

KAI KURIE ELEKTRONINIŲ ĮRODYMŲ PANAUDOJIMO
CIVILINIAME PROCESSE ASPEKTAI

Rytis Čėsna *

Mykolo Romerio universiteto Ekonomikos ir finansų fakulteto Informatikos ir statistikos katedra
Ateities g. 20, LT-08303 Vilnius
Elektroninis paštas rytis.cesna@gmail.com
Telefonas: +370 655 23103

Pateikta 2006 m. lapkričio 16 d., parengta spausdinti 2007 m. spalio 9 d.

Santrauka. Informacinių technologijų plėtra atvėrė iš esmės naujas globalaus bendravimo ir sąveikos galimybes – sukurta pasaulio komunikacinė erdvė be įprastų laiko ir atstumo suvaržymų. Milijonai elektroninių duomenų pranešimų sukuriama ir siunčiama šiuolaikinėmis elektroninės komunikacijos priemonėmis. Kai kurie verslo procesai, sutarčių sudarymas ir paslaugų teikimas jau yra perkelti į elektroninę erdvę, ir šių procesų rezultatai gali būti fiksuojami išimtinai tik elektroninėmis priemonėmis sukuriant (sugeneruojant) elektroninius duomenis. Kadangi tik tokie duomenys išimtinai gali liudyti atitinkamus faktus, svarbu, kad jie galėtų būti panaudoti įrodinėjant teisme be papildomų apribojimų ar reikalavimų. Tiesa, kol kas teisinė sistema nėra iki galo pasiruošusi tokiems iššūkiams, ir ne visais atvejais elektroniniai duomenys gali būti pateikti teismui ir panaudoti kaip įrodymai.

Pagrindinės sąvokos: elektroniniai duomenys, elektroniniai įrodymai, elektroninė komercija, elektroninis parašas.

IVADAS

Informacinių technologijų plėtra atvėrė iš esmės naujas globalaus bendravimo ir sąveikos galimybes – sukurta pasaulio komunikacinė erdvė be įprastų laiko ir atstumo suvaržymų. Naujosios technologijos turėjo įtakos ir naujo tipo komercinių santykių – elektroninės komercijos – raidai bei naujoms galimybėms verslo įmonėms rinkti, sugoti, perduoti ir analizuoti didelius duomenų kiekius, gaunamus iš klientų ir apie savo klientus.

2001 metų pabaigoje pasaulyje naudota 625 milijonai kompiuterių [1, p. 1–5]. 2001 metais vien Šiaurės Amerikoje verslo įmonės išsiuntė apie 2,5 milijardo elektroninio pašto žinučių [2, p. 4]. Pasaulio interneto vartotojų skaičius augo nuo 308,8 milijono vartotojų 2002 metų pradžioje iki 1,1 milijardo vartotojų 2005 metais [3, p. 7, 19]. International Data Corporation nurodo, kad kasdien išsiunčiama 31 bilijonas asmeninių elektroninio pašto žinučių ir prognozavo, kad 2006 me-

tais šis skaičius sieks 60 bilijonų elektroninio pašto žinučių per dieną [4, p. 2].

Šiuo metu vis daugiau komercinių santykių naudojamos elektroninės komunikacijos priemonės. Ne mažai įmonių keičiasi informacija (duomenimis), derasi dėl sandorių, priima vartotojų skundus, netgi sudaro sandorius pateikdamos užsakymus elektroniniu paštu arba parduodamos prekes interneto parduotuvėse. Kai kurie specialūs teisės aktai (pvz., Mokėjimų įstatymas) netgi įtvirtina konkrečius elektroninius instrumentus¹, leidžiančius vykdyti veiklą elektroninėje erdvėje [5, 7 str.].

Elektroninių duomenų panaudojimo teisiniame procese klausimai kaip tik ir yra vienas iš svarbiausių klausimų vienodinant elektroninėje ir materialiojoje erdvėje užfiksuotos informacijos panaudojimo galimybes taip panaikinant bet kokias abejones dėl elektroninės erdvės nepatikimumo.

Taigi visa tai rodo, kad elektroninių duomenų panaudojimo teisiniuose procesuose mokslinė analizė yra

* Mykolo Romerio universiteto Ekonomikos ir finansų fakulteto Informatikos ir statistikos katedros doktorantas.

¹ Mokėjimų įstatymo 7 str. įtvirtina nuostatą kad „mokėjimo nurodymai, mokėjimo, debeto bei inkasiniai pavedimai gali būti ne tik rašytinės, bet ir elektroninės formos“.

reikalinga, todėl šiame straipsnyje analizuojami elektroninių duomenų panaudojimo teisme leistinumo ir šių duomenų patikimumo aspektai bei jų panaudojimo teisme civilinėse bylose galimybės.

1. ELEKTRONINIŲ DUOMENŲ PANAUDOJIMO ĮRODYMAMS SVARBA

Elektroninėms informacijos apdorojimo priemonėms vis labiau skverbiantis į kasdienę veiklą, internetas ir daugialypė terpė vystomi neįtikinėtinais tempais. Komunikacija naudojant elektronines priemones tampa vis įprastesniu komunikavimo būdu vien todėl, kad turi nenuginčijamą pranašumą, palyginti su popierine komunikacija:

- 1) duomenys sukuriami (sugeneruojami) ir apdorojami bei išsiunčiami toje pačioje aplinkoje (elektroninėje erdvėje) ir tomis pačiomis priemonėmis;
- 2) duomenys gali būti siunčiami iš vienos pasaulio vietos į kitą nepaisant atstumų beveik be laiko sąnaudų;
- 3) elektroninių duomenų dauginimas ir kopijavimas yra palyginti nebrangus ir greitas procesas;
- 4) elektroniniai duomenys nereikalauja daug vietos saugoti ir archyvuoti.

Tačiau iškyla bent keletas aiškių elektroninių duomenų panaudojimo probleminių aspektų, kurių negalima nepaisyti. Pirmą, gana sudėtinga nustatyti ir susekti manipuliavimą elektroniniais duomenimis (duomenų pakeitimą). Įprastame popieriniame dokumente informacijos pakeitimus galima nustatyti kriminalistikoje gerai žinomais ir nuolat tobulinamais būdais, tuo tarpu elektroninių duomenų pakeitimai įprastiniais kriminalistikos metodais negali būti nustatyti. Antra, elektroninė komunikacija užtikrina galimybę susisiekti žmonėms visame pasaulyje per atstumą anonimiškai, asmenys, bendraujantys elektroninėmis priemonėmis, vienas kito nemato ir nepažįsta realioje erdvėje, todėl iškyla asmens, siuntusio ar sukūrusio elektroninius duomenis, identifikavimo problema.

Kai kuriais atvejais tam tikrų veiklų buvimą galima įrodyti tik elektroniniais duomenimis. Sprendžiant ginčus teismuose dėl tokių veiklų gauti elektroniniai duomenys dažniausiai yra vienintelė tokių bylų įrodymų rūšis ir pagrindas. Kaip tokių veiklų pavyzdys galėtų būti įvairūs manipuliavimai elektroninių ryšių didmeninėmis paslaugomis. Pavyzdys galėtų būti byla *UAB „Bitė GSM prieš AB „Lietuvos telekomas“* [6] dėl pokalbių srautų siuntimo nesutartomis kryptimis. Vieninteliai įrodymai šiuo atveju buvo apibendrinti skambučių duomenų įrašai (CDR)², generuojami telefonų stotyse. Kitas pavyzdys galėtų būti nepageidaujama reklaminių pranešimų platinimo (angl. *spamming*) byla (*Ž. Budros II „Sėkmės sistemos“ prieš AB „Lietuvos telekomas“*) [7, p. 2].

² CDR Call Data Record – elektroninis įrašas, kuriame saugoma informacija apie įvykusį skambutį.

Reikia pažymėti, kad kai kuriais atvejais sukuriant elektroninius duomenis ir tvirtinant jų tikrumą turi tiesiogiai dalyvauti žmogus, patvirtinantis atitinkamo fakto ar įvykio buvimą, kitais atvejais šie įrašai generuojami automatiškai. Bantin [8, p. 16–24] atsižvelgiant į žmogaus dalyvavimą procese išskiria dvi elektroninių duomenų rūšis:

- 1) elektroniniai duomenys, kurie parodo tam tikro įvykio ar fakto buvimą ir kurių sudarymui būtinas asmens ar kelių asmenų aktyvus dalyvavimas (pvz., elektroninė sutartis);
- 2) elektroniniai duomenys, kurie liudija faktą ar įvykį, tačiau generuojami automatiškai ir tiesioginis žmogaus dalyvavimas šių duomenų sukūrimo (generavimo) procese nėra būtinas.

Toliau šiame straipsnyje elektroninių duomenų panaudojimo aspektai ir bus nagrinėjami remiantis būtent šia klasifikacija.

2. TARPTAUTINIAI DOKUMENTAI

Elektroninių duomenų teisėtumo klausimai užsienyje analizuojami gana seniai. Dar 1981 metais Europos Taryba priėmė Rekomendaciją Nr. 81 (20) dėl teisės aktų, susijusių su reikalavimais rašytiniams įrodymams ir dokumentams bei užrašų kompiuterinių reprodukcijų leistinumu, harmonizavimo [9]. Šiame dokumente pabrėžiamas tradicinių (popierinių) dokumentų saugojimas elektroninėse laikmenose. Neabejotinai svarbus tarptautinis dokumentas – 1985 metų Jungtinių Tautų Tarptautinės prekybos teisės komisijos (UNCITRAL) Rekomendacija dėl kompiuterinių įrašų (dokumentų) teisinės galios [10]. Rekomendacijoje pateikiami teisės aktų, reglamentuojančių kompiuterinių dokumentų panaudojimą įrodinėjant aplinkybes teisiniuose procesuose, siūlymai. Siūloma užtikrinti elektroninių duomenų panaudojimo kaip įrodymų leistinumą ir atitinkamai keičiant teisės aktus neriboti technologijų vystymo ir jų panaudojimo nepagrįstais formaliais teisiniais reikalavimais.

1996 metais UNCITRAL patvirtino tipinį Elektroninės komercijos įstatymo modelį [12]. Šiame dokumente valstybėms Jungtinių Tautų narėms siūloma pašalinti formalias kliūtis sudarinėti sandorius elektroninėje erdvėje. Šiuo modeliu siekiama suvienodinti valstybių narių teisinę bazę, įteisinti elektroninę sutarties sudarymo formą ir prilyginti ją aiškinamajame šio įstatymo rašte rašytinei. Pavyzdiniame Elektroninės komercijos įstatyme įteisinamas funkcinio ekvivalentiškumo ir elektroninės dokumento formos nediskriminavimo principas – šios formos dokumentų teisinė padėtis ekvivalentiška kaip ir popierinių dokumentų.

Tipinis elektroninės komercijos įstatymo modelis nurodo keletą funkcinių reikalavimų elektroniniams duomenims, kuriuos turi atitikti elektroniniai duomenys, kad taptų leistinu įrodymu teisme [7, (6 ir 8)]:

- 1) elektroniniai duomenys turi būti perskaitomi;
- 2) elektroninius duomenis patvirtinantis asmuo turi būti aiškiai identifikuojamas;
- 3) elektroniniai duomenys turi nesikeisti gana ilgą laiką.

3. ELEKTRONINIAI DUOMENYS LIETUVOS CIVILINIAME PROCESE

Lietuvos Respublikos civilinio proceso kodekso (toliau – LR CPK) 177 str. nurodoma, kad įrodymais civilinėje byloje gali būti bet kokie faktiniai duomenys, kuriais remdamasis teismas įstatymų nustatyta tvarka konstatuoja, kad yra aplinkybių, pagrindžiančių šalių reikalavimus bei atsikirtimus, ir kitokių aplinkybių, turinčių reikšmės bylai teisingai išspręsti, arba kad jų nėra. Taip pat pateikiamas leistinių įrodinėjimo priemonių sąrašas: šalių ir trečiųjų asmenų paaiškinimai, liudytojų parodymai, rašytiniai įrodymai, daiktiniai įrodymai, apžiūrų protokolai ir ekspertų išvados [13, 177 str. 2 d.].

Akivaizdu, kad Lietuvos civiliniame procese elektroniniai duomenys kaip atskiros įrodinėjimo priemonės neišskiriama ir jų panaudojimo leistinumą klausimas gali būti sprendžiamas tik tinkamai aiškinant įstatymą. Lietuvos Aukščiausiasis Teismas civilinėje byloje konstatavo, kad „viena iš rašytinių tekstų perdavimo priemonių yra telekomunikacija, kurios techninė priemonė yra ir fakso aparatas“ [14]. Atsižvelgiant į tai, kad telekomunikacijų (elektroninių ryšių) priemonėmis perduodami būtent elektroniniai duomenys, galima drąsiai daryti išvadą, kad Aukščiausiasis Teismas nagrinėtoje byloje pripažino, jog elektroninė informacija yra viena iš rašytinės informacijos rūšių ir jos pateikimo leistinumą tiesiogiai susijęs su rašytinių įrodymų pateikimo leistinumu.

LR CPK 197 str. rašytiniais įrodymais pripažįstami dokumentai, dalykinio ir asmeninio susirašinėjimo medžiaga ir kitokie raštai, kuriuose yra duomenų apie aplinkybes, turinčias reikšmės bylai. Taip pat kodeksas nustato ir rašytinių įrodymų pateikimo teismui taisykles. Nurodoma, kad rašytinei dokumento formai prilyginami dalyvaujančių byloje asmenų pasirašyti dokumentai, įstatymų ir kitų teisės aktų nustatyta tvarka perduoti telekomunikacijų galiniais įrenginiais [13, 198 str.]. Iš pirmo žvilgsnio būtų galima daryti išvadą, kad elektroniniai duomenys, atspausdinti popieriuje ir pasirašyti byloje dalyvaujančių asmenų, būtų pakankami pripažįstant juos tinkamu įrodymu. Šiuo atveju šalys gali panaudoti elektroninius įrodymus, o teismas juos pripažinti leistiniais įprastais rašytiniais įrodymais. Taip nepažeidžiamas įrodymų leistinumą principas. Tačiau šis požiūris turi ir trūkumų:

1. Taip pateikti galima tik įrodymus, pateikiamus tik byloje dalyvaujančių asmenų. Iškyla problema, kaip tinkamai pateikti elektroninius duomenis, sukurtus (sugeneruotus) trečiųjų šalių (pvz., informaciją apie telekomunikacijų įvykius ir kt.). Vadovaujantis tokiu traktavimu šie duomenys turėtų būti tik popieriuje.
2. Kai kurie elektroniniai duomenys, atspausdinti popieriuje, praras savo prasmę ir jais nebus galima remtis. Pavyzdžiui, atspausdinus popieriuje įvairių programų ar duomenų bazių kodus, nebus galima įvertinti jų veikimo tinkamumo ir nustatyti, ar programinis kodas yra veiksnus ir ką konkrečiai programa atlieka.

3. Kai kuriais atvejais vienos iš proceso dalyvių pasirašytas popierinis dokumentas bus nepakankamas faktui įrodyti (elektroninė sutartis turi būti pasirašoma abiejų šalių).

Šiuo atveju galima daryti išvadą, kad teismui galima pateikti popieriuje atspausdintus elektroninius duomenis, tačiau ne visais atvejais tai bus pakankama ir tinkama tokių duomenų pateikimo forma.

4. ELEKTRONINĖS SUTARTYS

Kaip jau buvo minėta, nagrinėjant elektroninių duomenų panaudojimo kaip įrodymų aspektus šiame straipsnyje remiamasi Bantino pasiūlyta klasifikacija [8, p. 22–40]. Elektroninės sutartys šiuo atžvilgiu yra elektroniniai duomenys, kuriems sukurti ir patvirtinti būtinas žmogaus dalyvavimas. Sudarydamas sutartį asmuo patvirtina savo valią prisiimti įsipareigojimus. Valios patvirtinimas įprastai yra išreiškiamas pasirašant rašytinę sutartį, arba konkludentiniais veiksmais.

Lietuvos Respublikos civiliniame kodekse (toliau – LR CK) nurodyta, kokie sandoriai turi būti sudaromi rašytine forma, taip pat kad sandoriai ir sutartys gali būti sudaromi naudojant telekomunikacijų galinius įrenginius (elektronines ryšio priemones), ir tokie sandoriai ir sutartys yra vertinami kaip paprasta rašytine forma sudaryti, jeigu yra užtikrinta teksto apsauga ir galima identifikuoti jį siuntusios šalies parašą (LR CK 1.73 str. ir 6.192 str.). Taigi LR CK sutartims, sudarytoms elektroninėmis priemonėmis, kad jos būtų pripažintos kaip sudarytos paprasta rašytine forma, iš esmės numatyti du reikalavimai:

- 1) sutarties tekstas turi būti apsaugotas;
- 2) sutarties parašas turi būti identifikuojamas, t. y. nustatoma, kas yra sutartį pasirašęs asmuo.

Tokie reikalavimai pagrįsti principiniais civilinės teisės reikalavimais – sudarantys sutartis asmenys (sutarties šalys) turi būti aiškiai ir vienareikšmiškai identifikuojami, o sudarytos sutarties tekstas turi būti apsaugotas nuo pakeitimų, kad vėliau iškilus nesutarimams būtų galima juo remtis kaip įrodymu.

Detalesnius elektroninio pasirašymo ir elektroninės informacijos panaudojimo teisiniuose procesuose reikalavimus nustato Elektroninio parašo įstatymas. Elektroninio parašo įstatyme (EPI) 8 str. nurodyta, kad saugus elektroninis parašas, sukurtas saugia parašo formavimo įranga ir patvirtintas galiojančiu kvalifikuotu sertifikatu, turi tokią pat teisinę galią kaip ir parašas rašytiniuose dokumentuose ir yra leistinas kaip įrodinėjimo priemonė teisme. Taip pat EPI leidžia elektroninio parašo naudotojams susitarti dėl naudojamos elektroninio parašo sistemos galiojimo įtvirtinant, kad elektroninis parašas visais atvejais turi parašo rašytiniuose dokumentuose galią, jeigu parašų naudotojai tarpusavyje dėl to susitaria.

Saugiam elektroniniam parašui keliami tokie reikalavimai (EPI 2 str. 5 d.):

- 1) yra vienareikšmiškai susietas su pasirašiusiu asmeniu;
- 2) leidžia identifikuoti pasirašiusį asmenį;

- 3) yra sukurtas priemonėmis, kurias pasirašęs asmuo gali tvarkyti tik savo valia;
- 4) yra susijęs su pasirašytais duomenimis taip, kad kiekvienas šių duomenų pakeitimas yra pastebimas.

Reikalavimai, keliami saugiam elektroniniam parašui, susiję su LR CK reikalavimais teksto apsaugai ir pasirašiusio asmens identifikavimui, tik šie reikalavimai papildomai detalizuojami užtikrinant, kad tik pasirašantis asmuo galėtų pasirašyti elektroninę informaciją ir jokia trečioji šalis vietoj jo tokių veiksmų negalėtų atlikti. Taigi EPĮ 1, 2, ir 3 reikalavimai yra LR CK antrojo reikalavimo – parašo identifikavimo ir pasirašiusio asmens nustatymo – detalizavimas, o 4 reikalavimas visiškai atitinka LR CK nurodomą sutarties teksto apsaugos reikalavimą, todėl įgyvendinus EPĮ reikalavimus yra įgyvendinami ir LR CK reikalavimai.

LR CK pripažįstamos sutartys, sudaromos elektroninėmis priemonėmis. LR CK 6 knygos 4 skirsnyje aprašomas vartotojiškos pirkimo-pardavimo sutarties, sudarytos elektroninėmis priemonėmis, leistinumai ir reikalavimai šiai sutarčiai. Ir LR CK reikalavimai, ir Daiktų pardavimo ir paslaugų teikimo, kai sutartys sudaromos naudojant ryšio priemones, taisyklės nurodo du pagrindinius funkcinis elektroniniu būdu sudaromoms sutartims naudojamų ryšio priemonių saugumo ir asmenų, sudarančių šią sutartį, identifikavimo užtikrinimo reikalavimus. Iš esmės čia iškeliami du funkciniai reikalavimai: identifikavimo ir integrumo. Kadangi tokios sutarties egzistavimas, jos turinys ir vykdymo faktai bus paremti elektroniniais duomenimis, šie funkciniai reikalavimai elektroniniams duomenims (elektroninėms sutartims) taip pat turi būti taikomi.

5. ELEKTRONINIŲ DUOMENŲ VERTINIMAS

Nors LR CPK nurodoma, kad vertinant įrodymus jokiems įrodymams nėra suteikiama išankstinė įrodomoji galia ir teismas vertindamas įrodymų yra laisvas, tam tikrais atvejais yra išskiriami įrodymai, turintys didesnę įrodomąją galią. Čia susiduriama su *prima facie* įrodymų institutu, kuris yra laisvo įrodymo vertinimo principo išimtis [16]. Didesnė įrodomoji galia suteikiama dokumentams, išduotiems valstybės ar savivaldybės institucijų arba patvirtintiems kitų valstybės įgaliotų asmenų neviršijant jiems nustatytos kompetencijos ir laikantis tam tikriems dokumentams keliamų formos reikalavimų. Tokie įrodymai vadinami oficialiais rašytiniais įrodymais ir turi didesnę įrodomąją galią, reiškiančią, kad juose nurodyti juridiniai faktai laikomi visiškai įrodytais, kol jie nepaneigti kitais įrodymais, išskyrus liudytojų parodymus. LR CPK taip pat nurodoma, kad tokia įrodomoji galia gali būti suteikta ir kitiems dokumentams [13, 197 str.]. Kadangi elektroninė dokumentų forma taip pat neturi būti diskriminuojama, galima būtų teigti, kad tinkamai valstybės institucijos išduotas elektroninis dokumentas automatiškai turėtų oficialaus dokumento galią ir turėtų didesnę įrodomąją

galią. Tiesa, kol kas nėra nustatytos tvarkos, kaip tokie oficialūs elektroniniai dokumentai (pvz., Registrų centro išrašai, pažymos ir kt.) galėtų būti išduodami.

Visais atvejais nagrinėdamas pateiktų elektroninių duomenų įrodomąją vertę teisėjas turi nuspręsti, ar šie duomenys turi įrodomąją vertę, įvertinti, ar informacija, užfiksuota elektronine forma, yra patikima. Lietuvoje kol kas nėra elektroninių įrodymų vertinimo taisyklių, todėl galima bandyti remtis užsienio valstybių rekomendacijomis.

Jungtinių Valstijų Aukščiausiojo Teismo elektroninių įrodymų vertinimo taisyklėse pateiktas detalus sąrašas kriterijų, į kuriuos būtina atsižvelgti vertinant elektroninių duomenų patikimumą:

- 1) būdų ir metodų, kuriais buvo surinkti, saugoti ar perduoti įrodymai, patikimumas;
- 2) būdai, kuriais identifikuojamas dokumentą patvirtinęs asmuo (teksto autorius);
- 3) informacinių sistemų, kuriose elektroniniai duomenys buvo sugeneruoti ir saugomi, vientisumas, vertinant tiek techninę, tiek programinę įrangą;
- 4) informacijos, kuria remiantis buvo sukurti elektroniniai duomenys, tipas ir pobūdis;
- 5) kitokie veiksniai, kurie, teismo nuomone, galėjo turėti įtakos elektroninių duomenų vientisumui ir tikslumui [17, 7 str.].

Labai svarbi elektroninių įrodymų patikimumo užtikrinimo sritis – tinkamas elektroninių duomenų saugojimo procesas. Betts nurodo, kad elektroninės informacijos saugojimas yra rizikingas dėl palyginti gana greito šių duomenų saugojimo priemonių (elektroninių duomenų saugojimo laikmenų) nusidėvėjimo. Kitas elektroninių duomenų saugojimo iššūkis – greiti duomenų saugojimo įrangos (tiek techninės, tiek programinės) pokyčiai. Techninė įranga ir programos sensta palyginti labai greitai, nauja technika, naujos programos, duomenų įrašymo ir nuskaitymo būdai keičiasi kas dveji treji metai, ir kol kas nėra elektroninės sistemos, kurią būtų galima naudoti praėjus daugiau nei trisdešimčiai metų nuo jos įdiegimo.

Stephens (2000a) nurodo, kad daugelį metų archyvarai visame pasaulyje kūrė vertingų archyvinių duomenų išsaugojimo projektus, tiesa, šie projektai buvo skirti įprastiems duomenims, esantiems popieriuje, mikrofilmuose ar kitokiuose materialiuose saugojimo elementuose, išsaugoti [19, p. 8–26]. Šiuo metu archyvai materialia forma saugomus duomenis (dokumentus) perkelia į elektronines duomenų saugyklas. Aišku, saugant elektroninius, kaip ir materialios formos, duomenis, iškilis duomenų integruotumo bei prieinamumo užtikrinimo klausimai. Saugant duomenis elektronine forma iškilis bent du esminiai probleminiai saugojimo aspektai:

- 1) labai greiti technologiniai elektroninių duomenų saugojimo priemonių pokyčiai;
- 2) didėjantis visuomenės priklausomumas nuo elektroninių dokumentų.

Saugomų elektroninių duomenų rūšys yra:

- 1) elektroniniai duomenys, atspindintys verslo procesus ir veiklas, t. y. duomenys, susiję su veikos

pasekmėmis arba patys esantys šių veiklų rezultatais;

- 2) elektroniniai duomenys, patvirtinantys veiksmus ar transakcijas.

Stephens nurodo, kad materialūs archyviniai dokumentai, saugomi materialia forma, gali būti perskaityti ir suprasti be papildomų priemonių (tarpininkų) arba naudojant itin paprastas priemones (pvz., didinamąjį stiklą) [19, p. 8–26; 20, p. 68–71]. Archyvuojant tokie dokumentai paprastai įdedami į saugyklą, sukuriami jų paieškos aprašai ir dokumentai laikomi atitinkamoje saugoti tinkamoje aplinkoje. Tokie įrašai tinkamoje aplinkoje gali būti saugomi dešimtmečiais ir net amžiais, todėl materialių įrašų saugojimas dažniausiai yra vienkartinė užduotis, nereikalaujanti tolesnės papildomos priežiūros. Elektroniniai duomenys iš esmės skiriasi nuo materialių jau vien tuo, kad šių duomenų negalima pasiekti (perskaityti) be papildomų sudėtingų priemonių (tarpininkų). Šios priemonės yra techninė ir programinė kompiuterinė įranga, specialiai skirta pasiekti archyvuojamus duomenis ir, kaip žinoma, kintanti gana sparčiu tempu. Kintant kompiuterinei duomenų saugojimo technikai elektroninių duomenų saugojimas tampa nuolatinio proceso, siekiant užtikrinti duomenų išsaugojimą ir nuolatinį saugomų duomenų pasiekiamumą.

Elektroninis įrašas laikomas tinkamai suarchyvuotu ir saugomu, tik kai įrašo duomenys yra pasiekiami, perskaitomi ir autentiški. Siekiant įrodyti, kad saugomas elektroninis įrašas yra nepakeistas ir autentiškas, reikia atsakyti, ar:

- 1) duomenys yra tinkamai perkelti į saugojimo renginį;
- 2) duomenų saugykla (laikmena) nebuvo paveikta taip, kad duomenys joje išsikraipytų;
- 3) visi teisingi duomenys atgaminti iš saugyklos;
- 4) duomenų atgaminimo procesas buvo tinkamas ir tinkamai atliktas.

Stephens nurodo, kad dar vienas sunkumas, su kuriuo susiduriama saugant elektroninius duomenis, – elektroninių duomenų laikmenų tinkamumas saugoti ir jų atsparumas aplinkos poveikiui laikui bėgant [20, p. 68–71]. Lyginant su įprastomis rašytinės informacijos saugojimo priemonėmis (knygomis, segtuvais, bylomis, mikrofilmais), kuriose pažeidimai ir neigiamas aplinkos poveikis yra aiškiai matomi, pažaidimai elektroninėse informacijos saugojimo laikmenose dažniausiai nebus aiškiai pastebimi – juos galima pastebėti tik specialia įranga arba pradėjus naudoti laikmenoje saugomus elektroninius duomenis. Be to, netgi idealiomis informacijos saugojimo sąlygomis, elektroninės duomenų laikmenos yra patikimos tik palyginti trumpą laiką. Lawrence nurodo, kad elektroninės duomenų laikmenos kol kas nėra tinkamos saugoti duomenis ilgą laiką [21, p. 3–5]. Pavyzdžiui, šiuo metu informacijai saugoti plačiai naudojami optiniai CD ir DVD diskai gana greitai gali tapti nenaudojami atsiradus naujo tipo talpesnės ir patogesnės saugykloms. Su ta pačia problema susiduriama analizuojant naudojamus kompiuterinių failų formatus ir jų kaitą, kai informacijai saugoti naudojamas failų standartas laikui bėgant pakinta arba visiškai iš-

nyksta. Dėl išvardytų priežasčių kiekvienas elektroninių duomenų saugojimo būdas visuomet yra tik tarpinis sprendimas ir naudojamos duomenų saugyklos privalo būti laiku atnaujinamos (duplikuojamos) siekiant išvengti klaidų dėl duomenų laikmenų nusidėvėjimo ir duomenų saugojimo formatų ir struktūros naujovių.

Kaip jau buvo minėta anksčiau, svarbus elektroninių duomenų panaudojimo teisme aspektas yra šių duomenų autentiškumas. Iš pirmo žvilgsnio atrodytų, kad autentiški elektroniniai duomenys turi būti saugomi originalia technologija, kuria jie yra sukurti, ir originalios būsenos. Kita vertus, kuo labiau stengsimės išlaikyti duomenis tokia technologija kaip jie ir buvo sukurti, tuo nepraktiškesnis toks saugojimo būdas atrodys laikui bėgant. Elektroniniai duomenys laikui bėgant kaupsis, jų saugojimo technologijos keisis, ir ilgainiui saugykla virs ir techninių, ir programinių įrenginių sankaupa, kurią bus sunku prižiūrėti, sudėtinga bus vykdyti paiešką, nebūna išnaudojamos technologinės naujovės.

Svarbu žinoti, kad elektroniniai įrašai laikui bėgant taip pat šiek tiek keičiasi. Tokie pokyčiai turi įtakos saugomų duomenų autentiškumui ir nėra aiškiai pastebimi ir fiksuojami, jei saugykloje nėra patikimų saugojimo ir pasikeitimų nustatymo procedūrų. Tik tokios procedūros užtikrins, kad ilgainiui elektroninis įrašas išsaugos savo autentiškumą ir bus atgaminamas bei perskaitomas tinkamai, o tai yra vienas iš esminių elementų pateikiant įrodymus teismui ir vertinant šių įrodymų patikimumą. Galima teigti, kad elektroninių duomenų pažeidžiamumo [angl. *fragility*] problema turi įtakos šių duomenų patikimumui ir be tinkamo duomenų saugojimo procedūrų tokių elektroninių įrašų autentiškumas keltų rimtų abejonių.

Vienas iš galimų elektroninių duomenų saugojimo sprendimo būdų yra informacijos perkėlimas (kopijavimas) į naujos technologijos saugyklas arba elektroninės informacijos laikmenas. Elektroninių duomenų saugojimo ir apdorojimo programinės priemonės turi būti atnaujinamos ne rečiau kaip kas treji metai. Aišku, tokia veikla yra gana brangi ir kiekvienu atveju reikalauja didelių personalo pastangų ir tinkamo pasirėngimo. Darbuotojai turi išmanyti ne tik naujas priemones, bet ir senus duomenų formatus ir gebėti tinkamai sudėlioti duomenis, kad informacija arba svarbi jos dalis perkelti nebūtų prarasta. Neretai svarbių duomenų perkėlimo procesas pradamas nuo pilotinio (testavimo) proceso, kai į naują sistemą perkeliama bandomieji duomenys ir žiūrima, ar viskas tinkamai naudojama ir pritaikoma, taisomos klaidos ir neatitikimai, tobulinamas perkėlimo procesas, atrandamas tinkamiausias būsimas duomenų saugojimo formatus. Tik atitinkamai pasirenkus perkeliama tikrieji duomenys. Net dėl nedidelių programinės ar techninės įrangos netikslumų arba žmogaus klaidų perkeliamus elektroninius duomenis galima prarasti. Perkėlimo procedūros turi būti atliekamos taip, kad tokių duomenų praradimų būtų išvengta arba šie sutrikimai būtų laiku pastebėti ir tinkamai pašalinti.

Analizuojant duomenų saugojimą negalima praleisti ir tokios didelės ir svarbios duomenų dalies kaip metaduomenys – svarbios informacijos apie duomenų

struktūrą, tipus, formą ir kita. Metaduomenys yra informacija, kaip dokumentas turi būti atidaromas ir kokio tipo informacija jame yra, todėl jei nėra metaduomenų arba jie iškraipyti, saugoti elektroninius duomenis problemiška. Be to, jei nėra metaduomenų, tam tikrais atvejais elektroninių duomenų negalima vertinti kaip dokumentų ir pateikti jų teismui kaip tinkamo rašytinio įrodymo. Metaduomenų saugojimas ypač svarbus, kai organizacija vykdo transakcijas ir jos fiksuojamos elektroniniais duomenimis, t. y. organizacija naudoja elektroninių transakcijų apdorojimo sistemas (angl. *Transactions processing systems* (TPS)). Bantin nurodo, kad nepatikimos TPS naudojimas yra viena iš priežasčių, kodėl saugomi elektroniniai duomenys nebus pripažinti įrodymais [8, p. 12].

IŠVADOS

1. Šiuo metu teisinėje sistemoje iškyla nemažai papildomų problemų, susijusių su elektroninės informacijos panaudojimu teisinio įrodinėjimo procese – tai elektroninių duomenų pakeitimo (manipuliavimo) paprastumas; elektroninius duomenis siuntusių asmenų anonimiškumas; elektroninės informacijos originalo nebuvimas ir kitos.

2. Pagal galiojančius Lietuvos Respublikos įstatymus elektroniniai duomenys gali būti pateikiami atspausdinti kaip rašytinis įrodymas, tačiau tokiu atveju kyla formalių sunkumų pateikiant elektroninius duomenis, sugeneruotus trečiųjų šalių; neįmanoma įvertinti kompiuterių programų veikimo; atspausdinta elektroninė sutartis nebus pakankamas įrodymas susitarimo faktui įrodyti; sutarties spausdintame blanke nebus šalių parašų; nebus galima įsitikinti teksto apsauga.

3. Elektroninių įrodymų patikimumas priklauso ne tik nuo paties įrašo, bet ir nuo daugelio papildomų veiksnių: elektroninių duomenų generavimo būdų ir informacinių sistemų, kuriomis šie duomenys buvo generuojami, elektroninių duomenų saugojimo ir archyvavimo patikimumo, perdavimo sistemų saugumo, metaduomenų patikimumo ir kt., todėl abejonės dėl elektroninių duomenų patikimumo gali būti daug didesnės, nei vertinant kitus įrodymus.

4. Sprendžiant iškeltas šiame straipsnyje elektroninių įrodymų panaudojimo problemas svarstyti elektroninių duomenų kaip atskiros įrodymų rūšies civiliniame procese numatymas, atliekant atitinkamus pakeitimus civilinio proceso įstatymuose.

LITERATŪRA

1. **D'Laarni A. Ortiz**, *Where does the PC go from here?* // *BusinessWorld*, (Dec. 12, 2001).
2. **Weinstein E.** *Help Im Drowning in E-Mail!* // *The Wall Street Journal* (Jan. 10 2002)
3. *CyberAtlas, Top Online Properties of January 2002* (Feb. 8, 2002).
4. **Johnston Gretel.** *You've Got Mail!* // *International Data Corporation, News Service*, (Sept. 26, 2002).
5. **Lietuvos Respublikos** mokėjimų įstatymas // *Valstybės žinios*. 1999. Nr. 97-2775.
6. **Lietuvos** Vyriausiojo Administracinio Teismo byla Nr. 3K-3-35/2003 m. *UAB „Bitė GSM“ prieš AB „Lietuvos telekomą“*.
7. **Lietuvos Aukščiausiojo Teismo** byla Nr. 3K-3-35/2003 m. *AB „Lietuvos telekomas“ prieš Ž. Budros IĮ „Sėkmės vėjas“*.
8. **Bantin P. C.** (2001). *Indiana University electronic records project: lessons learned* // *Information Management Journal*. Vol 35, No 1.
9. **Council of Europe.** Recommendation No. R (81) 20 on the harmonisation of laws relating to the requirement or written proof and to the admissibility of reproductions of documents and recordings on computers.
10. **United Nations Commission on International Trade Law (UNCITRAL).** Recommendation on the Legal Value of Computer Records (1985). // <http://www.uncitral.org/english/texts/electcom/computerrecords.htm>
11. **United Nations Commission on International Trade Law (UNCITRAL)** Model law on electronic commerce // *United Nations General Assembly A/RES/21/162*. 1997-01-30
12. **UNCITRAL** Model Law on Electronic Commerce with Guide to Enactment // *UNITED NATIONS PUBLICATION Sales No. E.99.V.4 ISBN 92-1-133607-4*
13. **Lietuvos Respublikos** civilinio proceso kodeksas // *Valstybės žinios*. 2002. Nr. IX-743.
14. **Lietuvos Aukščiausiojo Teismo** 2000 m. gegužės 29 d. nutartis civilinėje byloje Nr. 3K-3-619/2000.
15. **Lietuvos Respublikos** civilis kodeksas // *Valstybės žinios*. 2000. Nr.VIII-1864.
16. **Laužikas E., Mikelėnas V., Nekrošius V.** *Civilinio proceso teisė*. I tomas. – Vilnius: Justitia, 2003.
17. **Rules** on electronic evidence of Supreme Court of the United States 2001.
18. **Betts M.** *Businesses worry about long-term data losses* // *Computerworld*, Vol. 33, No 38, pp. 22–40.
19. **Stephens D. O.** (2000a). *Digital preservation: a global information management problem* // *Information management journal* Vol 34. No. 19 pp. 8-26.
20. **Stephens D. O.** (2000b) *Digital preservation in the United Kingdom* // *Information management journal*, Vol 34, No. 4, pp. 68–71.
21. **Lawrence H. A.** *New perspectives on preserving documents* // *National Underwriter* Vol 105, No. 5, pp. 3–5.
22. **Lietuvos Respublikos** civilinio proceso kodeksas // *Valstybės žinios*. 2002. Nr. IX-743.
23. **Lietuvos Respublikos** civilis kodeksas // *Valstybės žinios*. 2000. Nr.VIII-1864.
24. **Wu R.** *Electronic Transactions Ordinance – Building a Legal Framework for E-commerce in Hong Kong*. 2000 (1) *The Journal of Information, Law and Technology (JILT)*.
25. **Bohm et al.** *Electronic Commerce: Who Carries the Risk of Fraud?* 2000 (3) *The Journal of Information, Law and Technology (JILT)*.
26. **Deturbide M.** *Liability of Internet Service Providers for Defamation in the US and Britain: Same Competing Interests, Different Responses*, 2000 (3) *The Journal of Information, Law and Technology (JILT)*.
27. **Howard D. I.** *The law of evidence* / by I. H. Dennis. 2nd ed. – London: Sweet & Maxwell, 2002. - LVI, 757 S. - 0-421-74200-3.
28. **Taylor P.** *The Scope of Government Access to Copies of Electronic Communications Stored with Internet Service Providers: A Review of Legal Standards* // *Journal of Technology Law and Policy* / FALL 2001 Volume 6, Issue 2.

29. **Heidi Pearlman Salow.** Liability Immunity for Internet Service Providers – How Is It Working? // Journal of Technology Law and Policy / FALL 2001 Volume 6, Issue 1.
30. Federal Trade Commission “Privacy Online: Fair Information Practices in the Electronic Marketplace” // A Federal Trade Commission Report to Congress, Canada No.1, May 2000.

ASPECTS OF USING ELECTRONIC EVIDENCE IN CIVIL PROCEEDINGS

Rytis Čėsna *

Mykolas Romeris University

S u m m a r y

New technologies empowered us not only to communicate faster and better, but also to create new business branches. Every day millions of digital messages and documents are sent through the global network or telecommunication systems. Some business processes, service provisioning and conclusion of contracts can be accomplished and all evidence can be accessed only in electronic environment (in cyberspace). When some facts or events can be evidentially fulfilled by electronic information only it is important to ensure acceptability of such information

in legal procedures. Everyone wants to be sure that in the case when some disputes regarding his interest violation arise, he would be able to defend himself using electronic data or electronic documents, made for or during the relationships with other parties. Unfortunately the litigation of these processes is not so clear as it should be. Internet as a global communication and information environment has very many problems regarding its internationality, anonymity and insecurity. The information can be accessed from everywhere and can be displayed everywhere. Thus we must have the possibility to use this information in the court to prove what has happened or should have happened.

It is clear that our country eventually will begin to use electronic evidences very widely because the computerization processes are very fast. The position of EU and Lithuanian Government on implementation of electronic communications like e-government, electronic studies, medicine and other forms of electronic relationships provide background for treating electronic evidences as equal to common evidences.

Keywords: electronic data, electronic evidence, electronic commerce, digital signature.

* Mykolas Romeris University, Faculty of Economic and finance, lecturer of the Department of informatics and statistics.