2 straipsnio 3 punktas) pasirašantįjį asmenį apibrėžia kaip asmenį, kuris turi parašo formavimo įrangą, taip netiesiogiai išskirdama faktinį parašo formavimo įrangos valdymą, kaip pakankamą asmens indentifikavimo pasirašančiuoju asmeniu kriterijų. Taigi, teisiniu požiūriu identifikacija atitiktų techninę asmens autentifikavimo sampratą, tačiau tenka apgailestauti, kad identifikacijos terminas tiek Komisijos dokumentuose, tiek valstybių narių įstatymuose perkeltas itin įvairiai ir dažnai klaidingai (ne išimtis ir Lietuva, kurios Įstatymo 2 straipsnio 4 dalyje įtvirtina identifikacijos funkcija turi asmens autentifikavimo reikšmę).

Direktyvos požiūriu elektroninis parašas nėra ir negali būti tradicinio parašo atitikmuo. Turi būti daromas skirtumas tarp teisinės „parašo“ sąvokos, kuri savyje sukaupia reikšmingą teisinių padarinių krūvį, ir techninės „elektroninio parašo“ sampratos, kuri apima įvairiausius veiksmus ar procesus, kuriuose ne visada dalyvauja žmogus ir kuriais nebūtinai siekiama teisinių parašo padarinių [23, 94 paragrafas] (pvz., duomenų autentifikavimas naudojamas teikiant automatizuotus užsakymus, patvirtinimu, išrašant sąskaitas [60, p. 15]).

Manytina, kad Direktyva, esanti takoskyroje tarp teisės ir technologijos, sujungia teisines ir technologines definicijas ir duomenų autentifikacijos sąvoką vartoja plačiuoju požiūriu, kaip apimančią tiek asmens tapatybės nustatymo ir patvirtinimo,

tiek pasirašiusio asmens neatšaukiamo susiejimo su pasirašomais duomenimis požymius [15], todėl elektroninis parašas pagal savo esmę turėtų atlikti mažiausiai dvi funkcijas: identifikuoti asmenį ir patvirtinti jo ketinimą būti susietam su pasirašomais duomenimis [23, 7 straipsnis], o vien tik identifikavimą atliekančios priemonės *pačios savaime* neturėtų būti laikomos elektroniniu parašu[4]. Be abejo, identifikavimui skirtos priemonės valiniais asmens (pvz., vartotojo, sistemos naudotojo) veiksmais gali atlikti ir likusią „autentifikacijos" funkcijos dalį, pagrįstą ne tik asmenybės atributų patikrinimu, bet ir valios išraiškos patvirtinimu. Reikia pripažinti, kad minėtas elektroninio parašo funkcijų atskyrimas iš esmės turi tik koncepcinę prasmę, o grynas jis paprastai neegzistuoja – pvz., vien identifikacijai skirtos elektroninės priemonės gali papildyti vėlesnius asmens veiksmus ir taip sukurti teisiškai reikšmingą sąsajumą su jais[5].

Komisija 2006 m. Direktyvos veikimo ataskaitoje [15] turėjo galimybę paaiškinti, kad Direktyva, nutolstant nuo 1996 m. UNCITRAL Elektroninės komercijos pavyzdiniame įstatyme [22] įtvirtintos funkcinio ekvivalentiškumo koncepcijos, nebuvo siekiama sukurti tradicinio parašo elektroninio analogo, o vietoje to buvo siekiama sukurti praktiškesnį, į elektroninės komercijos dalyvių poreikius orientuotą *sui generis* funkcijas atliekantį elektroninį parašą. Vietoje to, į valstybių teisines sistemas buvo nutransliuotas sprendimo, kuris teisinėje sistemoje būtų funkciškai ekvivalentus tradiciniam parašui, orientyras. Direktyva nepateikia aiškaus atsakymo į klausimą, kokiu lygiu elektroninio parašo duomenys turi būti susieti su pasirašomais duomenimis. Jeigu susiejimas turi atitikti saugaus parašo lygį, t. y. kad bet koks pasirašytų duomenų pakeitimas būtų pastebimas (2 straipsnio 2 p., d) punktas), šis požymis būtų neužtikrinamas tokiomis priemonėmis, pvz., vardo, pavardės parašymas po elektroniniu pranešimu, nors jie formaliai ir būtų susiję su pasirašomu tekstu. Reikėtų pripažinti, kad Direktyvos dvasioje glūdi elektroninio parašo formų pliuralizmas, todėl vieną ar kitą sprendimą pripažįstant elektroniniu parašu neturėtų būti reikalaujama, kad elektroninio parašo duomenys būtų neatskiriamai susiję su pasirašomais duomenimis[6].

Direktyvos 5 straipsnio 2 dalyje įvirtintas elektroninio parašo formų nediskriminavimo reikalavimas turėjo įteisinti įvairiausius Direktyvą atitinkančius sprendimus. Reikia apgailestauti, kad Direktyvos rengėjai taip ir nesugebėjo atsikratyti skaitmeniniu parašu (skaitmeniniai parašai yra naudojami viešojo rakto infrastruktūros (PKI) kontekste, naudojant asimetrinio rakto kriptografiją [51, p.7]) grįstos elektroninio parašo paradigmos. Nors Direktyvos preambulės 8 punkte ir deklaruojamas siekis plėtoti atvirą ir neutralų požiūrį į elektroninio duomenų autentiškumo patvirtinimo technologijas ir paslaugas, kaip parodė vėlesnė Komisijos pozicija ir valstybių narių požiūris į Direktyvą, jos sisteminį pamatą sudarė būtent kvalifikuotas

[4] Be abejo, tokios priemonės (pvz., PIN kodas) gali turėti sutartinio parašo galią (Įstatymo 8 straipsnio 3 dalis, Direktyvos 5 preambulės 16 punktas).

[5] Pvz., internetinės bankininkystės duomenys gali būti naudojami tiek kliento tapatybei patikrinti, tiek jo valiai išreikšti sudarant banko indėlio sutartis ir pan.

[6] Kaip įdomus pavyzdys paminėtinas Vengrijos įstatymas [33], kuriame įsakmiai reikalaujama, kad elektroninio parašo duomenys būtų logiškai neatsiejamai susieti su pasirašomais duomenimis (įstatymo 2 straipsnio 6 dalis).

elektroninis parašas. Ironiška tačiau Komisijos 2011 m. viešosios konsultacijos klausimyne, skirtame rinkos dalyviams [17], išvardijama 11 probleminių elektroninio parašo reguliavimo sričių, kurios susijusios tik su saugiu skaitmeniniu parašu.

Atrodytų, kad Direktyvoje įtvirtintą elektroninio parašo sąvoką kūrė informacinių technologijų specialistai, o teisininkai ją viso labo įvilko į Direktyvos teisinį rūbą. Iš čia ir kilęs šių dviejų sričių atstovų nesusikalbėjimas. Lietuvos teisinėje sistemoje turime gana iškalbingą pavyzdį, esantį CK 1.76 straipsnyje, kai kodifikuotos civilinės teisės normos *de jure* įtvirtina technologiškai neutralų, o *de facto* – skaitmeniniu parašu pagrįstą elektroninį parašą (nes reikalauja identifikuoti asmenį). Šitoks teisinės sistemos paradigmoje užkoduotas nepasitikėjimas technologiniais sprendimais taip pat prisidėjo prie to, kad įstatymų leidėjas instinktyviai kelia papildomus reikalavimus elektroniniam parašui ir apskritai rašytiniams sandoriams elektroniniu formatu (pvz., rašytiniams dokumentams elektroniniame dokumente specifiškai kelia parašo reikalavimą, nors tokio reikalavimo dokumentams popieriniame formate nekelia). Tokie papildomi reikalavimai elektroninį parašą padarė sunkiai įgyvendinamą praktiškai ir taip neleistinai iškreipė ilgus amžius kurtą dokumento ir sandorio formos užtikrinimo išlaidų ir jo suklastojimo rizikos pusiausvyrą.

Tiesa, Komisijos sprendimo 2009/767/EB 1 straipsnyje įtvirtinama valstybių narių teisė, atliekant administracinius formalumus ir procedūras pagal Paslaugų direktyvos 2006/123/EB 8 straipsnį [3, p. 36], pripažinti saugius elektroninius parašus, kurie gali būti sukurti nenaudojant saugios parašo formavimo įrangos, ar net parašus, kurie nėra saugūs parašai, pagrįsti kvalifikuotais sertifikatais ir sukurti nenaudojant saugios parašo formavimo įrangos (1 straipsnio 4 dalis). Būtų sveikintina, jeigu toks pažangus požiūris į skirtingo saugumo ir skirtingų formų elektroninio parašo panaudojimą būtų išplėstas apimant visas panaudojimo sritis vidaus rinkoje.

3. Skirtingos nacionalinės teisinės kategorijos

Kai kurios valstybės narės sukūrė „nacionalinę“ elektroninio parašo terminiją, kuri atitinka arba vieną iš Direktyvos numatytų elektroninio parašo rūšių, arba funkcionuoja kaip papildoma į Direktyvą patenkančių rūšių atmaina. Pvz., Bulgarijoje įvestas universalaus elektroninio parašo terminas (t. y. kvalifikuotas elektroninis parašas, pagrįstas sertifikatu, kurį išduoda pagal specialią tvarką registruoti sertifikavimo paslaugų teikėjai), Lenkijoje įtvirtinta saugaus elektroninio parašo sąvoka (skiriasi nuo *advanced* (t. y. pažangaus) elektroninio parašo termino), Slovakijoje žinoma garantuoto elektroninio parašo sąvoka. Nors kai kurie skirtumai tėra etimologiniai (pvz., Lietuvoje saugus elektroninis parašas yra visiškai tapatus Direktyvos 2 straipsnio 2 dalyje numatytam pažangiam elektroniniam parašui), kitur tie skirtumai gali sukurti realias kliūtis vidaus rinkai, pvz., nacionaliniuose įstatymuose numačius reikalavimus viešojo pirkimo procedūrų dalyviams pateikiamus elektroninius dokumentus pasirašyti kitoje valstybėje nežinoma, o Direktyvoje aiškiai nesureguliuota parašo rūšimi (pvz., iki 2011 m. liepos 1 d. Bulgarijos įstatyme [žr. 32, 13 straipsnio 3 dalis] buvo įtvirtinta universalaus elektroninio parašo, kuriam

suteikiama visuotinė ir automatinė teisinė parašo galia visuose teisiniuose santykiuose, sąvoka tiesa, 2011 m. liepos 1 d. įsigalioję įstatymo pakeitimai panaikino šią sąvoką ir ją pakeitė Direktyvą atitinkančia kvalifikuoto elektroninio parašo sąvoka).

Įdomu, kad Įstatyme elektroniniu parašu pripažįstamos ir vien asmens identifikavimo (teisingas būtų asmens autentifikavimo terminas) funkciją atliekančios technologijos [25, 2 straipsnio 4 dalis]. Manytina, kad toks platus įstatymų leidėjo požiūris suteikė pozityvų postūmį elektroninio parašo raidai Lietuvoje – iki pat 2005 m. elektroninės bankininkystės sistemos iš esmės buvo vienintelės naudojamo elektroninio parašo apraiškos. Be to, nors technologija, paremta įslaptintu PIN kodu, *stricto sensu* ir nėra pripažintina elektroniniu parašu, tačiau teisiniu požiūriu ji tokia buvo pripažinta 2002 m. Lietuvos Aukščiausiojo Teismo nagrinėtoje byloje *Ž. Šapalas v. AB „Lietuvos taupomasis bankas“* [35][7]. Direktyvos požiūriu toks elektroninio parašo supratimas nacionalinėje teisėje neturėtų būti peikiamas, nors galėtų kelti tarpvalstybinio panaudojimo teisinių garantijų, išplaukiančių iš Direktyvos 4 straipsnio, klausimą.

Parašo sąvokai skirtingose valstybėse suteikiama skirtinga teisinė reikšmė, susiformavusi savitoje teisinėje sąmonėje, o „elektroninio parašo“ prigimtis suteikia tik netiesioginę sąsają su „tikru“, tradiciniu parašu, todėl reikalavimai tradiciniam parašui gali lemti sunkumus juos pritaikant elektroninėms pasirašymo priemonėms. Tradicinis parašas pasirašiusį asmenį susieja su pasirašytu dokumentu, o elektroninis parašas viso labo susieja vienus duomenis su kitais – trūkstamą grandį pateikia teisinė prezumpcija, kuri nustato asmens susiejimo su parašo formavimo priemonėmis taisyklę. Elektroninio parašo sprendimai teikia galimybę asmens tapatybę nustatyti pagal tai, kokias priemones jis kontroliuoja [72]. Kadangi parašo formavimo duomenų ir priemonių kontrolė tik pasirašiusiojo valia yra vienas iš būtinųjų saugaus parašo atributų (Direktyvos 2 straipsnio 2 punkto, d) papunktis), o elektroninio parašu pasirašomi duomenys susiejami su privačiu raktu, kuris yra saugomas kompiuterio diske ar kitoje fizinėje laikmenoje (pvz., kortelėje), kyla tokios laikmenos kontrolės ir naudojimo tik privačiajam raktui saugoti klausimas (žr. plačiau: 58, p. 308].

Šiuo požiūriu įdomus 2009 m. Italijos Vicenza miesto teismo sprendimas [41] – kadangi įstatymų leidėjas teisinę galią siekė suteikti tik originaliems asmens *skaitmeniniu parašu* pasirašytiems įmonės akcijų perleidimo dokumentams, šį reikalavimą būtina taikyti taip, kaip jis taikomas pagal tradicines „popierinių“ sandorių taisykles. Kalbant apie notarinio patvirtinimo reikalavimą, jis apima realios pasirašiusio asmens tapatybės nustatymą, o kadangi skaitmeninio parašo formavimo procedūra to neužtikrina, norint, kad ji visiškai atitiktų įstatymo reikalavimus parašui, ją būtina papildyti tokiomis priemonėmis, kaip antai skaitmeninio parašo, atliekamo notaro akivaizdoje, patvirtinimas ir pan.

Valstybių nacionalinių įstatymų taikymo praktika ir istorija tradiciniam parašui gali kelti specifinius procedūrinius reikalavimus, pvz., tradiciškai civilinės teisės tradicijos valstybėse (pvz., Prancūzijoje, Vokietijoje), teisinė parašo sąvoka apėmė tik ranka atliktus parašus [48, p. 29],

[7] Teisingiau, PIN kodas gali būti laikomas ne pačiu elektroniniu parašu, o parašo formavimo įranga.

o bendrosios teisės tradicijos valstybėse (Jungtinėje Karalystėje, Airijoje) apskritai netaikomi dideli reikalavimai parašui (pvz., parašu pripažįstamas ir spaudas).

Taigi valstybės narės įstatymuose įtvirtinta elektroninio parašo sąvoka gali pažodžiui atitikti Direktyvą, tačiau turėti skirtingą turinį. Be to, nacionaliniai reikalavimai parašui ar jo atliekamoms funkcijoms gali lemti, kad vienoje valstybėje sukurtas elektroninis parašas bus pripažįstamas kitoje valstybėje kaip galiojantis elektroninis parašas, tačiau jo teisinė galia bus kvestionuojama.

Savita nacionalinė elektroninio parašo galia neatsiejamai susijusi su tais padariniais, kuriuos sukėlė Direktyvos 5 straipsnyje puoselėjamas funkcinio ekvivalentiškumo principas. Direktyva nesiekiama elektroniniam parašui suteikti savarankiškos, autonomiškos teisinės galios, kuri būtų vienodai suprantama ir sukeltų vienodus teisinius padarinius vidaus rinkoje. Direktyva valstybės nares įpareigojamos užtikrinti, kad kvalifikuotas elektroninis parašas būtų traktuojamas taip pat kaip ir ranka atliktas tradicinis parašas, tačiau tiesiogiai nereguliuojama elektroninio parašo naudojimo teisinių padarinių, tai paliekama nacionalinei teisei.

Darytina išvada, kad funkcinis ekvivalentiškumas, kaip pradžios koncepcija, leidžianti parinkti tinkamiausią elektroninio parašo vietą kiekvienos valstybės narės teisinėje sistemoje, pasirodė sunkiai suderinama su derinamąja Direktyvos prigimtimi. Deja, iš siūlomo Reglamento galima prielaida, kad šis disonansas iki šiol nėra girdimas Komisijos koridoriuose.

4. Kvalifikuotas elektroninis parašas

Nepaisant Direktyvoje deklaruojamo atvirumo įvairioms elektroninio parašo formoms, aiškesnę teisinę galią Direktyva garantuoja tik saugiam (arba patobulintam – angl. *advanced electronic signature*) elektroniniam parašui, atitinkančiam keturis Direktyvos 2 straipsnio 2 dalies reikalavimus: unikalumą, identifikavimą, saugumą (kontrolę tik pasirašytojo valia) ir integralumą [23, 6 straipsnio 3 dalis].

Be to, Direktyvos 5 straipsnio 1 dalyje įsitvirtino dar viena elektroninio parašo rūšis, kuri ne tik remiasi saugiu elektroniniu parašu, bet papildomai atitinka du specialius reikalavimus: paremtas kvalifikuotu sertifikatu ir sukurtas saugia parašo formavimo įranga. Šios rūšiese-parašo teisinė galia yra labiausiai apibrėžta: jis (a) laikomas atitinkančiu parašo teisinius reikalavimus dėl elektronine forma pateiktų duomenų taip pat kaip rašytiniai parašai atitinka tokius reikalavimus dėl duomenų popieriuje ir (b) yra leistinas įrodymas teisme[8]. Doktrina šią elektroninio parašo rūšį pakrikštijo kvalifikuotu elektroniniu parašu, kuris savo esme yra savybių rinkinys, būdingas tik skaitmeniniam parašui [58, p. 118]. Direktyva šiai elektroninio parašo kategorijai siejant su elektroniniais duomenimis aiškiai ir besąlygiškai suteikia tokį pat teisinį statusą koks yra suteikiamas

[8] Direktyvos nuostata 5 straipsnio 1 dalyje yra perteklinė – visose valstybėse elektroniniai įrodymai yra priimtini, tačiau reikšmingiausias yra jų svorio ir vertės kiekvienoje byloje klausimas, o Direktyvos preambulės 21 punkte nustatyta, kad Direktyva neriboja nacionalinio teismo teisės priimti sprendimą dėl jos reikalavimų atitikties ir neturi įtakos nacionalinėms taisyklėms, reglamentuojančioms nesuvaržyto įrodymų svarstymo teisme.

parašui popieriniame dokumente – visais atvejais, kai siejant su popieriniais dokumentais būtų pakankamas tradicinis parašas, kvalifikuotam parašui valstybės narės privalo suteikti ekvivalentį teisinį statusą. Kita vertus, valstybės gali įtvirtinti reikalavimus, viršijančius kvalifikuoto elektroninio parašo saugumo lygį (pvz., notarinio patvirtinimo reikalavimas).

Tarp rinkos dalyvių gajus mitas, kad kvalifikuotas elektroninis parašas yra vienintelis teisiškai galiojančio elektroninio parašo atitikmuo [48, p. 18], negali būti vertinamas kaip pagrįstas: Direktyvos 5 straipsnio 2 dalyje valstybės narės aiškiai įpareigojamos užtikrinti, jog nebūtų panaikinta elektroninio parašo teisinė galia ir jo kaip įrodymo leistinumas teisme vien tik dėl to, kad jis *inter alia* nėra paremtas kvalifikuotu sertifikatu, nėra sukurtas naudojant saugią parašo formavimo įrangą. Pagal Direktyvos 5 straipsnio 2 dalį paneigti elektroninio parašo galią galima tik tokiais pagrindais, kurie būtų nesusiję su konkrečia technologija, pvz., valstybės galėtų nepripažinti „paprasto elektroninio parašo“ tokiais pagrindais, kurie susiję su bendraisiais reikalavimais formai [71, p. 14–15] arba objektyviai egzistuojančiais ir konkrečioje situacijoje įvertintais parašo formavimo įrangos saugumo trūkumais ir pan. [63, p. 43].

Po Direktyvos įsigaliojimo elektroninio parašo sektorius neturėjo garantijos, kad kas nors apskritai naudos saugų elektroninį parašą, todėl kurti sprendimai, galintys tenkinti pačius įvairiausius poreikius, o kvalifikuotas elektroninis parašas tapo pavyzdžiu, kai buvo sukurtas formatas, kuris turėjo tikti viskam, bet netiko niekam [54]. Be to, sprendimai buvo kuriami autonomiški, skirti konkrečiai funkcijai [54, p. 6]. Vartotojai atsisakė savanoriškai naudoti kvalifikuotą elektroninį parašą, jiems buvo paprasčiau pasirinkti skaitmeninio parašo opciją *MS Office* ar *Adobe Acrobat* programose, nors tokie parašai formaliai ir neatitiko reikalavimų kvalifikuotajam elektroniniam parašui (beje, minėtos programos jau palaiko Direktyvą atitinkančius formatus).

Glaudi techninės įrangos ir programinės įrangos priklausomybė kvalifikuotą elektroninį parašą padarė sunkiai įgyvendinamu sprendimu, todėl menkas jo naudojimas buvo nulemtas ne tiek vartotojų pasitikėjimo stokos, kiek netinkamo oficialaus požiūrio – juk sandorių internete sudarymas tapo kasdienybe, tačiau jiems kvalifikuoto elektroninio parašo nereikia. Kvalifikuoto elektroninio parašo kategorija tapo netobulu mėginimu vartotojų pasitikėjimo trūkumą kompensuoti aukščiausio saugumo reikalavimais, nors elektroniniu būdu paslaugas teikiantys subjektai ir jų vartotojai pirmiausia pasveria išlaidas ir gaunamą naudą. Kvalifikuotas elektroninis parašas, kaip brangus ir nepatogus naudoti sprendimas, užtikrina aukštą saugumo lygį, kuris įprastiems sandoriams internete retai būtinas [54, p. 11], o vieno saugumo standarto primetimas visoms paslaugoms reiškė, kad paprastiems sprendimams taikomas brangus reikalavimas, kuris ne visada būtinas, pvz., valstybių narių elektroninės vyriausybės, elektroninės bankininkystės paslaugos pradėtos plėtoti paprastesnių sprendimų (PIN kodo) pagrindu. Be to, informacija, kurios reikia elektroniniam parašui kurti, nevisiškai atitinka tai, ko reikia verslo subjektams, sudarantiems sandorius su nauja šalimi, ir panašu, kad viena iš nedaugelio sričių, kurioje kvalifikuotas elektroninis parašas liks aktualus, yra elektroniniai viešieji pirkimai.

2012 m. pradžios duomenimis, Lietuvoje buvo išduota daugiau kaip 730 000 kvalifikuotų sertifikatų [57, p. 3–5], tačiau praktinis jų panaudojimas iki šiol apsiriboja iš esmės trimis sritimis: viešosios valdžios ir administravimo paslaugomis (elektroninės valdžios paslaugos), elektronine bankininkyste ir viešaisiais pirkimais elektroninėje erdvėje. Be to, privačiame sektoriuje saugūs parašai kartais naudojami elektroninėms sąskaitoms pasirašyti. Nors kvalifikuoto parašo naudojimą iki šiol labiausiai skatino elektroninės valdžios paslaugos, praktiškai elektroninio dokumento (ADOC) formatas[9] veikia gana sunkiai, iki šiol valstybės institucijos yra linkusios reikalauti popierinių dokumentų formatų.

Elektroninio parašo naudojimą dar labiau paskatins nuo 2013 m. liepos 1 d. įsigaliosiantys Lietuvos Respublikos civilinio proceso kodekso [24] (toliau – CPK) ir Teismų įstatymo [26] straipsniai, įteisinantys elektroninę bylą ir leisiantys elektroninių ryšių priemonėmis pateikti procesinius dokumentus ir jų priedus (įskaitant ir įrodymus)[10]. Pažangu tai, kad Lietuvos Respublikos teisingumo ministras, 2012 m. gruodžio 13 d. įsakymu Nr. 1R-332 [29] patvirtindamas procesinių dokumentų pateikimo teismui ir jų įteikimo asmenims elektroninių ryšių priemonėmis tvarkos aprašą, numatė kelis asmens autentifikavimo jungiantis prie LITEKO sistemos būdus: (a) viešojo administravimo institucijų informacinių sistemų interoperabilumo sistemos teikiamomis priemonėmis (asmens tapatybė nustatoma naudojant elektroninį parašą, patvirtintą kvalifikuotu sertifikatu, arba elektroninės bankininkystės sistemas); (b) naudojantis teismo suteiktais prisijungimo duomenimis[11].

Lietuvos teismai kaip leistinus rašytinius įrodymus pripažindami elektroninius įrodymus [45, p. 64–66], nebūtinai pasirašytus kvalifikuotuoju parašu, reikšmingai prisidėjo prie elektroninių priemonių pripažinimo ir naudojimo komerciniuose santykiuose. Lietuvos Aukščiausiasis Teismas savo formuojamoje praktikoje yra pažymėjęs [39], kad tais atvejais, kai įstatyme nereikalaujama bylos aplinkybes įrodinėti tik tam tikromis įrodinėjimo priemonėmis, teismas vertina visus įrodymus (kurių sąrašas pagal nuo 2011 m. spalio 1 d. įsigaliojusią CPK 177 straipsnio redakciją nėra išsamus), atitinkančius leistinumo, sąsajumo, patikimumo kriterijus. Teismų praktikoje tinkamu pripažįstamas rašytinis, faksimilinis, taip pat kitos formos pranešimai [žr., pvz.: 34, 36, 37].

---

[9] Elektroniniu parašu pasirašyto elektroninio dokumento specifikacija ADOC-V1.0, patvirtinta Lietuvos archyvų departamento generalinio direktoriaus 2009 m. rugsėjo 7 d. įsakymu Nr. V-60 [31], nustatanti valstybės ir savivaldybių institucijų, kitų subjektų, įgaliotų atlikti viešojo administravimo funkcijas, valstybės įgaliotų asmenų rengiamų ir iš nevalstybinių organizacijų, privačių juridinių ir fizinių asmenų gaunamų elektroniniu parašu pasirašytų oficialių elektroninių dokumentų programinių priemonių reikalavimus.

[10] Pvz., pagal CPK 175-1 straipsnį, procesiniai dokumentai teismui gali būti pateikiami elektroninės formos elektroninių ryšių priemonėmis. Procesinių dokumentų pateikimo teismui elektroninių ryšių priemonėmis tvarką ir formą nustato teisingumo ministras. 2012 m. gruodžio 20 d. Teismų įstatymo 36, 37, 93, 94, 120 straipsnių pakeitimo ir Įstatymo papildymo 37(1) straipsniu (*Valstybės žinios*, 2012, Nr. 153-7826) įstatymo 7 straipsnio pakeitimo įstatymas Nr. XII-74 37-1 straipsnio (Elektroninės bylos, informacinių ir elektroninių ryšių technologijų naudojimas teismuose) įsigaliojimą atidėjo iki 2013 m. liepos 1 d. 2012 m. gruodžio 20 d. įstatymu Nr. XII-72 (*Valstybės žinios*, 2012, Nr. 153-7824) CPK 175-1 straipsnio įsigaliojimas atidėtas iki 2013 m. liepos 1 d.

[11] Čia kalbama tik apie asmens autentifikavimą jungiantis prie informacinės sistemos, o tai, kaip jau minėta, *stricto sensu* nėra elektroninis parašas.

Vis dėlto 2011 m. spalio 10 d. Lietuvos apeliacinis teismas byloje *UAB „Furnitūra Marketingas“ v. UAB „DHL Lietuva“* [38] konstatavo, kad nesant ieškovo elektroniniuose laiškuose įstatymo reikalavimų atitinkančio elektroninio parašo, ieškovas nepateikė rašytinės formos pretenzijų kaip to reikėjo pagal sutartį. Šioje byloje teismas netiesiogiai pripažino, kad elektroninis dokumentas rašytinės formos reikalavimus gali atitikti tik tokiu atveju, kai jis pasirašytas Įstatymo 8 straipsnio 1 dalyje numatytus reikalavimus atitinkančiu kvalifikuotu elektroniniu parašu. Teismas netaikė 8 straipsnio 2 dalyje įtvirtinto kitų elektroninio parašo formų nediskriminavimo reikalavimo ir todėl Įstatymo 8 straipsnio prezumpciją pritaikė kaip įsakymų reikalavimą visais atvejais reikalauti kvalifikuoto elektroninio parašo. Tokia teismo argumentacija iš esmės pašalina galimybę kaip rašytinius įrodymus naudoti duomenis, kurie nėra pasirašyti kvalifikuotu elektroniniu parašu, o tai nesuderinama su Lietuvos teismų praktika elektroniniams duomenims suteikti nediskriminacinę lyginamąją dalį rašytinių įrodymų visete. Reikia tikėtis, kad ši nutartis nepaskatins minėtos praktikos pokyčių, ir šalims neginčijant paties el. laiško siuntimo ar gavimo fakto, teismai neatsisakys vertinti el. laiško kaip rašytinio įrodymo vien dėl to, kad jis nepasirašytas kvalifikuotu parašu.

5. Standartai ir technologinis neutralumas

Techninių elektroninio parašo reikalavimų vienodumas vidaus rinkoje yra neabejotinai vienas iš svarbiausių bendros elektroninio parašo rinkos funkcionavimo veiksnių [76]. Direktyvos siekiamą valstybių narių nacionalinių įstatymų derinamąjį efektą techninių reikalavimų suvienodinimo srityje papildo standartizacija. Direktyvos 3 straipsnio 5 dalyje, kalbant apie elektroninio parašo produktų pripažinimą vidaus rinkoje, pateikiama nuroda į *visuotinai pripažintus standartus*. Komisijos sprendimas 2003/511/EC [5, p. 45] (toliau – Sprendimas) pateikia nurodą į tris dokumentus[12]: CWA 14169 [18] (preziumuojama, kad laikantis šio standarto laikomasi Direktyvos III priede išdėstytų reikalavimų), CWA 14167-1 [19] ir CWA 14167–2:2002 [20] (preziumuojama, kad laikantis šių standartų laikomasi Direktyvos II priedo f punkto reikalavimų), kurie pagal Direktyvos 3 straipsnio 5 dalį yra vieninteliai „visuotinai pripažinti standartai“ ir kurie, kitaip nei suderintieji standartai (angl. *harmonised standards)*[13], yra įforminti kaip CWA (angl. *European Committee for Standardisation Workshop Agreements)*.

Direktyvos prieduose nepateikiama saugios parašo formavimo įrangos patikrinimo taisyklių, o tai, kad Sprendimas gali sukurti tik atitikties Priedui II(f) ir Priedui III prezumpciją, reiškia, kad nėra įmanoma pateikti aiškių gairių dėl likusių standartų (ETSI, EN ir kt.), kurių elektroninio parašo srityje yra apie 30, teisinės reikšmės[14].

Yra bendras neaiškumas dėl CWA dokumentų teisinės galios vidaus rinkoje [66, p. 37]. Sprendime pateikiamos tiesioginės nuorodos į konkrečius CWA (pateikiant

[12] Lietuvoje jie buvo priimti kaip nacionaliniai standartai: LST CWA 14167-1, LST CWA 14167-2 ir LST CWA 14169:2009.

[13] Suderintas standartas yra Europos standartas (EN), kurio atitiktis sukuria ES teisės aktų reikalavimų atitikties prezumpciją.

[14] CEN dirba ties šiais dviem standartais ir planuoja pateikti atnaujintą versiją (buvo planuojama iki 2012 m. vidurio). Atitinkamai Sprendimas 2003/511/EC būtų pakeistas iki 2013 m. vidurio taikant ES komitologijos procedūrą.

CWA dokumento numerį ir datą). Nuo 2003 m. CWA dokumentai buvo keisti, nors Sprendimas nekeistas nė karto, todėl kyla klausimas, ar galioja pakeistas, bet į Sprendimą neįtrauktas CWA?

Galiojančių ir nebegaliojančių bei persiklojančių standartų raizgalynę 2010 m. Komisija nusprendė išpainioti – Europos standartizavimo organizacijoms (CEN, CENELEC ir ETSI) buvo suteiktas standartizavimo mandatas M460 elektroninių parašų srityje [16]. Be to, dar 2008 m. Komisijos Elektroninio parašo ir elektroninės atpažinties veiksmų plane [11] buvo numatyta, kad iki 2009 m. vidurio Direktyvos sistema bus papildyta naujais standartais.

Pirmiau aprašytos problemos identifikuotos gana anksti, Komisija nevengdavo pripažinti teisinių suderinamumo ir elektroninio parašo veikimą stabdančių problemų, tačiau jos nebuvo sprendžiamos nuosekliai, sistemingai ir atkakliai. Be to, Komisijai niekas nedraudė inicijuoti kitų standartų, kurie yra už Direktyvos 3 straipsnio 5 dalies ribų, priėmimo.

Antroji su standartais susijusi problema ta, kad bendras reikalavimų saugiai parašo formavimo įrangai nustatymas Direktyvos lygmeniu nebuvo nuosekliai nuleistas į žemesnio lygio teisės aktus – CWA 14169 ir kiti visuotinai pripažinti standartai Sprendimu buvo Direktyvos 3 straipsnio 5 dalies pagalba „prirakinti“ prie Direktyvos ir taip saugią elektroninio parašo formavimo įrangą sutapatino tik su viena – išmaniųjų kortelių – technologija. Be to, tai nulėmė skirtingus tų pačių reikalavimų aiškinimus įvairiose valstybėse narėse (priimant nacionalinius standartus).

Praktinis rezultatas – dabartiniai į Direktyvos sistemą patenkantys standartai neapima modernesnių technologijų sprendimų [7]. Paskutiniu metu pastebima tendencija pereiti prie „nuotolinio parašo“ infrastruktūros, kai pasirašymo operacijos yra atliekamos ne pasirašytojo įrangoje, o paslaugos teikėjo saugiame serveryje (angl. *HardwareSecurity Module*) [64]. Tokia technologija apima mobiliuosius elektroninius parašus arba masinius sąskaitų pasirašymus. CWA 14169 reikalavimų įgyvendinimas HSM įrenginiams yra kur kas sudėtingesnis nei išmaniosioms kortelėms (angl. *smart cards*), nes technologiškai sudėtingesnis vartotojo autentifikavimas negu tais atvejais, kai ir pats privatusis raktas yra pasirašančio asmens rankose – Direktyvos 2 straipsnio 3 punktas pasirašantį asmenį apibūdina kaip asmenį, turintį parašo formavimo įrangą. Tai glaudžiai susiję su „kontrolės tik pasirašančio asmens valia“ reikalavimu (Direktyvos 2 straipsnio 2 dalies c) punktas). Kai kurie autoriai teigia, kad, atiduodamas privatųjį raktą saugoti nuotoliniame serveryje, pasirašytojas nebetenka galimybės kontroliuoti parašo įrangos [62, p. 3]. Direktyvos III priedo reikalavimus *de facto* gali tenkinti tik tokie mobiliojo parašo sprendimai, kai tiek parašo tikrinimo duomenys, tiek priemonės yra vienoje vietoje ir juos gali kontroliuoti tik pats pasirašytojas – tai praktiškai pasiekiama per specialią SIM kortelę, kurios mikroschemoje įrašomas privatusis raktas, sertifikatas ir kita elektroniniam parašui formuoti ir tikrinti svarbi pagalbinė informacija[15]. Yra vos keletas technologinių sprendimų, kurie nebūtų pagrįsti išmaniosiomis kortelėmis ir kartu būtų pripažinti saugia parašo formavimo

[15] Lietuvos apeliacinio teismo nagrinėtoje civilinėje byloje Nr. 2A-1726/2011 teismas netiesiogiai (nagrinėdamas ginčą, kylantį iš viešųjų pirkimų santykių) vertino mobiliojo elektroninio parašo techninius aspektus.

įranga pagal Direktyvą, nors ir ne pagal CWA 14169 reikalavimus [66, p. 55].

Be to, techninės sąveikos trūkumas sukūrė prielaidas atsirasti izoliuotoms taikomosioms programoms (pvz., sertifikatai gali būti naudojami tik toje konkrečioje programoje). Kadangi specifiniai reikalavimai visose valstybėse narėse skiriasi, nors ir gana nereikšmingai, beveik neįmanoma pagaminti tokio produkto, kuris vienu metu tenkintų visus tokius reikalavimus.

Lietuvoje, be ADOC formato, skirto bendrauti su viešojo administravimo subjektais, skirtingi sertifikavimo paslaugų teikėjai plėtoja kitus elektroninio parašo formatus, kurie dažniausiai nesuderinami. Skirtingos elektroninio parašo formavimo ir tikrinimo programos[16] pritaikytos tik atpažinti vienus ar kitus formatus. Tas pats pasakytina ir apie elektroninio parašo techninę įrangą – Lietuvoje iš esmės naudojamos trys rūšys – speciali SIM kortelė (mobilus parašas), lustinės kortelės (išmaniosios kortelės (kurios gali būti susietos su asmens tapatybės kortele) ir atminties saugyklos (USB atmintukai, microSD kortelės), tačiau kai kurie elektroninės valdžios sprendimai pripažįsta tik kai kuriuos iš jų. Keičiant sertifikavimo paslaugų teikėją (pvz., dėl to, kad nustojo galioti senas sertifikatas ir pan.), gali tekti keisti įrangą ir pan. Panašu, kad Lietuvos elektroninio parašo sistemą bus ištikusi bėda, kurios buvo galima išvengti, pvz., plėtojant vientisą elektroninio parašo formatą[17], neužkertant kelio ir kitoms elektroninio parašo formoms.

„Debesų“ technologijos (angl. *cloudcomputing*) [9] keičia verslą ir kitas socialiai reikšmingas elgsenos apraiškas elektroninėje erdvėje – kompiuterių programos ir infrastruktūra, verslo procesai, įvairūs skaitmeniniai produktai (audiovizualiniai kūriniai, vaizdinės, grafinės bylos ir pan.) – vartotojui pateikiami jau ne kaip įranga ar prekė, o kaip paslaugos. Pereinama nuo verslo modelio, pagrįsto IT priemonių pateikimu, prie į individualizuotų, tik konkrečiam vartotojui pritaikytų ir jo užsakytų paslaugų teikimo. Debesies technologijos kels ypatingų klausimų Direktyvos 2 straipsnio 2 dalies ir 3 dalies reikalavimų požiūriu, ypač dėl reikalavimų, kad įranga būtų kontroliuojama vien pasirašančio asmens (duomenų, esančių *cloud* aplinkoje, kontrolę apibrėžia sutartis su *cloud* paslaugų teikėju). Šiame kontekste tampa nebetinkama parašo, kaip neatsiejamos dokumento dalies, samprata, nes parašo duomenys reikalingi ne tik prisijungiant prie sistemos (*cloud* tipo aplinkos), bet ir save susiejant su tam tikrais toje aplinkoje atliekamais veiksmais. Siunčiant dokumentą iš *cloud* aplinkos kyla klausimas, ar iš tikrųjų parašas buvo suformuotas pasirašytojo įrangoje ir kiek tai suderinama su minėtais Direktyvos 2 straipsnio 2 dalyje įtvirtintais reikalavimais saugiam parašui. Be to, kils klausimas, kur bus sertifikavimo paslaugų teikimo vieta – ar bus laikoma, kad kvalifikuotas sertifikatas, naudojamas *cloud* aplinkoje, yra reikalau-

[16] Pvz., Lietuvos archyvų departamento generalinio direktoriaus 2008 m. spalio 9 d. įsakyme Nr. V-119 [30] nustatyta, kad valstybės institucijoms elektroniniu būdu teikiami dokumentai, kurių rengimą nustato norminiai teisės aktai, turi atitikti Lietuvos vyriausiojo archyvaro patvirtintose ar su juo suderintose elektroninių dokumentų specifikacijose nustatytus reikalavimus. Tokius dokumentus galima sukurti naudojant kompiuterių programą „Signa“. Lietuvoje dar naudojamos ir kitos elektroninio parašo pasirašymo programos: pvz., Justa GE.

[17] Žr. Estijos pavyzdį – visos elektroninės valdžios, elektroninio banko paslaugos, elektroninio viešojo transporto paslaugos yra užtikrinamos naudojantis išmaniąja kortele, integruota su asmens tapatybės kortele.

jantis pripažinimo Lietuvoje pagal Įstatymo 5 straipsnį.

6. Saugi parašo formavimo įranga

Direktyvos 3 straipsnio 4 dalyje nustatyta, kad valstybių narių paskirtos valstybės ar privačios institucijos[18] nustato, ar saugi parašo formavimo įranga atitinka jos Priede III nurodytus reikalavimus. Vadovaudamasi Direktyvos 9 straipsnyje nurodyta tvarka, Komisija nustato kriterijus, kuriais remdamosi valstybės narės skiria minimas institucijas.

Tai, kad skirtingos valstybės narės numatė skirtingus reikalavimus parašo formavimo įrangai, kurie yra griežtesni, nei numatyti Priede III, nėra blogiausias Direktyvos padarinys. Didesne blogybe tapo tai, kad neatsirado aiškių ir paprastų įrangos patikrinimo ir patvirtinimo saugia taisyklių, be to, skirtingų įrangos atitikties deklaracijų šaltinių ir formų teikiamas teisinis tikrumas tapo eklektiškas. Be abejo, stipriausią teisinį tikrumą suteikia institucijos, paskirtos pagal Direktyvos 3 straipsnio 4 dalį (nors valstybės narės ir neturi pareigos jas paskirti), formali atitikties deklaracija, kuri turi būti pripažįstama visose valstybėse narėse. Visais kitais atvejais nėra jokios teisinės atitikties prezumpcijos ir todėl taikomos bendrosios įrodinėjimo taisyklės. Kadangi valstybės narės neturi pareigos paskirti tokias institucijas, jos veikia ne visose valstybėse, o tai riboja laisvą parašo formavimo įrangos judėjimą vidaus rinkoje.

Antras pagal suteikiamą teisinį tikrumą lygmuo – saugios parašo formavimo įrangos sertifikavimas pagal CWA 14169 patvirtinant, kad ji buvo įvertinta kaip suderinama su CWA 14169, nesvarbu, ar tą įvertinimą atliko pagal Direktyvos 3 straipsnio 4 dalį paskirtoji įstaiga. Žemiausią teisinio patikimumo lygį suteikia paties parašo formavimo įrangos gamintojo deklaracija, kad ji atitinka Priedo III reikalavimus, neatsižvelgiant į tai, ar kuri nors pagal Direktyvos 3 straipsnio 4 dalį paskirtoji įstaiga atliko (tiksliau – buvo atliktas pagal jos nustatytą tvarką) tokios atitikties įvertinimą, ir nesvarbu, ar buvo atliekamas atitikties CWA 14169 vertinimas. Direktyvos rengėjai siekė, kad Priede III išvardytų reikalavimų tenkinimas būtų savaime pakankamas, tačiau pačiam įrangos gamintojui sunku įrodyti įrangos atitiktį, nes kyla klausimas dėl konkrečių vertinimo kriterijų ir metodų, kurie nei Direktyvoje, nei Sprendime tiesiogiai nėra aptarti. Be to, viena iš priežasčių, dėl ko gamintojai patys nesiekia savanoriškai įvertinti parašo formavimo įrangos, yra ta, kad, sukūrus naują ar patobulinus seną įrangą, vėl reikia pradėti ilgą ir brangią procedūrą [48, p. 11].

Be to, pažymėtina skirtinga valstybių narių pozicija dėl įrangos atitikties įvertinimo. Kai kurios valstybės Direktyvos 3 straipsnio 4 dalies reikalavimus aiškina labai griežtai nustatydamos, kad saugi parašo formavimo įranga visada turi būti patikrinta paskirtosios institucijos (pvz., Vokietija). Tokią griežtą poziciją užimančios valstybės linkusios nepasitikėti kitose valstybėse narėse galiojančiomis atitikties procedūromis ir reikalauja papildomo patikrinimo pagal savo nacionalinę procedūrą. Tiesa, valstybių savitarpį pasitikėjimą kitos valstybės atliktos patikros rezultatais iš dalies užtikrina tarptautiniai susitarimai

[18] 2000 m. lapkričio 6 d. Komisijos sprendimu 2000/709/EB [4] buvo nustatyti bendro pobūdžio kriterijai, į kuriuos turėtų atsižvelgti valstybės narės, skirdamos institucijas pagal Direktyvos 3 straipsnio 4 dalį.

[66, p. 26–29]. Kitos valstybės mano, kad nėra būtinas formalus atitikties Direktyvos III priede įtvirtintų reikalavimų įvertinimas (pvz., Belgija). Šie du pavyzdžiai reprezentuoja du galimus Direktyvos įgyvendinimo kraštutinumus, ir likusiose valstybėse narėse minėti reikalavimai išsidėsto intervale tarp jų [66, p. 22]. Lietuva šiuo požiūriu neužima išskirtinės vietos – nėra specialios parašo formavimo įrangos patikrinimo tvarkos, tačiau 2002 m. gruodžio 31 d. Lietuvos Respublikos Vyriausybės nutarime Nr. 2108 [28], be atitikties standartui LST CWA 14168 „Saugi parašo formavimo įranga EAL 4“, nurodomas papildomas reikalavimas – atitiktis LST CWA 14170 „Saugumo reikalavimai, keliami taikomosioms parašo formavimo sistemoms“.

Saugi parašo formavimo įranga veikia tam tikroje aplinkoje ir nėra vienintelis elementas, nulemiantis saugaus parašo sukūrimą – tai pripažįstama ir CWA 14169, kuris reikalauja sukurti saugų kanalą iki pat pasirašytojo, kuris leistų pasirašytinų duomenų pademonstravimą saugioje aplinkoje, saugiai pasirašytinus duomenis perduoti iš parašo programinės įrangos[19] parašo formavimo prietaisui[20] (tarp jų turi būti saugus kelias), sugeneruoto parašo susiejimą su pasirašytais duomenimis ir jų pavaizdavimą pasirašytojui, sugeneruoto parašo siuntimą gavėjui. Praktinė problema yra ta, kad šios saugumo sąlygos turi būti patenkinamos už saugios parašo formavimo įrangos ribų (pvz., programinė pasirašymo įranga, žmogiškasis veiksnys, pasirašytinų duomenų pavaizdavimas), o iš pačios Direktyvos nėra išplaukiančios teisinės pareigos užtikrinti parašo programinės įrangos ar ryšio saugumą (tai netiesiogiai išplaukia iš CWA 14169 [18]). Saugi parašo formavimo įranga, panaudota nesaugioje aplinkoje (pvz., išmanioji kortelė, nuskaityta nesaugia įranga, arba parašo duomenys, perduoti nesaugiu kanalu) technologiniu požiūriu negali sukurti saugaus parašo, nors teisiniu požiūriu ir būtų įmanoma. Vis dėlto, peržengus formalias saugios parašo formavimo įrangos ribas, įrangos saugumas negali būti kvestionuojamas [66, p. 41]. Be to, Direktyvos preambulės 15 punkte nurodoma, kad Priede III nėra nustatomi reikalavimai visai elektroninio parašo sistemos aplinkai, todėl saugią parašo formavimo įrangą panaudojus nesaugioje aplinkoje, formaliai neišnyksta saugaus elektroninio parašo sukūrimo prielaidos. Tai vis dar išlieka iki galo neišspręsta Direktyvos problema.

7. Sertifikatai

Nuo elektroninio parašo infrastruktūros neatskiriama sertifikavimo samprata. Sertifikatas – elektroninis liudijimas, kuris susieja pasirašantįjį su parašo tikrinimo duomenimis (Direktyvos 2 straipsnio 9 punktas). Kvalifikuotam sertifikatui nustatyti reikalavimai įtvirtinti Priede I, o juos išduodantiems sertifikavimo paslaugų teikėjams – Priede II (Direktyvos 2 straipsnio 10 punktas).

Pats savaime skaitmeninis parašas nieko nepasako apie tikrąją pasirašiusio asmens tapatybę, parašo verifikacijai padeda sertifikatas. Su kiekviena raktų pora sertifikavimo paslaugų teikėjas išduoda

[19] Programinė įranga, naudojama parašui sukurti, bet neapimanti pačios saugios parašo formavimo įrangos, leidžia atlikti: (a) pasirašytinų duomenų pateikimą pasirašyti, (b) pasirašytinų duomenų atvaizdo siuntimą privataus rakto generavimo programinei ir kompiuterinei įrangai, (c) prikabinti parašo duomenis prie pasirašomų duomenų.

[20] Įranga, kuri taiko parašo formavimo duomenis (kodus) formuojant konkretų elektroninį parašą.

skaitmeninį sertifikatą, kuriame yra viešasis raktas (parašo tikrinimo duomenys) ir informacija apie rakto turėtojo tapatybę, rakto galiojimo laikotarpį, parašo algoritmą, sertifikato numeris, sertifikavimo paslaugų teikėjo pavadinimas ir pan.Vis dėlto sertifikatas *ipso facto* nepateikia atsakymo į klausimą, kokiu lygiu galima pasitikėti sertifikatą išduodančiu subjektu. Direktyva pateikia šio klausimo sprendimą per priežiūros, atitikties patvirtinimo ir akreditacijos koncepciją.

Reikalavimas, kad saugus parašas leistų nustatyti pasirašančio asmens tapatybę (Direktyvos 1 straipsnio 2 punkto b), valstybėse narėse pritaikytas skirtingai, pvz., vienose valstybėse narėse kvalifikuotuose sertifikatuose reikalaujama nurodyti unikalų asmens kodą (pvz., Ispanijoje), kitose – ne (pvz., Vokietijoje, Švedijoje, Lietuvoje[21]). Be to, kai kuriose valstybėse neleidžiami pseudonimai (slapyvardžiai) (pvz., Estijoje, Bulgarijoje) [48, p. 95], nors Direktyvos preambulės 25 punktas neriboja galimybės sertifikate nurodyti pseudonimo. Tai – akivaizdus pagrindas objektyviems skirtumams, sukuriantis prielaidas tarpvalstybiniams barjerams.

8. Komisijos pasiūlymas dėl Reglamento

Komisijos pasiūlymui dėl Reglamento prielaidas sukūrė daug programinių ir koncepcinių Komisijos dokumentų. Vienas iš svarbesnių ES programinių dokumentų – 2010 m. Komisijos Europos skaitmeninė darbotvarkė [12]; viena iš jos numatytų pagrindinių priemonių – persvarstyti Direktyvą, kad būtų sukurtas saugių elektroninio tapatumo nustatymo sistemų tarpvalstybinio pripažinimo ir sąveikos teisinis pagrindas. 2011 m. Komisija paskelbė komunikatą „Bendrosios rinkos aktas – dvylika svertų augimui skatinti ir pasitikėjimui stiprinti „Bendros pastangos skatinti naująjį augimą“ [13], kuriame kaip

[21] Reikalavimai kvalifikuotam sertifikatui įtvirtinti Įstatymo 2 straipsnio 15 dalyje (4 punkte numatytas reikalavimas sertifikate nurodyti pasirašančio asmens specialius atributus, jei tai reikalinga atsižvelgiant į numatomus sertifikato naudojimo tikslus), ir juose nėra *expressis verbis* paminėtas asmens kodas. Asmens duomenų teisinės apsaugos įstatymo [27] 7 straipsnyje nurodomas imperatyvus reikalavimas, be asmens sutikimo asmens kodą leidžiantis tvarkyti tik įstatyme numatytais atvejais. Vis dėlto, pvz., VĮ Registrų centro sertifikavimo centro Sertifikavimo veiklos nuostatuose nurodoma, kad sertifikavimo tarnyba turi reikalauti, jog sudaromame sertifikate būtų nurodyti asmens vardas ir pavardė bei asmens kodas (3.1.1 punktas). 2012 m. gruodžio 18 d. Lietuvos vyriausiasis administracinis teismas byloje Nr. A143-2740/2012 [40] konstatavo, kad Asmens duomenų teisinės apsaugos įstatymas yra specialus teisės aktas Įstatymo atžvilgiu. Asmens duomenų teisinės apsaugos įstatymo 3 straipsnio 1 dalies 4 punkte nurodyta, kad duomenų valdytojas privalo užtikrinti, jog asmens duomenys būtų tapatūs, tinkami ir tik tokios apimties, kuri būtina jiems rinkti ir toliau tvarkyti. Žinoti asmens kodą yra būtina tam, kad pareiškėjas, vykdydamas sertifikato sudarymo funkciją, galėtų nustatyti (patikrinti) asmens tapatybę prieš sudarydamas sertifikatą. Asmens kodo nenurodymas kvalifikuotame sertifikate nepanaikina galimybės pareiškėjui, kaip sertifikavimo paslaugos teikėjui, vykdyti tokio sertifikato tvarkymo funkciją. Teismas padarė išvadą, kad asmens kodo panaudojimas kvalifikuotame sertifikate yra neleistinas asmens duomenų panaudojimas. Be to, minėto įstatymo 7 straipsnyje yra nustatytas ypatingas asmens kodo naudojimo reglamentavimas – t. y. jį naudoti, kai tvarkomi asmens duomenys, galima tik gavus duomenų subjekto sutikimą, išskyrus atvejus, nurodytus šio straipsnio 4 ir 5 dalyse, kai asmens kodą naudoti draudžiama. Aptariamos dalies 4 punkte nurodyta, kad draudžiama asmens kodą skelbti viešai. Teismas paliko galioti Valstybinės duomenų apsaugos inspekcijos nurodymą nenaudoti asmens kodo Registrų centro kvalifikuotuose sertifikatuose. Kyla įdomus teisinis klausimas, kaip elgtis su minėto sprendimo neatitinkančiais, bet tebegaliojančiais sertifikatais – minėtas teismo sprendimas automatiškai neturėtų panaikintiVĮ Registrų centro išduotų kvalifikuotų sertifikatų galiojimo, nes jis neturi *prejudicinės* ar *res judicata* galios sertifikavimo paslaugų teikėjų ir jų klientų tarpusavio santykiams.

viena iš skatinimo priemonių numatoma Direktyvos persvarstymas. Pasitikėjimo elektroniniais sandoriais didinimas įvardijamas kaip viena iš būtinų skaitmeninės vidaus rinkos plėtros sąlygų. Komisijos stabilumo ir augimo gairėse [14] pabrėžta, kad, plėtojant skaitmeninę ekonomiką, svarbus vaidmuo tenka būsimai bendrajai teisinei bazei, pagal kurią tarpvalstybiniu mastu būtų abipusiai pripažįstama ir priimama elektroninė atpažintis ir tapatumo nustatymas.

Jau seniai tapo dogma, kad pačios geriausios elektroninei komercijai ir su ja susijusiems santykiams reguliuoti skirtos teisės normos yra tos, kurios pasižymi tinkamu valstybių reguliavimo ir savireguliacijos deriniu [56, p. 206]. Nors elektroninio parašo santykių reglamentavimo būdų ir režimų įvairovė nusipelno atskiros studijos [55, p. 50], specialaus *sui generis* teisinio reguliavimo taisyklių kūrimas elektroniniam parašui, taip jį išskiriant iš kitų pasirašymo metodų, turi būti pagrįstas bet kurioje teisinėje sistemoje. Valstybės įsikišimas nėra tinkamas, jeigu veikia rinkos jėgos – kai kurie autoriai teigia, kad viešasis interesas tais atvejais, kai rinka yra ypač trapi ir turi tendenciją veikti neefektyviai, reikalauja reguliacinio įsikišimo [53, p. 39]. Vis dėlto Direktyvos, o dabar – ir reglamento rengėjai tik labai paviršutiniškai vertina būtinybę teisiškai sureguliuoti elektroninio parašo panaudojimą. Interneto savireguliacijos idėjos nesulaukė plataus atgarsio Komisijos koridoriuose, o tokie tradiciniai argumentai, kaip antai: vartotojų pasitikėjimo trūkumas, privatumas, teisinio tikrumo, saugumo užtikrinimas įvardijami kaip svarbiausi aiškaus ir detalaus sureguliavimo argumentai [10, preambulės 2 punktas]. Vertinant vien iš elektroninio parašo perspektyvų, abejotina, ar Direktyvos naikinimas ir visiškai naujo režimo kūrimas yra adekvati priemonė. Reikia pripažinti, kad viena iš esminių pasiūlymo idėjų yra po vienu stogu sutalpinti visas elektroninės atpažinties ir pasitikėjimo paslaugas, elektroninį parašą numatant tik kaip vieną iš tokių paslaugų.

Pasiūlyme [10] nurodoma, kad jis grindžiamas Sutarties dėl ES veikimo 114 straipsniu, susijusiu su taisyklių, skirtų esamoms vidaus rinkos veikimo kliūtims šalinti, priėmimu (siūlomo Reglamento preambulės 11 punktas). Vis dėlto toks ES teisės akto formos parinkimas neįtikina visų pirma dėl to, kad lygiai kaip ir Direktyva, reglamento nuostatos, taikomos kiekvienoje teisinėje sistemoje, gali įgyti savitą derinį su vietinėmis teisės normomis, o tai gali lemti skirtingą taikymo praktiką ir sukelti skirtingus padarinius. Pvz., pagal Siūlomo reglamento 20 straipsnio 2 dalį kvalifikuoto elektroninio parašo teisinė galia yra lygiavertė rašytiniam parašui. Šia nuostata kvalifikuotam elektroniniam parašui nėra garantuojama automatinė ir vienoda teisinė galia vidaus rinkoje.Vietoje to kvalifikuoto elektroninio parašo teisinius padarinius preciziškai apibrėš kiekvienos valstybės narės teisės aktai. Taigi, abejotina, ar pasirinktas reglamentavimo būdas tenkina subsidiarumo testą ir sudarys efektyvias sąlygas pašalinti minėtus trūkumus.

Pagrindžiant veiksmingumo testą nurodoma, kad savanoriškomis valstybių narių tarpusavio koordinavimo priemonėmis pirmiau aprašytų tikslų iki šiol nebuvo pasiekta ir nėra pagrindo manyti, kad jie bus pasiekti. Vis dėlto nereikia pervertinti ES teisės aktų poveikio – elektroninio parašo sprendimų, pagrįstų kvalifikuotu elek-

troniniu parašu, įgyvendinimo ES mastu veiksmingumą stabdo ne tiek reguliacinės priemonės, kiek rinkos dalyvių elgesys vertinant kaštus, riziką ir naudojimo paprastumą.

Vienas iš reikšmingų Siūlomo reglamento pokyčių yra tas, kad reguliavimo sistema dar labiau remtųsi nacionalinių priežiūros tarnybų darbu. Kaip parodė *DigiNotar* incidentas, valstybės institucijų priežiūra dar negarantuoja visiško saugumo ir neužkerta kelio dideliems pažeidimams. *DigiNotar*, kuri pasauliniu mastu teikė sertifikatus interneto svetainėms (www.diginotar.nl), taip pat buvo paskirta Olandijos vyriausybės, kad išduotų sertifikatus jos elektroninių paslaugų platformoms. Vis dėlto, kai 2011 m. buvo įsilaužta į šios paslaugos platformą, buvo išduota daugiau kaip 500 suklastotų sertifikatų [52]. *DigiNotar* buvo uždrausta teikti sertifikavimo paslaugas ir ji vėliau kreipėsi dėl bankroto bylos iškėlimo. Visi jos išduoti sertifikatai buvo atšaukti, o tai sukėlė teisinio neaiškumo bangą – staiga daugybė elektroninių parašų prarado kvalifikuoto elektroninio parašo statusą.

Nors Pasiūlymas ir sukuria skuboto dokumento įspūdį, jo poveikį vienodai įvertinti yra sunku vien jau dėl to, kad jis neįtvirtina baigto teisinio režimo. Siūlomame reglamente apsiribojama esminių principų susisteminimu, didelę dalį įgyvendinimo krūvio perkeliant Komisijai – ne mažiau nei 16 atvejų Komisijai suteikia kompetenciją priimti vadinamuosius deleguotuosius aktus (angl. *delegated acts*). Be to, numatoma nemažai atvejų, kai Komisijai suteikta galimybė įgyvendinimo aktais sudaryti numatyto reguliavimo sąlygas (pvz., Siūlomo reglamento 8 straipsnio 2 dalis).

Išvados

Direktyvos įgyvendinimo praktika atskleidė – kad Direktyva pasiektų numatomą derinamąjį efektą, kilmės valstybės principas turėjo būti nuosekliai derinamas su išsamesniu minimalių reikalavimų sertifikavimo paslaugų teikėjams ir nacionaliniams priežiūros režimams sąrašu, taip pat su platesniu aktyvių pareigų valstybėms narėms įtvirtinimu.

„Viešojo sektoriaus“ išlygos (Direktyvos 3 straipsnio 7 dalis), kurios imtos taikyti ankstyvuoju Direktyvos įgyvendinimo laikotarpiu, nulėmė, kad nacionalinės elektroninės atpažinties infrastruktūros imtos kurti atskirai. O sertifikavimo paslaugų teikėjų akreditacija (Direktyvos 3 straipsnio 2 dalis), kai jis taikomas kaip reikalavimas, tapo viena iš akivaizdžiausių diskriminacijos formų tų valstybių narių atžvilgiu, kuriose tokia schema apskritai neveikia. Netikėta, tačiau panašu, kad ilgai liaupsintas funkcinis ekvivalentiškumas, įtvirtintas Direktyvos 5 straipsnyje, lėmė teisinės ir technologinės elektroninio parašo sampratų painiavą. Tai, kad iki šiol nėra bendro požiūrio į elektroninio parašo funkcinę sampratą, dar labiau paryškina netobulą Direktyvos veikimą.

Direktyva teisinį tikrumą elektroninio parašo veikimui suteikė tik dviem lygiais: (a) aiškią teisinę galią garantuodama tik kvalifikuotam elektroniniam parašui ir (b) įtvirtindama nediskriminavimo reikalavimą. Tai lėmė skurdų Direktyvos binariškumą – iš plačios elektroninio parašo šeimos tik dviem jos nariams buvo suteiktas aiškesnis teisinis statusas. Nors Direktyvos 8 preambulės punkte ir deklaruotas siekis plėtoti atvirą ir neutralų požiūrį į elektroninio parašo technologijas, kaip pa-

rodė vėlesnė Komisijos ir valstybių narių praktika, sisteminį jos pamatą sukūrė tik kvalifikuotas elektroninis parašas.

Skirtingos nacionalinės elektroninio parašo sampratos susijusios su tais padariniais, kuriuos sukėlė Direktyvos 5 straipsnyje puoselėjamas funkcinio ekvivalentiškumo principas – Direktyva tiesiogiai nenustatė elektroninio parašo teisinės galios, tai paliko konkrečios valstybės nacionaliniams įstatymams. Pasenusių ir nekokybiškai prie Direktyvą lydinčio Sprendimo „prirakintų" standartų problema prisidėjo prie to, kad technologinio neutralumo postulatas tapo pamintas ne tiek rinkos dalyvių, kiek ES institucijų, atsakingų už Direktyvos raidą. Į Direktyvos rėmus nebepatenka pastaruoju metu populiariausi elektroninio parašo technologiniai sprendimai. Saugios parašo formavimo įrangos tarpvalstybinis pripažinimas tapo viena iš aktualiausių elektroninio parašo veikimo vidaus rinkoje opų. Parašo formavimo įrangos atitikties įvertinimas, standartizavimas, saugios parašo formavimo įrangos aplinka, kuri daro įtaką ir pačiai saugiai parašo formavimo įrangai, tapo tais klausimais, kurių, deja, Direktyva, o teisingiau jos taikymą nusakantys teisės aktai nepajėgė išspręsti.

Žvelgiant vien iš elektroninio parašo perspektyvų, Direktyvos naikinimas nėra adekvati priemonė – tikėtina, kad šiame straipsnyje identifikuotas bėdas būtų galima išspręsti priėmus naujus standartus, valstybių narių pareigų sąrašą išplėtus ir papildžius nacionalinės priežiūros nuostatomis, įtvirtinus regioninės akreditacijos modelį, nuleidus kartelę saugios parašo formavimo įrangos pripažinimui, iki galo įgyvendinus užsienio paslaugų teikėjų atpažinimo ir pripažinimo priemones.

LITERATŪRA

Teisės aktai ir jų rengimo medžiaga

1. 1999 m. gruodžio 13 d. Europos Parlemento ir Tarybos direktyva 1999/93/EB dėl Bendrijos elektroninių parašų reguliavimo sistemos. *Oficialus leidinys*, L 013, 2000-19-01, p. 12–20.
2. 2000 m. birželio 8 d. Europos Parlamento ir Tarybos direktyva 2000/31/EB dėl kai kurių informacinės visuomenės paslaugų, ypač elektroninės komercijos, teisinių aspektų vidaus rinkoje (Elektroninės komercijos direktyva). *Oficialus leidinys, L 178, 2000-7-17, p. 1–16.*
3. 2006 m. gruodžio 12 d. Europos Parlamento ir Tarybos direktyva 2006/123/EB dėl paslaugų vidaus rinkoje. *Oficialusis leidinys,* L 376, 27/12/2006 p. 36–68.
4. 2000 m. lapkričio 6 d. Komisijos sprendimas 2000/709/EB dėl būtiniausių kriterijų, į kuriuos turi atsižvelgti valstybės narės, skirdamos institucijas pagal Europos Parlamento ir Tarybos direktyvos 1999/93/EB dėl Bendrijos elektroninių parašų sistemos 3 straipsnio 4 dalį (pranešta dokumentu Nr. C(2000) 3179) *Oficialus leidinys,* L 289/42, 2000-11-16, p. 42–43.
5. 2003 m. liepos 14 d. Komisijos sprendimas 2003/511/EB dėl elektroninio parašo produktų visuotinai pripažintų standartų žymenų paskelbimo pagal Europos Parlamento ir Tarybos direktyvą 1999/93/EB (pranešta dokumentu Nr. C(2003) 2439). *Oficialus leidinys,* L 175, 2003-7-15, p. 45–46.
6. 2010 m. liepos 28 d. Komisijos sprendimas 2010/425/ES, kuriuo iš dalies keičiamos Sprendimo 2009/767/EB nuostatos dėl valstybių narių priežiūrimų ir (arba) akredituotų sertifikavimo paslaugų teikėjų patikimų sąrašų sudarymo, tvarkymo ir skelbimo (pranešta dokumentu Nr. C(2010) 5063). *Oficialusis leidinys*, L 199, 31/07/2010, p. 30–35.
7. 2012 m. birželio 4 d. Poveikio vertinimo santrauka. Komisijos darbinis dokumentas prie 2012 m. birželio 4 d. Komisijos pasiūlymo dėl Europos Parlamento ir Tarybos reglamento dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje. SWD(2012) 135 galutinis, Briuselis.

8. Proposal for a European Parliament and Council Directive on a common framework for electronic signatures / COM/98/0297 final – COD 98/0191. *Official Journal*, C 325, 23/10/1998.
9. Comission Staff Working Documentaccompanying the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions„Unleashing the Potential of Cloud Computing in Europe“, 27.9.2012, SWD (2012) 271 final, Brussels.
10. 2012 m. birželio 4 d. Komisijos pasiūlymas Europos Parlamento ir Tarybos reglamentas dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje. COM/2012/238 galutinis, Briuselis.
11. 2008 m. liepos 28 d. Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „E. parašo ir e. atpažinties veiksmų planas, skirtas tarpvalstybinių viešųjų paslaugų teikimui bendrojoje rinkoje palengvinti“. COM(2008) 798 galutinis, Briuselis.
12. 2010 m. rugpjūčio 26 d. Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Europos skaitmeninė darbotvarkė“. COM(2010) 245 galutinis/2, Briuselis.
13. 2011 m. balandžio 13 d. Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Bendrosios rinkos aktas – Dvylika svertų augimui skatinti ir pasitikėjimui stiprinti „Bendros pastangos skatinti naująjį augimą“. COM(2011) 206, galutinis, Briuselis.
14. 2011 m. spalio 12 d. Komisijos komunikatas „Stabilumo ir ekonomikos augimo gairės“. COM(2011) 669, galutinis, Briuselis.
15. 2006 m. kovo 15 d. Komisijos ataskaita Europos Parlamentui ir Tarybai. Direktyvos 1999/93EB dėl Bendrijos elektroninių parašų reguliavimo sistemos veikimo ataskaita. COM(2006) 120, galutinis, Briuselis.
16. 2009 m. gruodžio 22 d. Komisijos dokumentas M/460 EN, Standartizavimo mandatas Europos standartizavimo organizacijoms CEN, CENELEC ir ETSI informacinių ir ryšių technologijų srityje taikomas elektroniniams parašams, Briuselis.
17. Public consultation „Digital Agenda for Europe: Electronic identification, authentication and signatures in the European digital single market“, 18.02.2011, INFSO.C /A3/F5/H2, Brussels.
18. CWA 14169 (2002): saugi parašo formavimo įranga (pakeistas CWA 14169:2004: Saugūs parašo kūrimo įtaisai - EAL 4+).
19. CWA 14167–1 (2003): Saugumo reikalavimai, keliami patikimoms elektroninių parašų sertifikatų valdymo sistemoms. 1 dalis. Sisteminiai saugumo reikalavimai.
20. CWA 14167-2:2002: Saugumo reikalavimai, keliami patikimoms elektroninių parašų sertifikatų valdymo sistemoms. 2 dalis. Sertifikavimo paslaugų teikėjų pasirašymo operacijų šifravimo modulis. Apsaugos profilis (pakeistas CWA 14167-2:2004).
21. ETSI TS 101 456 v1.2.1(2002-04). Policy requirements for certification authorities issuing qualified certificates.
22. UNCITRAL Model Law on Electronic Commerce Guide to Enactment with 1996 with additional article 5 bis as adopted in 1998, UN, New York, 1999.
23. UNCITRAL Model Law on Electronic Signatures with Guide to Enactment. UN, New York, 2002.
24. 2002 m. vasario 28 d. Lietuvos Respublikos civilinio proceso kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas Nr. IX-743. Civilinio proceso kodeksas. *Valstybės žinios*, 2002, nr. 36-1340 (su vėlesniais pakeitimais ir papildymais).
25. 2000 m. liepos 6 d. Lietuvos Respublikos elektroninio parašo įstatymas Nr. VIII-1822. *Valstybės žinios*, 2000, nr. 61-1827 (su vėlesniais pakeitimais ir papildymais).
26. 1994 m. gegužės 31 d. Lietuvos Respublikos teismų įstatymas Nr. I-480. *Valstybės žinios*, 1994, nr. 46-851 (su vėlesniais pakeitimais ir papildymais).
27. 1996 m. birželio 11 d. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas Nr. I-1374. *Valstybės žinios*, 1996, nr. 63-1479 (su vėlesniais pakeitimais ir papildymais).
28. 2002 m. gruodžio 31 d. Lietuvos Respublikos Vyriausybės nutarimas Nr. 2108 „Dėl Reikalavimų kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams, Reikalavimų elektroninio parašo įrangai, Kvalifikuotus sertifikatus sudarančių sertifikavimo paslaugų teikėjų registravimo tvarkos ir Elektroninio parašo priežiūros reglamento patvirtinimo“, *Valstybės*

žinios, 2003, nr. 2-47 (su vėlesniais pakeitimais ir papildymais).
29. Lietuvos Respublikos teisingumo ministro 2012 m. gruodžio 13 d. įsakymas Nr. 1R-332 „Dėl Procesinių dokumentų pateikimo teismui ir jų įteikimo asmenims elektroninių ryšių priemonėmis tvarkos aprašo patvirtinimo“, *Valstybės žinios*, 2012, nr. 147-7579.
30. Lietuvos archyvų departamento prie Lietuvos Respublikos Vyriausybės generalinio direktoriaus 2008 m. spalio 9 d. įsakymas Nr. V-119 „Dėl elektroniniu parašu pasirašyto elektroninio dokumento specifikacijos reikalavimų aprašo patvirtinimo“. *Valstybės žinios,* 2008, nr. 118-4488.
31. Lietuvos archyvų departamento prie Lietuvos Respublikos Vyriausybės generalinio direktoriaus 2009 m. rugsėjo 7 d. įsakymas Nr. V-60 „Dėl Elektroniniu parašu pasirašyto elektroninio dokumento specifikacijos ADOC-V1.0 patvirtinimo“. *Valstybės žinios*, 2009, nr. 108-4574.
32. Law for the Electronic Document and Electronic Signature of the Republic of Bulgaria, SG. 34/6 April 2001 [interaktyvus. Žiūrėta 2012-09-25]. Prieiga per internetą: <http://www.crc.bg/files/_en/ZED_ENG_15.01.2008.htm>.
33. Act XXXV of 2001 on Electronic Signatures of the Republic of Hungary (2001. évi XXXV. törvény). *Kihirdetve: 2001. VI. 12* [interaktyvus. Žiūrėta 2012-09-25]. Prieiga per internetą: <http://english.nmhh.hu/dokumentum/150091/actxxxvof2001_110210.pdf>.

Teismų ir neteisminių institucijų praktika

34. Lietuvos Aukščiausiojo Teismo Civilinių bylų skyriaus teisėjų kolegijos 2000 m. gegužės 29 d. nutartis byloje *R. Beliackas v. UAB „Sabina“*, civilinė byla Nr. 3K-3-619/2000.
35. Lietuvos Aukščiausiojo Teismo 2002 m. vasario 20 d. nutartis civilinėje byloje *Ž. Šapalas v. AB Lietuvos taupomasis bankas*, civilinė byla Nr. 3K-3-390/2002.
36. Lietuvos Aukščiausiojo Teismo Civilinių bylų skyriaus teisėjų kolegijos 2005 m. lapkričio 2 d. nutartis civilinėje byloje *UAB „Miltzer and Munch Fortransas“ vs. UAB „Dalila ir partneriai“,* civilinė byla Nr. 3K-3-535/2005.
37. Lietuvos Aukščiausiojo Teismo Civilinių bylų skyriaus teisėjų kolegijos 2006 m. kovo 6 d. nutartis civilinėje byloje *„Simon Louwerse International Transport“ v. UAB „Dinaka“,* civilinė byla Nr. 3K-3-169/2006.
38. Lietuvos apeliacinio teismo 2011 m. spalio 10 d. nutartis byloje *UAB „Furnitūra Marketingas“ v. UAB „DHL Lietuva“,* civilinė byla Nr. 2A-435/2011.
39. Lietuvos Aukščiausiojo Teismo Civilinių bylų skyriaus teisėjų kolegijos 2012 m. vasario 1 d. nutartis byloje *UAB „Vidarta“ v. V.J.*, civilinė byla Nr. 3K-3-23/2012.
40. Lietuvos vyriausiojo administracinio teismo 2012 m. gruodžio 18 d. nutartis byloje Nr. A143-2740/2012.

Specialioji literatūra

41. BECHINI U. *Bread and Donkey for Breakfast: How IT law false friends can confound lawmakers: an Italian tale about digital signatares*. 2009 [interaktyvus. Žiūrėta 2012-10-21]. Prieiga per internetą: <home.datacomm.ch/ugobechini/BECHINI_Bread_and_Donkey.pdf>.
42. *Black's Law Dictionary* (ed. by Bryan A. Garner), Eighth ed., Thomson West, 2004.
43. CIMANDER, R.; HANSEN, M.; KUBICEK, H. *Electronic Signatures as Obstacle for Cross-Border E-Procurement in Europe Lessons from the PROCURE-project*. 2009 [Interaktyvus. Žiūrėta 2012-11-15]. Prieiga per internetą: <https://www.eid-stork.eu/dmdocuments/public/ElectronicSignaturesAsObstaclesForCross-BorderE-ProcurementInEurope_LessonsFromThePROCUREProject.pdf>.
44. CIVILKA, M.; LAMANAUSKAS, T. Elektroninio pašto įteisinimas: probleminiai aspektai pagal ES ir LR teisę. *Teisės problemos*, 2004, nr. 2 (44).
45. CIVILKA, M. Elektroninės komercijos teisinis reguliavimas: nuo durstinio iki siuvinio. *Justitia*, 2006, nr. 3.
46. DALBY, S. *Authenticity/Authentication Definitions and Sources*, InterPARES 2 Project, Policy Cross-domain, 2004. Prieiga per internetą: <http://www.interpares.org/display_file.cfm?doc=ip2%28policy%29authenticity_definitions-sources.pdf>.
47. DUMORTIER, J.; VANDEZANDE, N. *Critical Observations on the Proposed EU Regulation for Electronic Identification and Trust Services for Electronic Transactions in the Internal Market*. The Interdisciplinary Centre for Law and Information Technology (ICRI), K.U.Leuven, 2012 [Interaktyvus. Žiūrėta 2012-11-15]. Prieiga per

internetą: <https://www.law.kuleuven.be/icri/ssrnpapers/37ICRI_Working_Paper_9_2012.pdf>.
48. DUMORTIER, J.; KELM S.; *et al*. *The Legal and Market Aspects of Electronic Signatures in Europe*, Study for the European Commission. 2003 [interaktyvus. Žiūrėta 2012-11-15]. Prieiga per internetą: <http://ec.europa.eu/information_society/policy/esignature/docs/electronic_sig_report.pdf>.
49. FICHER, N. The rise and Fall of the Country of Origin Principle in the EU Services Directive. *Essays in Transnational Economic Law*, 2006, No. 54. Martin-Luther-Universität Halle-Wittenberg.
50. GRIJPINK, J. M.; PRINS, J. E.J. New Rules for Anonymous Electronic Transactions? An Exploration of the Private Law Implications of Digital Anonymity. In NICOLL C.; *et al*. (Eds), *Digital Anonymity and the Law. Tensions and Dimensions*. 2003, ITeR, The Hague. [Interaktyvus. Žiūrėta 2012-11-15]. Prieiga per internetą: <http://arno.uvt.nl/show.cgi?fid=4933>.
51. HOEPNER, P. *Study PKI and Certificate Usage in Europe 2006*, Fraunhofer Institute FOKUS, 2006 [interaktyvus. Žiūrėta 2012-11-15]. Prieiga per internetą: <http://www.ecom.or.jp/report/Study_on_PKI_2006_in_EUROPE-FINAL.pdf>.
52. KIRK, J. *Comodo Hacker Claims Credit for DigiNotar Attack in PC World*. 2011 m. rugsėjo 6 d. [interaktyvus. Žiūrėta 2012-12-15]. Prieiga per internetą: <http://www.computerworld.com/s/article/9219739/Comodo_hacker_claims_credit_for_DigiNotar_attack>.
53. KORSAKAITĖ, D. Viešasis interesas valstybinio reguliavimo požiūriu: sampratos analizė ir formulavimas. *Ekonomika*, 2006 (76).
54. KRAWCZYK, P. *When the EU qualified electronic signature becomes an information services preventer* [interaktyvus. Žiūrėta 2012-10-20]. Prieiga per internetą: <ipsec.pl/files/ipsec/when_electronic_signature_becomes_a_information_services_preventer_v5.pdf>.
55. LABORDE, C. M. *Electronic Signatures in International Contracts*. Frankfurt am Main: Peter Lang GmbH, 2010.
56. LEROUGE, J. F. Internet Effective Rules: The Role of Self-regulation. *The EDI Law Review* 8, Kluwer Law International, 2002, p. 197–207.
57. Lietuvos Respublikos ryšių reguliavimo tarnybos Lietuvos Respublikos elektroninio parašo įstatymo įgyvendinimo 2011 metų ataskaita [interaktyvus. Žiūrėta 2012-11-15]. Prieiga per internetą: <http://www.rrt.lt/download/15929/2011%20epi%20ataskaita%20final.pdf>.
58. MASON, S. *Electronic Signatures in Law.* 3rd ed., Cambridge University Press, 2012.
59. MASON, S.; BROMBY, M., *Response to Digital Agenda for Europe: Electronic identification, authentication and signatures in the European digital single market Public consultation* [interaktyvus. Žiūrėta 2012-10-21]. Prieiga per internetą: <http://ec.europa.eu/information_society/policy/esignature/docs/pub_cons/offline_contrib/bileta.pdf>.
60. NODLER, J. M. *Legal Framework of Electronic Signatures in the European Union and Germany*. Seminar in Network Security Institute of Computer Science Georg-August-Universitat Gottingen, 2006 [interaktyvus. Žiūrėta 2012-11-15]. Prieiga per internetą: <http://noedler.de/artikel/legal-framework-of-electronic-signatures.tex>.
61. REED, C. *Internet law: text and materials*. Butterworths, London, 2000.
62. ROSSNAGEL, H. *Mobile Qualified Electronic Signatures for Secure Mobile Brokerage* [interaktyvus. Žiūrėta 2012-12-15]. Prieiga per internetą: <http://publikationen.stub.uni-frankfurt.de/files/2030/MobileQualifiedElectronicSigna1085.pdf>.
63. SEALED; *et al. Study on an electronic identification, authentication and signature policy (IAS)*. 17 August 2012 [Interaktyvus]. [Žiūrėta 2012-12-15] Prieiga per internetą:<http://www.iasproject.eu/attachments/File/deliverables/IAS_Deliverable_D1_%28version_3_-_Final_17_aug2012%29.pdf>.
64. SEALED, et al. *Study on the standardisation aspects of eSignature.* A study for the European Commission (DG Information Society and Media). 2007 [interaktyvus. Žiūrėta 2012-11-15]. Prieiga per internetą: <http://ec.europa.eu/information_society/policy/esignature/docs/standardisation/report_esign_standard.pdf>.
65. SEALED, *et.al. Study on Cross-Border Interoperability of e-signatures* [interaktyvus. Žiūrėta 2012-11-15]. Prieiga per internetą: <http://ec.europa.eu/information_society/policy/e-signature/ crobies_study/index_en.htm>.

66. SEALED, *et. al. Study on Cross-Border Interoperability of eSignatures (CROBIES): Framework for Secure Signature Creation Devices cross-border recognition.* (Final report). 2010 [interaktyvus. Žiūrėta 2012-11-15]. Prieiga per internetą: <http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd4.pdf>.
67. SEALED, *et. al. Study on Cross-Border Interoperability of eSignatures (CROBIES): "Trusted Lists" Implementer's Guide.* (Final report). 2010 [interaktyvus. Žiūrėta 2012-11-15]. Prieiga per internetą: <http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables /crobiesd2.1.pdf>.
68. SEALED, *et. al. Study on Cross-Border Interoperability of eSignatures (CROBIES): Common Supervision Model of Practices of Certification Service Providers issuing Qualified Certificates.* (Final report). 2010 [interaktyvus. Žiūrėta 2012-11-15]. Prieiga per internetą: <http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd1.pdf>.
69. SIEMENS, Time.lex. *Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications.* Prepared for the IDABC programme. 2007 [interaktyvus. Žiūrėta 2012-11-15]. Prieiga per internetą: <ec.europa.eu/idabc/servlets/Docba2e.pdf?id=29484>.
70. SIEMENS, Time.lex. *Preliminary Study on the electronic provision of certificates and attestations usually required in public procurement procedures*. 2007 [interaktyvus. Žiūrėta 2012-11-15]. Prieiga per internetą: <http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/ecertificates-study_en.pdf>.
71. SIEMS, M. The EU Directive on Electronic Signatures – A Worldwide Model or a Fruitless Attempt to regulate Future. *International Review of Law, Computers and Technology*, 2002, Vol. 16, No. 1.
72. ŠTITILIS, D.; *et al*. Preconditions for personal identification in cyberspace. *Jurisprudencija,* 2011, 18(2), p. 716–718.
73. The Interdisciplinary Centre for Law & Information Technology (ICRI). Legal study on the national legal and administrative practices regarding the validity and mutual recognition of electronic documents, with a view to identifying the existing legal barriers for enterprises. A study for the European Commission (DG Information Society and Media (ELDOC Study). D3.6 – Final Report, 2006 [interaktyvus. Žiūrėta 2012-11-15]. Prieiga per internetą: <http://ec.europa.eu/enterprise/sectors/ict/files/dumortier-final-report-draft_en.pdf>.
74. VAITKEVIČIŪTĖ, V. *Tarptautinių žodžių žodynas*. Vilnius, 2001.
75. *Webster's Revised Unabridged Dictionary*, 1998, ed. by MICRA, Inc. of Plainfield, NJ.
76. WUBBEN, M.; *et al*. Legal aspects of the Digital Single Market Current framework, barriers and developments, Considerati, Amsterdam, 2012 [interaktyvus. Žiūrėta 2012-11-30]. Prieiga per internetą: <http://www.considerati.com/fileadmin/Legal_aspects_of_Digital_Single_Market.pdf>.

ISSUES OF OPERATION OF ELECTRONIC SIGNATURES IN THE INTERNAL MARKET

Mindaugas Civilka

S u m m a r y

This article analyses the set of reasons, which have conditioned the failure of the functioning of the Directive. The author discusses the most topical aspects pertaining to achievement of cross-border operation of electronic signatures in the internal market, especially those, which have become real obstacles for the free circulation of electronic signatures (Article 4, paragraph 2). This paper focuses on analysis of the Directive, those EU legal acts, which have been designated for its implementation acts as well as other related EU documents. This article also focuses on few selected aspects critical for assessment of transposition of the Directive into Lithuanian legal system, highlighting some of the peculiarities of operation and use of electronic signature within the boundaries of Lithuanian legal system. The paper also presents a concise analysis of the preconditions for the regulatory framework as newly proposed by Commission.

Įteikta 2013 m. sausio 10 d.
Priimta publikuoti 2013 m. kovo 21 d.