

КОСТЕНКО О. В.,

головний науковий співробітник

(наукової установи)

*(Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України)***КОСТЕНКО В. В.,**

старший науковий співробітник

(Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України)

УДК 342.9(004.9)

ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ СФЕРИ ЕЛЕКТРОННИХ ПІДПИСІВ У ЗАКОНОДАВСТВІ КРАЇН ЛАТИНСЬКОЇ АМЕРИКИ

У статті проаналізовано законодавчий досвід регулювання правовідносин у сфері електронного підпису та електронних довірчих послуг країн Латинської Америки. Досліджено основні напрями правового застосування електронних підписів та їх сертифікатів. Розглянуто проблематику взаємного визнання електронних довірчих послуг у транскордонному режимі між країнами світу.

Ключові слова: електронний підпис, сертифікат електронного підпису, електронні довірчі послуги, транскордонний режим електронних довірчих послуг, визнання іноземних сертифікатів електронних підписів.

В статье проанализирован законодательный опыт регулирования правоотношений в сфере электронной подписи и электронных доверительных услуг стран Латинской Америки. Исследованы основные направления правового применения электронных подписей и их сертификатов. Рассмотрена проблематика взаимного признания электронных доверительных услуг в трансграничном режиме между странами мира.

Ключевые слова: электронная подпись, сертификат электронной подписи, электронные доверительные услуги, трансграничный режим электронных доверительных услуг, признания иностранных сертификатов электронных подписей.

The article analyzes the legal experience of regulation of legal relations in the area of electronic signature and electronic trust services of Latin American countries. The main directions of legal application of electronic signatures and their certificates are investigated. The problems of mutual recognition of electronic trust services in a cross-border mode between countries of the world are considered.

Key words: electronic signature, electronic signature certificate, electronic trusted services, cross-border electronic trust services, recognition of foreign certificates of electronic signatures.

Вступ. Розвиток світової економіки, процеси глобалізації у всіх сферах життєдіяльності громадян та держав, фактичне рознесення за територіальною ознакою багатьох елементів світового виробництва призводять до прискорення транскордонної торгівлі, в тому



числі і інформацією, як різновиду товару та послуг. Швидкими темпами розбудовуються основи єдиного світового цифрового ринку на основі принципу онлайн довіри, яка тісно пов'язана з надійною цифровою ідентифікацією та автентифікацією. У всьому світі уряди та підприємства для безпечної автентифікації використовують мільйони електронних підписів та електронних довірчих послуг.

За даними компанії Statistics-MRC [1], у 2016 р. світовий ринок електронних підписів становив 662,4 млн доларів США, очікується, що він збільшиться до 3209,4 млн доларів у період до 2029 р. Такі фактори, як збільшення використання електронних підписів із метою зменшення наслідків шахрайства, підвищення надійності та цілісності електронних даних, стимулюють зростання світового цифрового ринку. За даними Statistics-MRC, ключовими виробниками на світовому ринку електронних підписів є компанії Adobe Systems Inc., Ascertia, Microsoft Corporation, Docusign Inc, Entrust Datacard Corp, Gemalto Inc., IdenTrust Inc., International Business Solutions LLC, Kofax Limited, Korea SYSTEM's TECH Inc., Kotrade Inc., Right Signature LLC, Secured Signing Limited, Signix Inc та Oracle Corporation.

Нині розвиток технології електронних підписів та електронних довірчих послуг здебільшого розвивається в напрямі покращення технічних компонентів систем електронних підписів та розширення спектру електронних довірчих послуг із використанням електронного підпису.

Разом із тим співіснування правових систем різних країн із різними базовими дефініціями в сферах електронної торгівлі, електронних послуг та цифрового підпису призводить до суттєвих правових проблем, які пов'язані з використанням електронних довірчих послуг та електронного підпису.

Однією із таких проблем є складність правового регулювання визнання іноземних електронних довірчих послуг та транскордонного визнання сертифікатів електронних підписів у контексті розвитку цифрових транскордонних послуг.

Якнайшвидше урегулювання суспільних відносин, які виникають у процесі використання іноземних довірчих послуг міжнародними та іноземними суб'єктами права, а також встановлення надійного правового регулювання визнання іноземних електронних довірчих послуг та транскордонного визнання сертифікатів електронних підписів нині є актуальною проблемою.

Постановка завдання. Метою статті є порівняння та науковий аналіз базових понять «електронний підпис» та «електронна довірча послуга», підходів визнання транскордонних іноземних довірчих послуг та сертифікатів електронних підписів у законодавстві різних країн світу.

У вітчизняній та закордонній науці міжнародного приватного права наукову думку нині сконцентровано на розвитку технологічних аспектів електронних довірчих послуг. Питаннями правового регулювання суспільних відносин, пов'язаних із технологічною складовою частиною використання електронного підпису, займалися такі вчені: І. Горбенко, О. Потій, Е. Elgar, S. Mason, T.C. Guercio, S. Kinsella, С. Laborde та інші. Водночас питанню правового регулювання визнання іноземних електронних довірчих послуг та транскордонного визнання сертифікатів електронних підписів не приділено необхідної уваги, а дослідження в цьому напрямі практично відсутні.

Результати дослідження. Запровадження і широке використання технологій швидкого обміну електронними даними в різних сферах людської діяльності дало поштовх розвитку нових суспільних відносин у сфері електронної комерції, електронного документообігу та електронного підпису.

Історично вперше, ще у 1984 р., на 17-й сесії Міжнародної торгової палати і Європейської економічної комісії (UNCITRAL) було порушено питання необхідності внесення змін у правові норми країн, маючи за мету створення законних умов використання електронного повідомлення або даних як доказу у суді, а також законодавчого забезпечення однакової юридичної сили за паперовими та електронними документами.

Згодом UNCITRAL розроблено Закон «Про електронну комерцію» («UNCITRAL, Model Law on Electronic Commerce») [2] та Типовий закон ЮНСІТРАЛ «Про електронні підписи» 2001 р. («UNCITRAL Model Law on Electronic Signatures with Guide to Enactment



2001» [3], які стали основною для розвитку законодавства в галузі електронного підпису, електронної комерції та електронних довірчих послуг.

Протягом досить короткого часу більшість країн світу розробила та запровадила законодавчі акти, які регулюють правовідносини під час використання електронних підписів та сервісів. Однак відмінність юрисдикцій, технологічних підходів, технічних стандартів, а в окремих випадках і технологій взагалі, створили проблему юридичного визнання іноземного сертифіката або створеного відповідно до права іншої країни електронного підпису та електронної довірчої послуги [4,5].

Цілком очевидно, що без порівняльного аналізу законодавства, що регулює правовідносини в сфері електронного підпису та електронних довірчих послуг, досить складно дати відповідь на питання, яка потрібна правова процедура визнання іноземних сертифікатів електронного підпису.

Розглянемо на прикладі законодавства країн Латинської Америки та Мексики, як вирішується проблема транскордонного визнання іноземних сертифікатів у різних юрисдикціях з урахуванням досвіду розробки інфраструктури відкритого ключа (PKI) та запровадження національних законів про електронний підпис.

Зазначимо, що географічна відокремленість та національний фактор завжди впливали на формування суспільних відносин з огляду на специфіку регіону. Законодавство в сфері електронного підпису не стало виключенням і має характерні особливості.

Так, Конгресом Колумбії у 1999 р. прийнято Закон № 527 про повідомлення даних, електронну комерцію та цифровий підпис, яким визначається і регулюється доступ, використання і обмін електронними даними, електронна комерція, застосування цифрових підписів, а також встановлюється порядок діяльності органів сертифікації. Законом вводиться дефініція «цифровий підпис», що визначається як «числове значення, що додається до повідомлення математичною процедурою і пов'язане із особистим ключем підписувача, що дає змогу визначити особу підписувача та встановити відсутність змін у даних підписаного документа». Визнання іноземних сертифікатів цифрового підпису виданих іноземними органами сертифікації здійснюються на підставах і згідно з процедурами, які застосовуються до національних органів сертифікації.

Аргентинська Республіка у 2001 р. прийняла «Закон цифрового співробітництва» [7], що запроваджує одночасно дефініції цифрового та електронного підпису. Цифровий підпис є результатом застосування математичної процедури до цифрового документа за наявності інформації про особу підписувача, забезпечення абсолютного контролю з боку підписувача, процедури перевірки третіми сторонами. Електронний підпис визначається як набір інтегрованих або логічно пов'язаних із ними електронних даних, що використовуються як підпис задля їх ідентифікації, які не мають будь-яких юридичних вимог, аналогічних цифровому підпису. Тобто електронний підпис може не містити даних підписувача.

Визнання іноземних сертифікатів цифрового підпису, виданих закордонними сертифікаційними центрами, здійснюється за двома схемами: 1) іноземні сертифікати відповідають умовам, встановленим законом Аргентини та відповідними положеннями щодо сертифікатів, виданих національними сертифікаційними центрами в межах угоди про взаємовизнання між Аргентинською Республікою та країною походження іноземного сертифіката; 2) іноземні сертифікати можуть видаватися іноземним сертифікаційним центром на підставі ліцензії, виданої уповноваженим органом державної влади Аргентинської Республіки – секретаріатом Кабінету Міністрів Республіки.

Федеративна Республіка Бразилія також у 2001 р. прийняла відповідний закон про електронні підписи під назвою «Тимчасовий захід 2.200-2, 24 серпня 2001» [8]. Закон цікавий тим, що вводить поняття «інфраструктура відкритих ключів» і одночасно оминає деталізацію визначення електронного підпису, натомість досить деталізовано регламентує структуру, права і повноваження PKI.

Особливість законодавства Бразилії полягає в тому, що воно дозволяє використовувати лише такі електронні підписи, які створені бразильською інфраструктурою відкритого ключа.



Водночас законодавство залишає можливість визнання іноземних сертифікатів електронного підпису в межах двосторонньої міждержавної угоди між Бразилією та іншою країною.

Національний конгрес Республіки Чилі у 2002 р. прийняв Закон «Про електронні документи, електронний підпис та послуги сертифікації» [9]. Зазначений законодавчий акт запроваджує визначення електронного підпису як «будь-який звук, символ або електронний процес, який дозволяє одержувачу електронного документа визначити принаймні формально його автора». Закон переважно стосується взаємодії державних органів, процедури сертифікації надавачів послуг електронного підпису, а також вперше законом затверджуються права і обов'язки підписувачів електронного підпису. Однак питання визнання іноземних сертифікатів електронних підписів або електронних довірчих послуг Закон «Про електронні документи, електронний підпис та послуги сертифікації» не порушує.

У 2002 р. національним Конгресом Республіки Перу прийнято Закон «Про електронні підпис та сертифікати» № 27269 [10]. Закон визнає лише правовий статус цифрових або удосконалених електронних підписів, виданих у країні, та одночасно використовує дефініції «електронний підпис» та «цифровий підпис». Так, під електронним підписом розуміються будь-які електронні дані, що пов'язані з документом або автентифікують автора і відповідають характеристикам власноручного підпису. Водночас у визначенні цифрового підпису вперше законодавчо закріплюється конкретна технологія криптосистем із відкритим ключем. Цифровий підпис – це підпис, що використовує техніку асиметричної криптографії на основі застосування унікальної пари ключів: приватного ключа і, відповідно, відкритого ключа, які пов'язані між собою таким чином, що користувачі, які знають відкритий, не можуть вивести з нього приватний ключ. Законодавство Перу визнає дійсність цифрових сертифікатів, виданих в інших країнах, лише якщо вони відповідають перуанським стандартам.

Закон «Про електронні документи та електронний підпис» прийнято Республікою Уругвай (Уругвай) у 2009 р. [11]. Для правознавців цей закон цікавий тим, що вперше в законодавстві запроваджується дефініція «Національна електронна інфраструктура сертифікації». Також вперше в законодавстві країн Латинської Америки застосовуються одночасно визначення «електронний підпис» та «удосконалений електронний підпис». Так, «електронний підпис» означає дані в електронній формі, додані до електронного документа або логічно пов'язані з ним та використовувані підписувачем як засіб ідентифікації. «Удосконалений електронний підпис» означає електронний підпис, який відповідає таким вимогам: а) має інформацію про дані підписувача, що дає змогу однозначно ідентифікувати; б) зберігається і використовується виключно під контролем підписувача; в) доступний для перевірки третіми сторонами; г) пов'язаний з електронним документом таким чином, що будь-які подальші зміни в ньому були неможливі; г) створений із використанням технічно безпечного та надійного пристрою для створення підпису і має базуватися на визнаному сертифікаті, дійсному під час підписування. Визнання іноземних сертифікатів електронним підписом цим законом не регулюється і відбувається за принципом «за згодою сторін», що укладають угоди або контракти.

У 2012 р. Мексиканськими Сполученими Штатами прийнято низку змін у Торговий кодекс, Федеральний цивільний кодекс, Федеральний кодекс про Цивільні процедури одночасно із прийняттям Закону «Про електронний підпис» [12]. Законом, як і відповідним законом Уругваю, запроваджується поняття удосконаленого електронного підпису. Удосконалений електронний підпис – це електронний підпис, який має відповідати принципам функціональної еквівалентності, автентифікації та цілісності, які викладаються доволі деталізовано. Також законодавчо визначено порядок визнання іноземних сертифікатів електронного підпису шляхом застосування процедур укладання базових угод про співпрацю або координацію в сфері електронного підпису. Вказані процедури можуть здійснювати Секретаріат Конгресу, Міністерство економіки та Служба податкової адміністрації та інші сертифікаційні органи, за умови взаємного сповіщення про укладені угоди.

Висновки. Як ми бачимо, законодавство країн Латинської Америки та Мексики по-різному формує підходи до унормування суспільних відносин у сфері електронного



підпису та вирішення проблеми транскордонного визнання іноземних сертифікатів електронних підписів. Запроваджені законодавчі акти відрізняються базовими дефініціями електронного або цифрового підпису та нормами, за якими можна визнати іноземний сертифікат. Переважно застосовується підхід на основі Типового закону ЮНСІТРАЛ «Про електронні підписи» шляхом укладання міждержавних угод. Однак такі країни, як Бразилія та Перу, застосували практику нормативного геоблокування: визнання іноземних сертифікатів електронного підпису можливе лише за умови виключного використання іноземними сертифікаційними центрами національних стандартів та вимог РКІ, що обмежує споживацьку зможу отримувати закордонні електронні довірчі послуги в транскордонному режимі.

Список використаних джерел:

1. Global trends, forecast and opportunity assessment (2016–2022). Digital signature market. URL: <https://www.prnewswire.com/news-releases/routers-global-market-outlook--trends-forecast-and-opportunity-assessment-2014-2022-300168241.html> (дата звернення 07.08.2018).
2. Типовой закон ЮНСИТРАЛ об электронной торговле. *Издание Организации Объединенных Наций No R.99.V.4.* 1996. URL: http://www.uncitral.org/pdf/russian/texts/electcom/05-89452_Ebook.pdf (дата звернення 12.06.2018).
3. UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001. *United Nations Publication Sales No. E.02.V.8 ISBN 92-1-133653-8.* 2002. URL: <http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf> (дата звернення 12.06.2018).
4. Mason S. *Electronic Signatures in Law.* URL: <http://stephenmason.co.uk/books/electronic-signatures-law> (дата звернення 12.03.2019).
5. Carolina M. Laborde. *Electronic Signatures in International Contracts.* URL: https://books.google.com.ua/books?id=Cne-igPOkhgC&printsec=frontcover&hl=uk&source=gb_s_ge_summary_r&cad=0#v=onepage&q&f=false (дата звернення 12.05.2018).
6. Ley 527 sobre Mensajes de Datos. Comercio Electronico y Firma Digital de 18 de agosto de 1.999. URL: <https://co.groupseres.com/images/d/rs/Ley-527-1999.pdf> (дата звернення 12.05.2018).
7. Ley De Firma Digital № 25.506. URL: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm> (дата звернення 12.05.2018).
8. Medida Provisoria № 2.200-2, de 24 de Agosto de 2001 Institui a Infra-Estrutura de Chaves Pъblicas Brasileira – ICP-Brasil, e дb outras providkncias URL: <http://www.v-brazil.com/science/internet/digital-id/law.html> (дата звернення 12.05.2018).
9. Ley Sobre Documentos Electronicos, Firma Electronica y Servicios de Certificaciyn de Dicha Firma № 19.799, 25 de marzo 2002. URL: <https://www.leychile.cl/Navegar?idNorma=196640> (дата звернення 12.05.2018).
10. Ley No 27269 Ley de Firmas y Certificados Digitales. URL: <https://www.minjus.gob.pe/wp-content/uploads/2014/03/Ley27269.pdf> (дата звернення 12.05.2018).
11. Ley №18.600 de 21.09.009 Documento Y Firma Electrynica URL: <https://www.dgi.gub.uy/wdgi/page?2,principal,Ampliacion-Normativa,O,es,0,PAG;CONC;1059;7;D;ley-no-18-600-de-21-09-009;3;PAG> (дата звернення 12.05.2018).
12. Ley de firma electronica avanzada texto vigente. URL: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFEA.pdf> (дата звернення 12.05.2018).

