https://doi.org/10.25143/socr.16.2020.1.087-099

Personas elektroniskās identifikācijas tiesiskā regulējuma problemātika

Dace Mote

ORCID: 0000-0002-1145-4951

Rīgas Stradiņa universitāte, Juridiskā fakultāte, Latvija
dace.mote@gmail.com

Kopsavilkums

Attīstoties informācijas tehnoloģijām un digitālajiem risinājumiem, pieaug iedzīvotāju vēlme saņemt pakalpojumus elektroniski – vai tie būtu sadzīviska rakstura pakalpojumi vai valsts un pašvaldības iestāžu piedāvātie elektroniskie pakalpojumi. Lai persona varētu saņemt attālinātus iestāžu pakalpojumus, tai ir nepieciešams elektroniski identificēties. Personas veiksmīgas elektroniskās identifikācijas būtiskākās komponentes ir abu pušu saistību izpilde personas datu drošības jautājumos un pakalpojumu sniedzēja spēja tehniski nodrošināt personas elektronisko identifikāciju.

Rakstā tiek apskatīti elektroniskās identifikācijas veidi, to raksturojums un tiesiskie aspekti, izvērtējot tiesisko regulējumu, pieejamo literatūru un aktuālo tiesu praksi elektroniskās identificēšanas jautājumos. Raksts ir balstīts uz autores izstrādāto maģistra darbu, kurā tika pētīti personas elektroniskās identifikācijas riski un tiesiskā regulējuma problemātika.

Atslēgvārdi: personas elektroniskā identifikācija, digitālā drošība, personas identifikācija, eIDAS.

Ievads

Cilvēka ikdiena vairs nav iedomāja bez interneta, tehnoloģijām, digitālajiem un mākslīgā intelekta risinājumiem, kas to atvieglo. Pirms pāris gadu desmitiem savu uzvaras un attīstības gājienu sāka internets, bez kura vairs neiztikt ne tikai personiskas lietošanas nolūkos, bet arī darba vidē. Arvien vairāk darbu cilvēka vietā veic rūpīgi izstrādātas tehnoloģijas, manuālais darbs tiek nomainīts ar digitālajiem un mākslīgā intelekta risinājumiem. Šis ir digitālais laikmets, kurā aug nepieciešamība pēc digitāliem risinājumiem un dažādām inovācijām tehnoloģiju jomā.

Ir gan novērots, ka cilvēka dabā ir katru jauno risinājumu vispirms kritizēt un neatzīt par lietošanai derīgu, taču pēc kāda laika tas kļūst pierasts, bez tā nevar iztikt. Piemēram, tā bija, kad bankas sāka piedāvāt klientiem iespēju lietot to pakalpojumus attālināti, izmantojot internetbanku, nevis ierodoties saņemt pakalpojumus klātienē bankas filiālē.

Latvijā personas identitātes apliecināšana e-vidē sāka veidoties pirms apmēram 20 gadiem. Dažādos pakalpojumu sniedzēju portālos cilvēki varēja reģistrēties, izmantojot speciāli vietnes apmeklējumam radītu lietotājvārdu un paroli. Finanšu sektoram attīstoties, arvien plašāk dažādu nozaru tīmekļa vietnēs tika integrēta iespēja apliecināt maksājumus ar tā sauktajiem internetbankas rīkiem, un rezultātā internetbankas sāka plaši lietot autentifikācijai [11].

Atšķirībā no privātajiem biznesa modeļiem, kuros persona var autorizēties ar e-pasta vai lietotājvārda un paroles palīdzību, kas ir visvienkāršākais personas identifikācijas veids, valsts un pašvaldību iestādēm ir jānodrošina augstāks personas identifikācijas standarts, ja persona vēlas saņemt pakalpojumu. Tas nepieciešams, lai nodrošinātu pakalpojuma pieejamību tādā pašā apjomā kā klātienē saņemamo. Turklāt, sniedzot attālināto pakalpojumu, ir jābūt pārliecībai, ka pakalpojumu saņem tiešām tā persona, kura tiek identificēta, nevis kāds cits ir autorizējies un vēlas saņem pakalpojumu autorizētās personas vietā.

Šā pētījuma mērķis bija izpētīt fizisko personu elektroniskās identifikācijas tiesisko regulējumu, konstatēt problēmas un riskus personas elektroniskās identifikācijas procesā, ieteikt tiesiskā regulējuma pilnveidošanas un uzlabošanas iespējas, lai mazinātu personas kļūdainas identifikācijas risku un novērstu personas elektronisku identificēšanu pret pašas gribu, kā arī nodrošinātu personai tiesisko paļāvību, ka elektroniskās identifikācijas pakalpojuma sniedzējs atbilst tiesiskajā regulējumā noteiktajām prasībām. Pamatojoties uz veikto pētījumu, mērķis bija izstrādāt secinājumus un sniegt priekšlikumus.

Pētījuma gaitā tika izmantotas vispārzinātniskās pētījuma metodes – aprakstošā, salīdzinošā, sistēmiskā un analītiskā. Tāpat tika lietotas arī tiesību normu interpretācijas metodes – gramatiskā (filoloģiskā) interpretācijas metode, vēsturiskā, sistēmiskā un teoloģiskā (jēgas un mērķa) interpretācijas metode.

Elektroniskās identifikācijas tiesiskais regulējums

Uz interneta vidi, tāpat kā tas ir reālajā dzīvē, tiek attiecināts Latvijas Republikas Satversmes 96. pants, kurā noteikts, ka ikvienam ir tiesības uz privātās dzīves, mājokļa un korespondences neaizskaramību [8]. Satversmes pants ir spēkā arī interneta vidē – nevienam nav tiesības piekļūt personas datiem, kas tiek glabāti personas datorā vai sociālajos kontos, kā arī nedrīkst ar personas datiem interneta vidē veikt prettiesiskas darbības. Satversmes 96. panta pārkāpums ir arī e-pasta korespondences "uzlaušana", neatļauta publiskošana, privātu fotogrāfiju publiskošana (droši vien pēc 10–15 gadiem šis jautājums būs aktuāls, jo būs izauguši tie zīdaiņi un bērni, kuru attēli šobrīd aktīvi tiek publicēti interneta vietnēs, un, bērniem pieaugot, aktualizēsies tiesību aizskāruma jautājumi).

Satversmes 96. pants nav vienīgais, kurā noteikta personas privātās dzīves neaizskaramība, tas ir noteikts arī starptautiskajos dokumentos:

- ANO Vispārējās cilvēktiesību deklarācijas 12. pantā – nedrīkst patvaļīgi pārkāpt neviena cilvēka privātās dzīves, ģimenes, mājokļa un korespondences neaizskaramību, ne arī apdraudēt viņa godu un reputāciju. Katram cilvēkam ir tiesības uz likuma aizsardzību pret šādiem pārkāpumiem vai apdraudējumiem [10];
- Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijas 8. pantā – ikvienam ir tiesības uz savas privātās un ģimenes dzīves, dzīvokļa un korespondences neaizskaramību. Sabiedriskās institūcijas nedrīkst traucēt nevienam izmantot šīs tiesības, izņemot gadījumos, kas paredzēti likumā un ir nepieciešami demokrātiskā sabiedrībā, lai aizstāvētu valsts drošības, sabiedriskās kārtības vai valsts labklājības intereses, lai nepieļautu nekārtības vai noziegumus, lai aizsargātu veselību vai morāli vai lai aizstāvētu citu tiesības un brīvības [1];
- Eiropas Savienības pamattiesību hartas 7. pantā – ikvienai personai ir tiesības uz savas privātās un ģimenes dzīves, dzīvokļa un saziņas neaizskaramību [4].

Latvijas tiesiskajā regulējumā personas elektroniskā identificēšana un ar to saistītie jautājumi ir noteikti vairākos likumos un Ministru kabineta noteikumos.

Personu apliecinošu dokumentu likums

Lai persona būtu elektroniski identificējama tādā pašā veidā kā klātienē, nepieciešams regulējums, kurā definēts, kāda var būt elektroniskā personas identifikācija un kādi kritēriji ir jāizpilda, lai tā varētu notikt. Latvijā personu apliecinoši dokumenti ir pase un personas apliecība, savukārt personas elektroniskai identifikācijai jāizmanto informācija, kas iekļauta elektroniskā formā personas apliecībā – tas noteikts Personu apliecinošu dokumentu likuma 5. panta piektajā daļā [9]. Personas apliecībā iekļautajā elektroniskajā identifikācijas kartē (eID) kā identifikācijas veids tiek izmantots eID iekļautais identifikācijas sertifikāts. eID karte nodrošina vizuālo personas identifikāciju un autentifikāciju arī elektroniskajā vidē, turklāt efektīvāk tā ir izmantojama elektroniskajā vidē, lai saņemtu e-pakalpojumus un lietotu tajā iekļauto e-parakstu saskarsmē ar valsts un pašvaldību institūcijām. Šobrīd šis ir viens no drošākajiem identifikācijas veidiem elektroniskā vidē.

Kredītiestāžu identifikācijas veids tehnoloģiski ir balstīts uz internetbanku nodrošināto identifikācijas mehānismu, kuru, savietojot ar iestāžu informācijas sistēmām, iespējams izmantot lietotāju atpazīšanai un piekļuvei iestāžu pakalpojumiem un informācijai [13]. Identitāte vēl var tikt apliecināta, izmantojot likumā noteikto kredītiestādes elektronisko norēķinu sistēmas autentifikācijas līdzekli, t. i., *SmartID* vai autorizēšanos internetbankā ar kodu kalkulatoru.

Saeima ir pieņēmusi likumprojektu par grozījumiem Personu apliecinošu dokumentu likumā, kuros paredzēts, ka no 2023. gada eID karte būs obligāts personu apliecinošs dokuments [16]. Tā kā likumprojektā galvenokārt paredzēta eID noteikšana par obligātu personu apliecinošu dokumentu, tam jāseko citu saistīto likumu grozīšana, piemēram, jānoteic, ka eID ir oficiāls elektroniskās identifikācijas rīks Saeimas vēlēšanās un par personas balss atdošanu tiks veikta elektroniska atzīme, ka tiks paredzēta pakalpojumu nodrošināšana, izmantojot elektronisko identifikāciju citu ES dalībvalstu pilsoņiem, kuriem būs attiecīgās dalībvalsts eID.

Ņemot vērā, ka šāda personu identifikācija tiek balstīta tikai uz vienošanās pamata, banku izmantotajiem līdzekļiem publisko pakalpojumu sniegšanas jomā netiek izvirzītas un kontrolētas drošības prasības ne konkrētam tehniskajam risinājumam, ne arī procedūrām, kādā veidā attiecīgie identifikācijas rīki tiek izsniegti personām. Turklāt valsts institūcijas nevar garantēt šādas vienošanās un banku iniciatīvas, un piekrišanas ilglaicīgu darbību, līdz ar to arī elektronisko pakalpojumu nepārtrauktu pieejamību, izmantojot banku izsniegtos identifikācijas līdzekļus. Banku piedāvātie identifikācijas rīki ir paredzēti izmantošanai konkrētas informācijas sistēmas (internetbankas) ietvaros. Tāpēc attiecīgo identifikācijas rīku izmantošana ārpus konkrētās bankas sistēmas būtiski palielina iespējamo drošības risku līmeni, bet bankai nav iespēju un pienākuma veikt drošības risku pārvaldību ārpus savā pārziņā esošās informācijas sistēmas. Izvēloties un izmantojot banku identifikācijas rīkus publisko elektronisko pakalpojumu saņemšanai, personai tiek uzlikts par pienākumu pašai izvērtēt iespējamo pušu atbildību gadījumā, ja iestājies incidents, kas radījis nelabvēlīgas sekas vai jebkāda veida kaitējumu attiecīgajai personai [18]. Vienlaikus, lai arī ir uzsvērts, ka kredītiestāžu nodrošinātie identifikācijas līdzekļi nav uzskatāmi par drošiem un, tos izmantojot, pastāv vairāki drošības riski, saskaņā ar likumprojekta anotāciju tie tik un tā paliks kā alternatīva personas elektroniskai identifikācijai – nosakot eID karti par obligātu personu apliecinošu dokumentu, netiek aizliegti vai ierobežoti citi autentifikācijas un identifikācijas rīki, to skaitā banku identifikācijas rīki. Tādējādi tiek noteikta viena valsts garantēta identifikācijas rīka pieejamība neatkarīgi no citu identifikācijas pakalpojumu sniedzēju piedāvātiem alternatīviem identifikācijas rīku pakalpojumiem, kuru izmantošanu paredz gan Regula (ES) Nr. 910/2014, gan Fizisko personu elektroniskās identifikācijas likums. Likumdevēja nostāja ir šāda: dažādu elektronisko identifikācijas līdzekļu pieejamība nodrošina konkurenci digitālajā vidē un garantē pakalpojumu pieejamību lielākai iedzīvotāju daļai, tajā pašā laikā uzņemoties lielākus drošības riskus. Likumprojektā paredzēta arī Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93 EK (turpmāk – eIDAS) normu ieviešana, nodrošinot, ka persona varēs tikt elektroniski identificēta arī ar citu ES valstu personas apliecībām, kas satur eID datus.

Fizisko personu elektroniskās identifikācijas likums

Personas elektronisko identifikāciju Latvijā regulē Fizisko personu elektroniskās identifikācijas likums. Šā likuma ieviešana bija nepieciešama, lai būtu vienots tiesiskais regulējums, ar kuru noteikt dažādu elektroniskajā vidē pieejamo un lietojamo elektroniskās identifikācijas līdzekļu izmantošanu. Pirms šis likums stājās spēkā pastāvēja sadrumstalota elektroniskās identifikācijas sistēma, kas būtībā bija katra elektroniskā pakalpojuma sniedzēja ziņā, t. i., pakalpojuma sniedzējs noteica, kas jāievēro, lai nodrošinātu piekļuvi tā sniegtajiem elektroniskajiem pakalpojumiem, kāda ir pušu atbildība un pienākumi. Piemēram, Valsts ieņēmumu dienesta elektroniskās deklarēšanās sistēmu varēja lietot pēc tam, kad bija noslēgts rakstisks līgums ar iestādi un saņemts lietotājvārds un parole, lai persona varētu izmantot iestādes elektroniskos pakalpojumus.

Fizisko personu elektroniskās identifikācijas likuma mērķis ir noteikt elektroniskās identifikācijas prasības, lai fiziskai personai nodrošinātu iespēju pieprasīt vai saņemt elektronisko pakalpojumu, ko publiska persona sniedz, pildot tai noteiktās funkcijas vai uzdevumus, kā arī noteikt elektroniskās identifikācijas pakalpojuma sniedzējiem reģistrācijas un uzraudzības kārtību un prasības elektroniskās identifikācijas veidiem, lai tie būtu pielīdzināmi personas identitātes pārbaudei klātienē, uzrādot personu apliecinošu dokumentu [6]. Likuma 3. panta trešajā daļā noteikts, ka elektroniskā identifikācija ir uzskatāma par notikušu un ir pielīdzināma personas identitātes pārbaudei klātienē, uzrādot personu apliecinošu dokumentu, vienā no šiem gadījumiem:

- ja tā veikta ar kvalificētu vai kvalificētu paaugstinātas drošības elektroniskās identifikācijas līdzekli un atbilst šā likuma prasībām – šim identifikācijas veidam atbilst tikai VAS "Latvijas Valsts radio un televīzijas centrs" sniegtie elektroniskās identifikācijas pakalpojumi: eID karte, e-paraksts karte, e-paraksts karte+, e-paraksts un e-paraksts *mobile*;
- ja elektroniskās identifikācijas pakalpojuma sniedzējs un elektroniskā pakalpojuma sniedzējs rakstveidā vienojušies par elektronisko identifikāciju un tās veidu, neizmantojot kvalificētu vai kvalificētu paaugstinātas drošības elektronisko identifikāciju – personas elektroniskā identifikācija ar *SmartID* un internetbanku, par kuru izmantošanu kā autorizācijas līdzekli persona ir vienojusies ar kredītiestādi – piekrišana *SmartID* lietošanai tiek dota, lejupielādējot lietotni un atzīmējot, ka persona piekrīt tās lietošanas noteikumiem, savukārt autorizācijai ar internetbanku tās lietotājs sniedz rakstisku piekrišanu klātienē, parakstot līgumu par internetbankas lietošanu;
- ja elektroniskā pakalpojuma sniedzējs un fiziskā persona rakstveidā vienojušies par fiziskās personas identitātes pārbaudi elektroniskajā vidē, neizmantojot kvalificētu vai kvalificētu paaugstinātas drošības elektronisko identifikāciju – identificēšanai kalpo lietotājvārdi un paroles – šāda kārtība ir EDS sistēmā, Ceļu satiksmes drošības direkcijas informācijas sistēmā u. c. Personai tiek piedāvāta arī elektroniskā identifikācija, lietojot vietni *Latvija.lv*, tā aizstājot lietotājvārda un paroles nepieciešamību.

Kvalificētus vai kvalificētus paaugstinātas drošības elektroniskās identifikācijas pakalpojuma sniedzējus uzrauga un reģistrē Digitālās drošības uzraudzības komiteja, kura ir koleģiāla uzraudzības institūcija aizsardzības ministra pakļautībā. Tā izveidota, pamatojoties uz Ministru kabineta noteikumiem Nr. 695 "Digitālās drošības uzraudzības komitejas nolikums", kuri izdoti saskaņā ar Fizisko personu elektroniskās identifikācijas likumu un Informācijas tehnoloģiju drošības likumu. Komiteja veic Fizisko personu elektroniskās identifikācijas likumā noteiktās uzraudzības institūcijas funkcijas un uzdevumus, kā arī informē Eiropas Komisiju par elektroniskās identifikācijas shēmām, sagatavo priekšlikumus normatīvo aktu projektiem par kvalificētu vai kvalificētu paaugstinātas drošības elektroniskās identifikācijas pakalpojumu sniedzēju un tā sniegto pakalpojumu uzraudzību, kā arī savas kompetences ietvaros sagatavo priekšlikumus valsts un pašvaldības iestādēm [12]. Komitejas mērķis ir uzraudzīt un reģistrēt kvalificētus un kvalificētus paaugstinātas drošības elektroniskās identifikācijas pakalpojuma sniedzējus un to pakalpojumus kvalificētu elektroniskās identifikācijas pakalpojumu sniedzēju reģistrā, uzraudzīt un apstiprināt uzticamus sertifikācijas pakalpojumu sniedzējus un to pakalpojumus, kā arī izveidot, uzturēt un publicēt uzticamības sarakstus, pārbaudīt un sertificēt parakstu vākšanas tiešsaistes sistēmas atbilstību drošības un tehniskajiem parametriem un uzraudzīt pamatpakalpojuma un digitālā pakalpojuma sniedzējus [2].

Publiski iepazīties ar uzticamu sertifikācijas pakalpojumu sniedzēju sarakstu nav viegli, jo Aizsardzības ministrijas mājaslapā tiek piedāvātas datnes tikai *.xml* un *.sha2* formātā, kas parasti netiek lietots, ērtāks būtu *.pdf* formāts. Savukārt Datu valsts inspekcijas mājaslapā Latvijā akreditētu uzticamu sertifikācijas pakalpojumu sniedzēju reģistrā norādīts tikai VAS "Latvijas Valsts radio un televīzijas centrs", kas ir arī vienīgais kvalificētu un kvalificētu paaugstinātas drošības elektroniskās identifikācijas pakalpojumu sniedzējs.

Informācijas tehnoloģiju drošības likums

Saskaņā ar Informācijas tehnoloģiju drošības likuma 4. pantu uzraudzību interneta vidē veic arī Informācijas tehnoloģiju drošības incidentu novēršanas institūcija jeb *CERT.LV,* kuras uzdevums ir veicināt informācijas tehnoloģiju drošību Latvijā. *CERT.LV* ir Latvijas Universitātes Matemātikas un informātikas institūta struktūrvienība, kas darbojas Latvijas Republikas Aizsardzības ministrijas pakļautībā atbilstīgi Informācijas tehnoloģiju drošības likumam. Galvenie *CERT.LV* uzdevumi ir uzturēt un aktualizēt informāciju par informācijas tehnoloģiju (IT) drošības apdraudējumiem, sniegt atbalstu valsts institūcijām IT drošības jomā, sniegt atbalstu IT drošības incidentu novēršanā jebkurai fiziskai vai juridiskai personai, ja incidentā iesaistīta Latvijas IP adrese vai *.LV* domēns, organizēt informatīvus un izglītojošus pasākumus gan valsts iestāžu darbiniekiem, gan IT drošības profesionāļiem, gan citiem interesentiem [17].

Par informācijas tehnoloģiju drošības incidentu novēršanu Aizsardzības ministrijas un tās padotībā esošajās iestādēs un Nacionālajos bruņotajos spēkos atbildīgs ir Militārās izlūkošanas un drošības dienests.

Informācijas tehnoloģiju drošības likuma mērķis ir uzlabot informācijas tehnoloģiju drošību, nosakot svarīgākās prasības, lai garantētu tādu būtisku pakalpojumu saņemšanu, kuru sniegšanai tiek izmantotas šīs tehnoloģijas [7]. Likumā ir noteiktas IT drošības normas, kas pakalpojumu sniedzējiem jāievēro, apstrādājot elektroniskos datus un garantējot datu drošību, kā arī tajā paredzēts IT kritiskās infrastruktūras tiesiskais regulējums.

Informācijas tehnoloģiju drošības incidents ietekmē konfidencialitāti, ja incidenta rezultātā dati kļūst pieejami neautorizētām personām. Vispārīgā gadījumā konfidencialitāte ir ietekmēta arī tad, ja dati ir pazaudēti vai organizācija vai persona ir zaudējusi kontroli pār tiem. Piemēram, ja informācijas sistēmai piekļūst persona, izmantojot cita sistēmas lietotāja paroli vai citus autorizācijas rīkus [18, *22–23*]. Informācijas tehnoloģiju drošības incidenti var ietekmēt arī elektroniskās identifikācijas veikšanu – persona var tikt nepareizi identificēta vai arī personas vietā var tikt identificēts kāds cits, var tikt "uzlauzta" informācijas sistēmas datubāze, tādējādi trešās personas var uzzināti personas datus. Drošības incidents var notikt arī gadījumā, ja kļūst pieejami personas uzglabātie datiem vai dati par personu, kas var tikt izmantoti pret šo vai citām personām. Likumdevējs ir būtiski novērtējis informācijas tehnoloģiju drošības riskus, un līdz ar likuma subjektu loka paplašināšanu likumdevējs ir noteicis visiem – ar informācijas tehnoloģiju saistītajām iestādēm un uzņēmumiem – pienākumu ievērot IT drošības prasības, gādājot par personu aizsardzību pret nesankcionētu datu izmantošanu, neatbilstošu uzglabāšanu vai arī personu kļūdainu identifikāciju.

Elektronisko dokumentu likums

Elektronisko dokumentu aprite un elektroniskā paraksta tiesību normas noteiktas Elektronisko dokumentu likumā. Šajā likumā noteikts elektroniskā dokumenta un elektroniskā paraksta tiesiskais statuss un noteikumi tā izpildei, likumā ietvertie noteikumi attiecināmi ne tikai uz elektronisko dokumentu apriti starp valsts un pašvaldību iestādēm, bet tie ir piemērojami arī citām publiskām personām un to iestādēm, tiesām, tiesu sistēmai piederīgajām personām un iestādēm, kā arī sabiedrisko pakalpojumu sniedzējiem likuma "Par sabiedrisko pakalpojumu regulatoriem" izpratnē [5]. Elektronisko dokumentu likumā ir iestrādātas eIDAS regulas prasības, nosakot vienotu regulējumu ES dalībvalstīs un aizstājot sadrumstalotību elektronisko dokumentu un e-paraksta identifikācijā starp ES dalībvalstīm. Elektroniskais dokuments pielīdzināms pašrocīgi parakstītam dokumentam, ja tam ir drošs elektroniskais paraksts. Drošs elektroniskais paraksts ir gan e-paraksts, kuru nodrošina VAS "Latvijas Valsts radio un televīzijas centrs", gan *SmartID* piedāvātais elektroniskais paraksts, kas arī ir kvalificēts elektronisks paraksts un satur drošības sertifikātus, kuri tiek atzīti visā ES, bet šeit saskatāma arī problēma – kaut arī *SmartID* tiek pozicionēts kā drošs elektroniskais paraksts ar

kvalifikācijas sertifikātiem, tomēr *SmartID* izstrādātājs un pakalpojumu sniedzējs nav norādīts nevienā reģistrā – ne kvalificēto pakalpojumu sniedzēju reģistrā, ne arī uzticamības pakalpojumu sniedzēju reģistrā. Saskaņā ar Elektronisko dokumentu likumu drošs elektroniskais paraksts tiek pielīdzināts personas pašrocīgam parakstam. Attiecībā uz personas identitātes noskaidrošanu drošs elektroniskais paraksts ir personu apliecinoša dokumenta izpausme elektroniskā vidē. Identitātes piederība e-parakstam ir pārbaudīta uz droša elektroniskā paraksta piešķiršanas brīdi, klātienē pārbaudot personu apliecinošu dokumentu, jo elektroniskajā vidē tas ir sasaistīts ar personas apliecību. Darījumus starp klāt neesošām pusēm būtu drošāk slēgt ar drošu elektronisko parakstu, jo e-paraksts nodrošina iespēju pārliecināties par parakstītāja identitāti lielākā mērā nekā pastā atsūtīts pašrocīgi parakstīts dokuments [14, *19*], kas varētu būt arī kvalitatīvs viltojums. Ja tiek izmantots drošs elektroniskais paraksts, to ir iespējams pārbaudīt interneta vietnē *eparaksts.lv* – augšupielādējot dokumentu, tiek parādīts dokumenta elektroniskais parakstītājs, parakstīšanas vieta un laika zīmogs.

Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014

Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93 EK mērķis ir stiprināt elektronisko darījumu uzticamību iekšējā tirgū, nodrošinot vienotu pamatu drošai elektroniskai mijiedarbībai starp iedzīvotājiem, uzņēmumiem un publiskām iestādēm, tādējādi palielinot publisko un privāto tiešsaistes pakalpojumu, elektroniskās darījumdarbības un elektroniskās komercijas efektivitāti Savienībā [3]. Būtībā eIDAS regula ir iedalāma divās daļās [15]. Pirmajā daļā aplūkotas valdības atzītas elektroniskās identifikācijas sistēmas un izveidots tiesiskais regulējums, kas ļauj visām ES dalībvalstīm savstarpēji atzīt citai citas identifikācijas sistēmas. Šī daļa attiecas uz publisko sektoru un ir vērsta uz to, lai dalībvalstis ļautu citu dalībvalstu pilsoņiem izmantot savus elektroniskos identifikācijas līdzekļus piekļuvei jebkuras dalībvalsts tiešsaistes pakalpojumiem. eIDAS neietekmē privātā sektora darbību.

eIDAS otrajā daļā aplūkoti elektroniskie paraksti – tajā ir ne vien precizēti spēkā esošie noteikumi, bet arī ieviests jauns tiesiskais regulējums elektroniskajiem parakstiem un zīmogiem, kurus dalībvalstis var integrēt savas valsts tiesiskajā regulējumā. eIDAS piedāvā vienotu normatīvo bāzi visām dalībvalstīm, lai nodrošinātu vienotu piekļuvi elektroniskajiem pakalpojumiem ar elektroniskajiem identifikatoriem.

eIDAS regulas 8. pantā noteikts, ka identitātes apliecināšanu var iedalīt trīs uzticamības līmeņos – zemā, būtiskā un augstā:

- zems uzticamības līmenis – attiecas uz elektroniskās identifikācijas līdzekļiem saistībā ar elektroniskās identifikācijas shēmu, kas sniedz ierobežotu ticamības pakāpi attiecībā uz personas apgalvotu vai paustu identitāti, un to raksturo

atsauce uz tehniskajām specifikācijām, standartiem un procedūrām, kas ar to ir saistītas, tostarp uz tehnisko kontroli, kā mērķis ir mazināt identitātes nepareizas izmantošanas vai izmainīšanas risku, t. i., pakalpojumu sniedzēju piedāvātie elektroniskie pakalpojumi, kuru vietnēs persona pati var norādīt savu identitāti un izveidot savu lietotājvārdu un paroli. Zemākajā uzticamības līmenī atrodas internetveikali, koppasūtījumu vietnes, sadzīves pakalpojumu vietnes un sociālie tīkli;

- būtisks uzticamības līmenis – attiecas uz elektroniskās identifikācijas līdzekļiem saistībā ar elektroniskās identifikācijas shēmu, kas sniedz būtisku ticamības pakāpi attiecībā uz personas apgalvotu vai paustu identitāti, un to raksturo atsauce uz tehniskajām specifikācijām, standartiem un procedūrām, kas ar to ir saistītas, tostarp tehnisko kontroli, kā mērķis ir būtiski mazināt identitātes nepareizas izmantošanas vai izmainīšanas risku. Būtiska uzticamības līmeņa identifikācijas līdzekļi ir kredītiestāžu piedāvātie identifikācijas rīki – personas elektroniskā identifikācija ar *SmartID* un autorizācija ar internetbanku;
- augstākais uzticamības līmenis – attiecas uz elektroniskās identifikācijas līdzekļiem saistībā ar elektroniskās identifikācijas shēmu, kas sniedz augstāku ticamības pakāpi attiecībā uz personas apgalvotu vai paustu identitāti nekā būtiskā uzticamības līmenī, un to raksturo atsauce uz tehniskajām specifikācijām, standartiem un procedūrām, kas ir saistītas ar to, tostarp tehnisko kontroli, kā mērķis ir novērst identitātes nepareizu izmantošanu vai izmainīšanu. Šeit uzsvars būtu jāliek uz to, ka augsta uzticamības līmeņa mērķis ir novērst identitātes nepareizu izmantošanu. Augstākā līmeņa pakalpojumiem atbilst eID un e-paraksta izmantošana, kas ir kvalificētu pakalpojumu nodrošināti identifikācijas rīki.

Secinājumi

Fizisko personu elektroniskās identifikācijas likuma 3. panta trešajā daļā noteikts, kāda elektroniskā identifikācija ir uzskatāma par veiksmīgu un ir līdzvērtīga klātienē veiktai personas identifikācijai. Savukārt eIDAS regula elektroniskās identifikācijas veidus un līdzekļus iedala trīs uzticamības līmeņos – zemā, būtiskā un augstā. Diemžēl pašreizējais tiesiskais regulējums nav pietiekošs, jo pēc likumā noteiktajām normām nav iespējams identificēt, kurš personas elektroniskās identifikācijas līdzeklis kuram veidam atbilst, izņemot kvalificētus vai kvalificētus paaugstinātas drošības elektroniskās identifikācijas līdzekļus – t. i., VAS "Latvijas Valsts radio un televīzijas centrs" izstrādātos un kvalificētos elektroniskās identifikācijas līdzekļus – eID un e-parakstu.

Tādējādi Fizisko personu elektroniskās identifikācijas likuma 3. panta trešā daļa būtu papildināma, sasaistot to ar Regulu 910/2014 jeb eIDAS regulu. Papildinātā redakcija būtu jāizteic tādā pašā veidā kā Elektronisko dokumentu likumā – ar norādi un hipersaiti uz Regulas 910/2014 interneta vietni.

Papildinātā elektroniskās identifikācijas definīcija un elektroniskās identifikācijas veidi būtu jāizsaka šādā redakcijā:

> "Elektroniskā identifikācija uzskatāma par notikušu un ir pielīdzināma fiziskas personas identitātes pārbaudei klātienē, uzrādot personu apliecinošu dokumentu, gadījumā, ja tā veikta:
> 1) ar kvalificētu vai kvalificētu paaugstinātas drošības elektroniskās identifikācijas līdzekli, atbilst šā likuma prasībām un Regulas 910/2014 8. panta otrās daļas "c" apakšpunkta augstākā drošības apliecinājuma līmeņa prasībām;
> 2) elektroniskās identifikācijas pakalpojuma sniedzējam un elektroniskā pakalpojuma sniedzējam rakstveidā vienojoties par elektronisko identifikāciju un elektroniskās identifikācijas veidu, neizmantojot kvalificētu vai kvalificētu paaugstinātas drošības elektronisko identifikāciju, un tā atbilst Regulas 910/2014 8. panta otrās daļas "b" apakšpunktā minētajām būtiska drošības apliecinājuma līmeņa prasībām;
> 3) elektroniskā pakalpojuma sniedzējam un fiziskai personai rakstveidā vienojoties par fiziskās personas identitātes pārbaudi elektroniskajā vidē, neizmantojot kvalificētu vai kvalificētu paaugstinātas drošības elektronisko identifikāciju, un tā atbilst Regulas 910/2014 8. panta otrās daļas "a" apakšpunktā minētajām zemākā drošības apliecinājuma līmeņa prasībām."

Līdz ar to augstākajam uzticamības līmenim atbilst eID un e-paraksts jeb kvalificētie identifikācijas līdzekļi, būtiskajam uzticamības līmenim – *SmartID* un kredītiestāžu piedāvātie autorizācijas rīki, savukārt zemākajam uzticamības līmenim – lietotājvārda un paroles izmantošana, ko nodrošina pats pakalpojuma sniedzējs, un šajā gadījumā lielākoties patiesa identitātes norādīšana ir pašas personas interesēs (piemēram, internetveikalā veicot pasūtījumu, persona ir ieinteresēta norādīt pareizu savu identitāti, jo pretējā gadījumā var nesaņemt preci, kuru preces piegādātājs var neizsniegt, ja personas identitāte klātienē nesakritīs ar interneta vietnē norādīto).

Šāda tiesiskā regulējuma papildināšana sniedz plašāku identifikācijas veida skaidrojumu, nodrošinot to ar precizējumu, kuros gadījumos elektronisko identifikāciju var uzskatīt par pielīdzināmu personas identifikācijai klātienē.

Tiesiskajā regulējumā ir noteikta elektroniskā pakalpojuma sniedzēja atbildība un pienākumi, ja pakalpojuma sniedzējs ir kvalificēts vai kvalificēts paaugstinātas drošības pakalpojumu sniedzējs. Valsts un pašvaldību elektroniskos pakalpojumus var saņemt, identificējoties arī ar kredītiestāžu piedāvātajiem elektroniskās identifikācijas līdzekļiem, kas atbilst būtiska drošības apliecinājuma līmeņa elektroniskās identifikācijas līdzekļiem, taču tiesiskajā regulējumā netiek paredzēta atbildība un pienākumi šiem pakalpojumu sniedzējiem.

Tādējādi būtu nepieciešami grozījumi Fizisko personu elektroniskās identifikācijas likuma 19. pantā, to papildinot ar jaunu pirmās daļas 1. punktu, kurā tiktu ietverta pakalpojuma sniedzēja atbildība arī tajos gadījumos, kuros pakalpojuma sniedzējs nepieder kvalificētiem un kvalificētiem paaugstinātas drošības elektroniskās pakalpojumu sniedzējiem, tomēr nodrošina personas elektronisko identifikāciju valsts un pašvaldību pakalpojumu saņemšanai.

Fizisko personu elektroniskās identifikācijas likuma 19. panta pirmās daļas 1. punkts būtu jāizsaka šādā redakcijā:

> "Elektroniskā pakalpojuma sniedzējam, nodrošinot personas elektronisko identifikāciju valsts vai pašvaldību elektronisko pakalpojumu saņemšanai, jāievēro normatīvie akti, kas regulē personas datu aizsardzību un informācijas sistēmu drošību, un jāveic aizsardzības pasākumi, lai novērstu iespējamas prettiesiskas darbības pret autentifikācijas apliecinājumu, kas atrodas pie elektroniskā pakalpojumu sniedzēja."

Papildus jāveic grozījumi arī Fizisko personu elektroniskās identifikācijas likuma 19. panta trešajā daļā, lai noteiktu tehniskās un organizatoriskās prasības tiem elektronisko pakalpojumu sniedzējiem, kas nodrošina personas elektronisko identifikāciju piekļuvei valsts vai pašvaldību elektroniskajiem pakalpojumiem. Jaunā Fizisko personu elektroniskās identifikācijas likuma 19. panta trešās daļas redakcija būtu šāda:

> "Ministru kabinets nosaka tehniskās un organizatoriskās prasības, kas elektroniskā pakalpojuma sniedzējam jāievēro, nodrošinot elektroniskās identifikācijas pakalpojumu valsts vai pašvaldību elektroniskajiem pakalpojumiem vai saņemot kvalificētu vai kvalificētu paaugstinātas drošības elektroniskās identifikācijas pakalpojumu."

Līdz ar izmaiņām tiesiskajā regulējumā arī Ministru kabinetam būtu jāizstrādā jauni noteikumi, kas ietvertu gan tehniskās un organizatoriskās prasības autentifikācijai un elektroniskās identifikācijas līdzeklim, gan elektroniskās identifikācijas līdzekļa darbības izbeigšanas un veicamo drošības pārbaužu veikšanas kārtību.

Tiesiskajā regulējumā ir noteikta pārraugošā iestāde tikai kvalificētiem un kvalificētiem paaugstinātas drošības pakalpojumu sniedzējiem, taču nav paredzēta pārraudzība būtiska drošības apliecinājuma līmeņa elektroniskās identifikācijas pakalpojuma sniedzējiem, piemēram, kredītiestāžu piedāvātājiem elektroniskās identifikācijas līdzekļiem, kurus var izmantot, lai identificētos valsts vai pašvaldību elektronisko pakalpojumu saņemšanai. Lai būtu noteikta Digitālās drošības uzraudzības komitejas pārraudzība elektroniskās identifikācijas pakalpojumu sniedzējiem valsts vai pašvaldību pakalpojumu saņemšanai, nepieciešams veikt grozījumus Ministru kabineta noteikumos Nr. 695 "Digitālās drošības uzraudzības komitejas nolikums". Nepieciešams papildināt šo noteikumu 1. punktu ar piekto apakšpunktu, to izsakot šādi:

> "uzraudzīt elektroniskās identifikācijas pakalpojumu sniedzējus valsts vai pašvaldību elektronisko pakalpojumu saņemšanai".

Person's Electronic Identification Legislation Issues

Abstract

With the development of information technologies and digital solutions, desire of people to receive services electronically increases – whether it is a domestic or an electronic service offered by state or municipal authorities. In order to receive services of

authorities remotely, a person needs to be identified electronically. The most important components of a person's successful electronic identification are the fulfillment of both parties' obligations on personal data security issues and the ability of the service provider to technically secure the person's electronic identification. The Author of the paper has analysed types of person's electronic identification, their characterisation and legal aspects, evaluating legal regulation, available literature and current court practice in electronic identification issues. The article is based on the author's Master's thesis, which explored the risks of electronic identification of a person and the issues of legal regulation.

Keywords: person's electronic identification, digital security, person's identification, eIDAS.

Avoti un literatūra

Tiesību akti

1. Cilvēka tiesību un pamatbrīvību aizsardzības konvencija: starptautisks dokuments. *Latvijas Vēstnesis.143/144 (858/859)*, 13.06.1997.
2. Digitālās drošības uzraudzības komitejas nolikums: Latvijas Republikas Ministru kabineta 04.11.2016. noteikumi Nr. 695. *Latvijas Vēstnesis. 215(5787)*, 03.11.2016.
3. Eiropas Parlamenta un Padomes (ES) Regula Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93 EK: starptautisks dokuments. *Eiropas Savienības Oficiālais Vēstnesis. L257/73*, 28.08. 2014.
4. Eiropas Savienības pamattiesību harta 2016/C 202/02: starptautisks dokuments. *Eiropas Savienības Oficiālais Vēstnesis. C202/389*, 07. 06. 2016.
5. Elektronisko dokumentu likums: Latvijas Republikas likums: pieņemts 31.10.2002. un stājās spēkā 01.01.2003. *Latvijas Vēstnesis. 169(2744)*, 20.11.2002.
6. Fizisko personu elektroniskās identifikācijas likums: Latvijas Republikas likums: pieņemts 05.11.2015. un stājās spēkā 08.12.2015. *Latvijas Vēstnesis. 230(5548)*, 24.11.2015.
7. Informācijas tehnoloģiju drošības likums: Latvijas Republikas likums: pieņemts 28.10.2010. un stājās spēkā 01.02.2011. *Latvijas Vēstnesis. 178(4370)*, 10.11.2010.
8. Latvijas Republikas Satversme: Latvijas valsts likums: pieņemta 15.02.1922. un stājās spēkā 07.11.1922. *Latvijas Vēstnesis. 43*, 01.07.1993.
9. Personu apliecinošu dokumentu likums: Latvijas Republikas likums: pieņemts 12.01.2012. un stājās spēkā 15.02.2012. *Latvijas Vēstnesis. 18(4621)*, 01.02.2012.
10. Universal Declaration of Human Rights: international document: proclaimed on 10 December 1948. *United Nations*. Iegūts no: https://www.un.org/en/universal-declaration-human-rights/

Literatūra

11. Digitālais laikmets: iespējas un izaicinājumi darbam un nodarbinātībai. *Eurofond*. 21.05.2020. Iegūts no: https://www.eurofound.europa.eu/lv/topic/digital-age
12. Digitālās drošības uzraudzības komiteja. *Latvijas Republikas Aizsardzības ministrija*. Iegūts no: https://www.mod.gov.lv/lv/nozares-politika/kiberdrosiba/digitalas-drosibas-uzraudzibas-komiteja

13. Elektroniskā identitāte. *Latvijas Republikas Vides aizsardzības un reģionālās attīstības ministrija.* Iegūts no: http://www.varam.gov.lv/lat/darbibas_veidi/e_parv/Epakalp/?doc=12671
14. Garda, A. 2018. Tiesību un digitālo risinājumu aktualitātes kredītiestāžu skatījumā. *Jurista Vārds. 7(1013),* 19. lpp.
15. Hill, P., Puterbaugh, D. Understanding eIDAS – All you ever wanted to know about the new EU Electronic Signature Regulation. *Legal IT insider.* 01.03.2016. Iegūts no: https://legaltechnology.com/understanding-eidas-all-you-ever-wanted-to-know-about-the-new-eu-electronic-signature-directive/
16. Likumprojekta "Grozījumi Personu apliecinošu dokumentu likumā" sākotnējās ietekmes novērtējuma ziņojums (anotācija). *Latvijas Republikas Ministru kabineta tiesību aktu projekti.* Iegūts no: http://tap.mk.gov.lv/doc/2018_09/VARAMAnot_050618_Groz_PADL.1286.docx
17. Par mums. *CERT.LV.* Iegūts no: https://cert.lv/lv/par-mums
18. Skujiņa, I., Tauriņš, E. 2018. Informācijas tehnoloģiju drošības incidenti: sagatavoties, atpazīt, ziņot, atrisināt. *Jurista Vārds. 1(1007),* 22.–23. lpp.