بررسی تطبیقی رویکردهای مختلف قوانین و مقررات نسبت به امضای الکترونیکی و امنیت آن

قاسم بختیاری فر [۱]- دکتر پرویز ساورائی [۲]- دکتر میر قاسم جعفر زاده [۳]- دکتر علی زارع [۴]

تاریخ دریافت: ۱۳۹۵/۹/۲۱- تاریخ پذیرش:۱۳۹۵/۱۰/۴

چکیده

امضاء بخش مهمی از شخصیت و اعتبار حقوقی، تجاری و حتی هنری اشخاص است و برای اعتبار بخشیدن به اسناد بین‌المللی وجود آن ضروری است. امضای یک سند مهمترین دلیل انتساب مفاد سند به ممضی و نشان دهنده پذیرش و قبول محتویات و مندرجات سند توسط متعاملینی است که ذیل آن را با رضایت امضاء کرده‌اند. به همین لحاظ امنیت در چنین فرایندی از اهمیت بسزایی برخوردار است و ورود این فرایند در فضای الکترونیکی و دیجیتال اهمیت این موضوع را دو چندان می‌نماید. به همین خاطر بدون وجود زیر ساخت‌های لازم امنیتی در فضای دیجیتال، امکان ارائه خدمات الکترونیکی وجود ندارد... نیاز به قانونگذاری در کنار فن آوری‌های مذکور در جهت تامین این امنیت، یکی از موثرترین موارد تحقق این موضوع می‌باشد.

لذا در این پژوهش در ابتدا بطور خلاصه و کلی به بررسی و تبیین امضای الکترونیکی در نظامات حقوقی مختلف می‌پردازیم و سپس سعی بر تبیین رویکردهای مختلف این نظامات، نسبت به موضوع امنیت امضاهای الکترونیکی می‌نماییم. تا در نهایت بتوان با بررسی برخی از قوانین کشورهای مختلف از جمله ایالات متحده امریکا، فرانسه و ایران، رویکردی متناسب با موضوع امنیت در فضای امضاهای الکترونیکی را تعیین نمود.

واژگان کلیدی: رویکرد، قوانین، امضاء الکترونیکی، امنیت، دستورالعمل اتحادیه اروپا

---

[۱]- دانشجوی دوره دکترای تخصصی حقوق خصوصی، گروه حقوق خصوصی، دانشکده حقوق و علوم سیاسی، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران

G.bakhtiyarifar52@gmail.com

[۲]- استادیار مدعو گروه حقوق خصوصی، دانشکده حقوق خصوصی، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران. (نویسنده مسئول)

[۳]- دانشیار مدعو گروه حقوق خصوصی، دانشکده حقوق خصوصی، واحد علوم و تحقیقات ، دانشگاه آزاد اسلامی، تهران، ایران

[۴]- استادیار گروه حقوق خصوصی ، دانشکده حقوق خصوصی ، واحد علوم و تحقیقات ، دانشگاه آزاد اسلامی، تهران، ایران

مقدمه

وجه مشترک اسناد اعم از رسمی یا عادی، تجاری یا غیرتجاری، عقود یا ایقاع و حتی نامه-های دوستانه، وجود امضاء است. همچنین به فراخور پیشرفت علم و بهره‌مندی از تکنولوژی و تحولات ناشی از ظهور پدیده‌های نوین الکترونیکی، امضاء نیز دستخوش تحول قرار گرفت و امروزه به اشکال نوین و الکترونیکی قابل صدور است. با این حال هر چند بهره‌مندی از دستاورد-های امضاء الکترونیکی، مرهون زحمات متخصصین علوم کامپیوتری، فناوری اطلاعات و ارتباطات است، ولی مطابق هر پدیده نوظهور اجتماعی آثار حقوقی آن دخالت و حضور حقوق‌دانان را اجتناب ناپذیر می‌سازد. به همین دلیل است که توجه روز افزون به مفهوم این نوع از امضاء به حدی رسیده است که تمامی قانونگذاران ملی و بین‌المللی را وادار ساخته حساسیتی ویژه به آن داشته باشند و در کنار تصویب مقررات تجارت الکترونیکی، به وضع قوانین ویژه‌ای برای امضای الکترونیکی مبادرت ورزند.

به همین لحاظ در ابتدا به بررسی قوانین کشور فرانسه، دستورالعمل اتحادیه حقوق اروپا و مقررات آنسیترال در رابطه با امضای الکترونیکی می‌پردازیم تا تعریف و مفهوم هر قانون نسبت به این فراین تعیین گردد و در ادامه به موضوع مورد پژوهش که همان امنیت امضای الکترونیکی از منظر قوانین است خواهیم پرداخت.

یکی از مهمترین موضوعاتی که باید با رعایت تمامی نکات فنی و تکنولوژی نسبت به آن وضع قوانین صورت گیرد موضوع امنیت امضاهای الکترونیکی است. چرا که لازمه استفاده بهینه از این فرایند تضمین هر چه بیشتر امنیت آن و اعتماد کاربران است.

قانون یکنواخت مبادلات و قانون امضاهای الکترونیکی ایالات متحده امریکا، استفاده از امضا-های الکترونیکی به جای امضای سنتی را مجاز می‌دانند و در خصوص نقش مسائل امنیتی این-گونه از امضاها سخنی به میان نیاورده است و مسائل امنیتی امضاهای الکترونیکی و تضمین این امنیت را از طرق دیگر تامین نموده است.

به طور کلی آنچه در هر شاخه ی از علوم مهمتر از فرضیه بنظر می‌رسد، طرح پرسش‌هایی است که با پاسخگویی به آنها، بستر مطالعه و تحقیقات بعدی فراهم شده و برای ذهن پرسشگر، دریچه‌ای جدید رو به افق تحقیقاتی در آن حوزه می‌گشاید. پاره‌ای از سوالات مطرح در زمینه

بررسی تطبیقی رویکردهای مختلف قوانین و مقررات موجود نسبت به مسایل امنیتی امضاهای الکترونیکی به شرح ذیل می‌باشد:

• قوانین ناظر بر موضوع امضای الکترونیکی در حال حاضر کدامند و اهمیت لزوم وضع قوانین در حوزه امنیت امضاهای الکترونیکی بصورت خاص تا چه حد است ؟

•رویکردهای مختلف قوانین و مقررات موجود نسبت به امضاهای الکترونیکی چیست؟

• کشورهای جهان از جمله ایالات متحده امریکا، فرانسه و ایران نسبت به امنیت در امضاهای الکترونیکی از چه قوانینی برخوردارند؟

که در این پژوهش سعی در پاسخ به سوالات مذکور و بررسی تطبیقی رویکردهای مختلف قوانین امنیتی امضاهای الکترونیکی شده است. تا بتوان رویکردی متناسب با شرایط و ویژگی خاص این فرایند را تعیین نمود.

از جمله مهمترین کشورها در این زمینه می‌توان به کشورهای کامن لا از جمله ایالات متحده امریکا اشاره نمود. که بررسی قوانین آن در کنار قوانین کشورهای سیویل لا از جمله فرانسه و ایران، نتایج خوبی را به همراه خواهد داشت. لازم به ذکر است که در این پژوهش از روش گردآوری استفاده نشده و بیشتر مطالب نتیجه برسسی مستقیم قوانین مربوطه می‌باشد و به همین لحاظ ارجاعات محدود می‌باشد.

لذا مطالب این پژوهش در قالب پنج بخش ارائه خواهد شد. به گونه‌ای که در بخش اول بصورت مختصر و کلی به امضای الکترونیکی در نظام‌های حقوقی و معرفی قوانین مربوطه می-پردازیم. چرا که لازمه تامین امنیت این فرایند شناخت دقیق و ارائه تعریفی مشخص و روشن از آن است و تعاریف ارائه شده از امضای الکترونیکی در قوانین بین‌المللی و قوانین کشورها متفاوت است و در بخش دوم به موضوع عدم توجه به مسائل امنیتی می‌پردازیم و در بخش سوم موضوع امنیت به عنوان پیش شرط قابلیت اجرا را بررسی کرده و سپس موضوع امنیت به عنوان وسیله-ای برای تخصیص ضمان را مورد بررسی قرار می‌دهیم و در آخر به مهمترین بخش پژوهش و موضوع امارات قانونی و بررسی قوانین مختلف در این حوزه خواهیم پرداخت.

۱- امضای الکترونیکی در نظامات حقوقی مختلف

از مهمترین منابع حقوقی خارجی در سطح بین‌المللی در مورد امضای الکترونیکی و به طور کلی حقوق اسناد الکترونیکی می‌توان به قانون نمونه آنسیترال راجع به تجارت الکترونیکی[۱]،

قانون نمونه آنسیترال راجع به امضای الکترونیکی[۲]، کنوانسیون سازمان ملل متحد راجع به استفاده از ارتباطات الکترونیکی در قراردادهای بین‌المللی[۳]، دستورالعمل اتحادیه اروپا راجع به تجارت الکترونیکی[۴]، دستور العمل اتحادیه اروپا راجع به امضای الکترونیکی[۵]و قانون ۲۰۳ مورخ ۱۳ مارس ۲۰۰۰ فرانسه و آئین نامه‌های بعدی آن اشاره کرد. که در بخش آتی در ابتدا به تبیین قانون نمونه آنسیترال و دستورالعمل اتحادیه اروپا راجع به امضاهای الکترونیکی می-پردازیم و موادی از این قوانین که در رابطه با امضاهای الکترونیکی وتعریف آنها می باشد را مورد بررسی قرار خواهیم داد و سپس به بررسی مختصر نظام حقوقی فرانسه و برخی از قوانین این کشور، بعنوان یکی از نظامات حقوقی پیشرو در زمینه اسناد الکترونیکی و طبعا امضاهای الکترونیکی خواهیم پرداخت.

۱-۱-قانون نمونه آنسیترال

بند الف ماده ۲ قانون نمونه امضای الکترونیکی ۲۰۰۱ آنسیترال مقرر می‌دارد:

«امضای الکترونیکی به معنای داده‌ای در شکل الکترونیکی است که چسبیده یا به طور منطقی به یک داده پیام متصل شده است و می‌تواند برای شناسایی هویت امضاء کننده در ارتباط با داده پیام و یا نشان دادن رضایت امضاءکننده نسبت به اطلاعات موجود در داده پیام مورد استفاده قرار گیرد» [۶].

همین قانون در تعریف داده پیام در بند ج ماده ۲ مقرر می‌دارد:

«داده پیام عبارت است از اطلاعاتی که با وسایل الکترونیکی، نوری یا مشابه از جمله مبادله الکترونیکی داده‌ها، پست الکترونیکی، تلگراف، تلکس، تلکوپی، تولید، ارسال یا دریافت و یا ذخیره می‌شود و از طرف خود یا کسی که از جانب او نمایندگی دارد عمل می‌کند»[۷].

مهمترین نکته در تعریف مزبور، این است که امضای الکترونیکی به عنوان «داده» مطرح می-شود و این تعریف مبین ماهیت فنی و جنس حقیقی و منطقی امضاست. ضمنا برخلاف تعریف امضاء الکترونیکی در حقوق ایران که در آن صرفا به جنبه شناسایی هویت امضاء کننده از طریق صدور امضای الکترونیکی به عنوان تنها آثار و کاربرد امضا اشاره شده است، در مصوبه آنسیترال دو کارکرد شناسایی هویت امضاءکننده و نشان دادن رضایت شخص ممضی نسبت به اطلاعات موجود در داده پیام (سند الکترونیکی یا قرارداد الکترونیکی) برای امضای الکترونیکی احصا شده است.

در رابطه با حقوق امضای الکترونیکی از منظر مصوبات آنسیترال، می‌توان گفت که مطابق قانون نمونه تجارت الکترونیکی مصوب ۱۹۹۶، آن دسته از اسناد و مدارک الکترونیکی که کارکردهای اسناد کاغذی را احراز می‌کنند، از نظر حقوقی معتبرند. عمده این کارکردها عبارتند از : شناسایی شخص امضاء کننده، ایجاد قطعیت در دخالت شخص مذکور در تولید امضاء، ایجاد ارتباط بین شخص مذکور و محتوای سند، نشان دهنده رضایت فرد امضاء کننده نسبت به محتوای سند

۱-۲- دستورالعمل اتحادیه اروپا

دستورالعمل ۱۹۹۹ اتحادیه اروپا بعنوان تاثیرگذارترین سند در زمینه ایجاد بستر حقوقی مناسب برای ترویج استفاده از امضای الکترونیکی و تصویب مقررات لازم در کشورهای اروپایی محسوب می‌شود. هر چند که دستورالعمل مذکور برای اعضای این اتحادیه الزام آور است و صرفا کشورهای عضو موظفند در تدوین قوانین خود از آن تبعیت نمایند، اما این سند الگوی اصلی برای فعالیت‌های تحقیقاتی و قانونگذاری در جهان بوده است. دستورالعمل مزبور در ماده یک خود، حوزه اجرائی و اهداف دستورالعمل را تعیین کرده است و در متن آن آمده است که:

«هدف از این دستورالعمل تسهیل استفاده از امضاء الکترونیکی و کمک به رسمیت شناختن قانونی آن است. این دستورالعمل یک چارچوب قانونی برای امضاء الکترونیکی و برخی از گواهی-های الکترونیکی به منظور اطمینان از عملکرد مناسب آنها در بازار داخلی ایجاد می‌کند».

بند ۱ ماده ۲ این دستورالعمل به تعریف امضای الکترونیکی پرداخته و اعلام می‌دارد:

«امضای الکترونیکی داده ای است که به شکل الکترونیکی، به سایر داده‌های الکترونیکی ضمیمه و یا متصل است و به عنوان روشی برای اثبات هویت به کار میرود»[۸].

دستورالعمل اتحادیه اروپا در تعاریف مندرج در ماده یک خود، با تعاریف موارد و جوانب مختلف مرتبط با امضای الکترونیکی، راه تفاسیر مختلف را بسته و این خود از نکات مثبت این دستورالعمل است. بند ۳ از ماده ۲ این دستورالعمل مقرر می‌دارد:

«امضاء کننده فردی است که ابزار ایجاد امضاء را دارد و از سوی خود یا یک فرد حقیقی یا حقوقی یا یک واحد مستقل که نماینده آن است، عمل می‌کند»[۹].

بند ۴ از ماده مذکور مقرر می‌دارد:

«داده‌های منحصر به فرد مثل کدها و کلیدهای خصوصی رمز نگاری است که توسط امضاء کننده برای ایجاد امضای الکترونیکی به کار می‌رود» [۱۰].

لازم به ذکر است، اتحادیه اروپا بعدها در تکمیل دستورالعمل ۱۳ دسامبر ۱۹۹۹ خود، دستور العمل هشتم ژوئن ۲۰۰۰ را به تصویب رساند که هدف از تصویب آن، نزدیک سازی و تطبیق برخی از مقررات ملی قابل اجرا نسبت به خدمات شرکت‌های اطلاع رسانی در مواردی همچون بازار داخلی، ارتباطات تجاری، قوانین راهنمایی و رانندگی، قراردادهای الکترونیکی و غیره بود.[۱]

۱-۳- حقوق فرانسه

حقوق فرانسه بعنوان یکی از نظامات حقوقی پیشرو در زمینه اسناد الکترونیکی، در حال حاضر سه متن قانونی مرجع و اصلی به شرح ذیل دارد:

۱- قانون شماره ۲۳۰ - ۲۰۰۰ مورخ ۱۳ مارس ۲۰۰۰

۲- آئین نامه شماره ۲۷۲ - ۲۰۰۱ مورخ ۳۰ مارس ۲۰۰۱

۳- آئین نامه شماره ۹۷۳ - ۲۰۰۵ مورخ ۱۰ اوت ۲۰۰۵

که در ذیل به اختصار به شرح دستاوردهای هر یک از سه مورد فوق الذکر می‌پردازیم.[۲]

در تاریخ ۱۳ مارس ۲۰۰۰، پارلمان فرانسه، قانونی[۱۱] را برای پذیرش امضای الکترونیکی تصویب و از طریق آن مفهوم امضای الکترونیکی، وارد قانون مدنی فرانسه شد. این قانون، در قانون مدنی با شماره مواد ۱۳۱۶ الی ۴ -۱۳۱۶ گنجانده شده است. لازم به ذکر است که این قانون به سرعت قابلیت اجرایی یافت.

قسمت ابتدایی بند اول ماده ۴-۱۳۱۶ قانون مدنی فرانسه در بیان کارکرد امضاء مقرر می‌دارد:

«امضای مورد نیاز برای تکمیل یک سند حقوقی، شخص امضا کننده را شناسایی و تایید اصالت می‌نماید. این امضا خود بیانگر رضایت طرفین معامله بر تعهداتی است که از سند ناشی می‌گردد...» [۱۲].

ماده ۱۳۱۶ این قانون بدون پرداختن و توجه به تعریف امضای الکترونیکی، به قواعد ماهوی امضای الکترونیکی می‌پردازد.[۳] بند ۳ این ماده مقرر می‌دارد:

---

[1] -KAINIYA, Mohammad, LA SIGNATURE ELECTRONIQUE, Mémoire pour le master 2 de droitnotariat. Université Jean-Moulin Lyon III, 2008, p.55.

[۲]-کینیا، محمد، امضای الکترونیک منطبق با حقوق فرانسه، بنیاد حقوقی میزان، ۱۳۸۸، ص ۳۰

[3] - KAINIYA, Mohammad, La dématérialisation des acteset conventions, Thèse de doctorat. Université Jean-Moulin Lyon3, 2011 p. 63.

«.. با اثبات صدور امضاء از سوی شخص معین، قرارداد (توافق) دارای ارزش و اعتبار مساوی با معادل کاغذی آن خواهد بود» [۱۳]. همچنین این قانون صرفاً و به سادگی، نوشته الکترونیکی را مشابه و برابر با نوشته کتبی می‌داند و برای آن ارزش حقوقی نوشته کتبی را قائل است.[1]

ماده ۱-۱۳۱۶ قانون مدنی فرانسه در تبیین ارزش حقوقی امضای الکترونیکی مقرر می دارد:

«نوشته به شکل الکترونیکی همانند نوشته کتبی و با همان میزان از اعتبار، به عنوان دلیل پذیرفته می‌شود، به شرط اینکه بتواند شخصی را که نوشته مزبور از او نشات می‌گیرد را بدقت شناسایی کند و نوشته به نحوی ایجاد و نگهداری شود که تمامیتش تضمیین گردد»[۱۴].

همانطور که بیان گردید، بند اول ماده ۴-۱۳۱۶ قانون مدنی فرانسه به بیان کارکرد امضاء می‌پردازد و بند دوم ماده ۴ ـ ۱۳۱۶ قانون مدنی فرانسه به اصل صحت اختصاص یافته است. این بند مقرر می‌دارد:

«زمانی یک امضاء، امضایِ الکترونیکی است که آن امضاء عبارت باشد از استفاده از شیوه مطمئن شناسایی و تایید اصالت، و (نیز) متضمن رابطه آن امضاء با سندی که به آن منضم گردیده است. صحت و درستی این فرآیند از پیش، فرض شده است (اصل بر صحت و درستی است) تا زمانی که خلاف آن ثابت گردد. هنگامی که امضای الکترونیکی ایجاد شد، هویت امضاء کننده تضمین گردیده و تمامیّت سند در شرایطی که شورای دولتی به موجب حکمی معین می‌کند، تضمین می‌شود».

همچنین قانونگذار فرانسه در راستای به رسمیت شناختن سند رسمی الکترونیکی در پایان بند اول ماده ۴-۱۳۱۶مقرر می‌دارد: «... زمانی که امضای مزبور (امضای الکترونیکی) توسط مامور دولتی صورت می‌گیرد، آن امضا به سند رسمیت می‌بخشد» بنابراین قانونگذار فرانسه اولین و تنها قانونگذاری است که سند رسمی الکترونیک را به رسمیت شناخته است.

شورای دولتی فرانسه در اجرای قانون شماره ۲۳۰ – ۲۰۰۰، آئین نامه شماره ۲۷۲-۲۰۰۱ را در تاریخ ۳۰ مارس ۲۰۰۱ تصویب نمود. فراز اول از ماده یک آئین نامه مذکور به تعریف امضای الکترونیکی پرداخته است و مقرر می‌دارد:

«امضای لکترونیکی داده‌ای است که با استفاده از فرآیندی مطابق با شرایط تعریف شده در اولین جمله از بند دوم ماده ۴-۱۳۱۶ قانون مدنی ناشی می‌گردد».

[1] -KAINIYA, op. cit, 2008, p.93.

نکته قابل ملاحظه در این آئین نامه این است که قانونگذار فرانسوی در قانون مصوب ۱۳ مارس ۲۰۰۰، صرفا به کلیات، قواعد ماهوی و نتایج و آثار امضای الکترونیکی پرداخته و به طور غیرقابل باوری از تعریف امضای الکترونیکی خودداری نموده است.[1] اما همانطور که ملاحظه می‌شود شورای دولتی در شروع آئین نامه در فراز اول از ماده یک آن، ابتدا به تعریف امضای الکترونیکی می‌پردازد.

۲- بررسی تطبیقی حقوق ایران، فرانسه، دستورالعمل اتحادیه حقوق اروپا و مقررات آنسیترال در مورد امضای الکترونیکی

قانون نمونه آنسیترال، فرانسه و دستورالعمل اتحادیه اروپا با معرفی امضای الکترونیکی به عنوان «داده»، مناسب تر از قوانین داخلی عمل نموده است. همانطور که اشاره شد، با توجه به تعریف امضای الکترونیکی در قانون تجارت الکترونیکی و بکاربردن واژه علامت، چندان صحیح به نظر نمی‌رسد.

در اکثر نظام‌های حقوقی دنیا، برای امضاء دو کارکرد اساسی مطرح شده است:

۱- اینکه هویت کسی که سند از طرف او صادر شده است را مشخص می‌نماید.

۲- آنکه اصالت محتوای سند و آثار حقوقی آن ثابت شود

قانون آنسیترال نیز به دو کارکرد امضاء یعنی؛ شناسایی هویت امضاء کننده و رضایت وی به مفاد سند، توجه کرده است اما در قانون ایران به رضایت امضاءکننده نسبت به مفاد سند توجه نشده و تنها به شناسایی امضاء کننده اشاره شده است. بنابراین شایسته‌تر این بود که قانونگذار ایران برای تکمیل تعریف خود، قصد التزام امضاء کننده به مفاد سند را متذکر می‌شد.

متون قانون فرانسه ساختاری را می‌سازند که مبتنی بر فرض صحت بوده و پیش بینی این فرض خود متفاوت با سیستم اتحادیه اروپا می‌باشد و به نوعی امتیازی برای قانونگذار فرانسه محسوب می‌گردد.

۳- امنیت به عنوان پیش شرط قابلیت اجرا ووسیله‌ای برای تخصیص ضمان[2]

برخی قوانین و مقررات، سطحی از امنیت را برای قابل اجرا بودن قانون مبادله الکترونیکی

[1]-KAINIYA, op. cit, 2011, p.66.
[2]-Risk Allocation

ضروری می‌دانند و برخی دیگر از قوانین، وجود یا فقدان امنیت را به عنوان ضابطه‌ای برای تخصیص مسئولیت تلقی نموده‌اند.

۳-۱-پیش شرط قابلیت اجرا

قانون نمونه آنسیترال در خصوص امضاهای الکترونیکی عنصر قابل اعتماد بودن[1] را به عنوان شرط معتبر شمردن امضاهای الکترونیکی در نظر گرفته است و مقرر می‌دارد:

«هرگاه قانون، امضای شخص را لازم بداند این شرط در رابطه با داده پیام با به کارگیری امضای الکترونیکی محقق می‌شود که با توجه به تمامی اوضاع و احوال از جمله هرگونه توافق موجود میان طرفین به اندازه کافی به تناسب هدفی که داده پیام بدان منظور، تولید و یا ارسال شده قابل اعتماد باشد».

بند سوم این ماده معیار قابل اعتماد بودن امضای الکترونیکی را بیان کرده است و در قالب چهار مورد بیان می‌نماید که عبارتند از:

الف) داده‌های مربوط به تولید امضاء، در شرایط به کارگیری آنها، صرفاً با امضاءکننده مرتبط باشد و نه شخص دیگری

ب) داده‌های مربوط به تولید امضاء، در زمان امضاء کردن، تحت کنترل انحصاری امضاءکننده باشند و نه شخص دیگری

ج) هرگونه تغییر حاصل در امضای الکترونیکی پس از امضاء کردن، قابل شناسایی باشد

د) در مواردی که هدف از شرط قانونی (وجود) امضاء تضمین تمامیت اطلاعات باشد که امضاء با آنها مرتبط است، هرگونه تغییر حاصل در این اطلاعات، پس از امضاء کردن قادر به شناسایی باشد.

۳-۲- وسیله‌ای برای تخصیص ضمان

ماده ۱۰ قانون یکنواخت مبادلات الکترونیکی ایالات متحده[2] در برخی موارد مسئولیت ناشی از اشتباهات پیش آمده را متوجه طرفی می‌داند که تشریفات امنیتی مورد توافق را رعایت نکرده باشد. همچنین قانون یکنواخت تجارت ایالات متحده امریکا نیز خسارات ناشی از دستورهای متقلبانه پرداخت الکترونیکی را بر مبنای رعایت یا عدم رعایت ضوابط امنیتی مورد توافق، تخصیص می‌دهد.

[1]- Reliability
[2]- Uniform Electronic Transactions Act (U E T A)

۴- تأسیس امارات قانونی[۱]

در برخی از قوانین، مقرر شده که تقریباً تمامی انواع امضاهای الکترونیکی می‌توانند واجد آثار قانونی بوده و جایگزین امضاهای سنتی شوند. این قوانین در عین حال پذیرفته‌اند که بعضی از امضاهای الکترونیکی نسبت به مابقی مطمئن‌تر هستند.

قوانین مذکور به منظور ایجاد انگیزه در اشخاص و استفاده بیشتر از این دسته امضاهای الکترونیکی و فراهم آوردن سطح بالایی از امنیت و اطمینان نسبت به اصالت و یا تمامیت اسناد الکترونیکی که در آنها از این نوع امضاها استفاده شده، نوعاً اماره‌ای قانونی به سود طرف اعتماد کننده در خصوص هویت فرستنده و یا تمامیت آن سند تأسیس نموده‌اند.

لازم به ذکر است که این دسته از قوانین خود به دو دسته تقسیم شده و هر دسته رویکرد خاص خود را دارد:

۴-۱- قوانینی که در آنها به فناوری خاصی از امضای الکترونیکی اشاره شده است[۲]

این دسته از قوانین، اماره مطمئن بودن را صرفاً در خصوص امضاهای دیجیتال قابل اجرا می‌دانند.

به عنوان نمونه قوانین تصویب شده در ایالات متحده مینه سوتا، میسوری، یوتا و واشنگتن آمریکا، آلمان، ایتالیا، مالزی و سنگاپور چنین رویکردی را اتخاذ کرده‌اند.

به منظور تضمین این امر که امضای دیجیتال برای برخورداری از اماره مذکور به اندازه کافی قابل اعتماد است قوانین مذکور معمولاً چارچوب قانونی ویژه‌ای را برای فعالیت مراجع گواهی، که داوطلبانه جهت تأیید به مراجع دولتی ذیربط مراجعه می‌کنند پیش‌بینی کرده است. بر مبنای این اماره که گواهی‌های صادره توسط مراجع تأیید شده را قابل اعتماد می‌داند و امضای دیجیتال ایجاد شده از طرق کلید خصوصی مرتبط با کلید عمومی معرفی شده در گواهی‌های مذکور، امضای قابل اعتمادی خواهد بود.[۳] قوانین مذکور اسناد مجهز به این امضاها را نیز قابل اعتماد دانسته‌اند.

---

[1]- Legal Presumptions

[2]- Technology- Specific Statutes

[3]-Torrubia, Andres, Mora, Francisco J., Marti, Luis, Cryptography Regulations for E-commerce and Digital Rights Management, Computers & Security Vol.20, No.8, 2001, p.p. 730-731.

به عنوان مثال مطابق قانون امضای دیجیتال ایالت یوتای[1] آمریکا هرگاه یک امضای دیجیتال از طریق کلید عمومی مندرج در گواهی معتبر صادره، توسط یک مرجع گواهی تأیید شده، قابل شناسایی باشد دادگاه‌های ایالات یوتا فرض خواهند نمود که:

الف) امضای دیجیتال به مشترک معرفی شده در گواهی مذکور، تعلق دارد.

ب) امضای دیجیتال توسط این مشترک به قصد امضای پیغام به آن منضم شده است.

۴-۲- قوانینی که در آنها به فناوری خاصی اشاره نشده است

این قوانین در ابتدا و به صورت کلی، امضاهای الکترونیکی را معتبر می‌دانند. اما در ادامه معیارها و ضوابطی را اعلام می‌نمایند که امضاهای واجد این ضوابط و معیارها، عنوان ویژه‌ای را می‌گیرند و از اماره قابل اعتماد بودن برخوردار خواهند شد. بدین ترتیب صرفاً معیارهایی ارایه شده است بدون آنکه از مکانیسم معینی، نامی به میان آید.

قانون مدنی فرانسه، دستورالعمل امضاهای الکترونیکی اتحادیه اروپا و قانون تجارت الکترونیکی جمهوری اسلامی ایران در این دسته قرار می‌گیرند.

۴-۲-۱- قانون فرانسه

همانطور که پیش‌تر هم ذکر شد، با تصویب قانون ۱۳ مارس ۲۰۰۰ راجع به هماهنگ سازی حقوق ادله اثبات با فناوری‌های نوین و مرتبط با امضای الکترونیکی، اصلاحاتی در قانون مدنی فرانسه صورت گرفت. از جمله اینکه با ارایه تعریفی کاربردی از امضاء، امضای الکترونیکی در این کشور برسمیت شناخته شد.

همچنین امضای الکترونیکی درماده ۴-۱۳۱۶ قانون مدنی فرانسه تعریف شده است و بدین بیان است که:

«امضای الکترونیکی شامل به بکارگیری فرآیندی مطمئن برای شناسایی است که ارتباط خود را با سندی که بدان منضم شده تضمین می‌نماید. کسی که مدعی مطمئن بودن فرآیند مذکور است باید آن را در دادگاه به اثبات برساند».

اما در ادامه ماده ۴-۱۳۱۶ فوق‌الذکر آمده است:

«هرگاه ایجاد امضای الکترونیکی و تضمین هویت امضاء کننده و تمامیت سند تحت شرایط

[1]- Utah

مقرر توسط شورای دولتی صورت گیرد، مطمئن بودن این فرآیند، جز در صورت وجود دلیل مخالف، مفروض خواهد بود».

شورای دولتی فرانسه در فرمان ۳۰ مارس ۲۰۰۱ [۱] این شرایط را بیان کرده که در ذیل به آنها می‌پردازیم:

مطابق ماده ۲ فرمان فوق الذکر، جز در صورت وجود دلیل مخالف، فرآیند ایجاد امضای الکترونیکی منوط به تحقق شرایط ذیل، مطمئن فرض خواهد شد:

۱- هرگاه فرآیند مشتمل بر به کارگیری یک امضای الکترونیکی ایمن [۲] باشد؛

۲- در نتیجه به کارگیری ابزاری ایمن برای ایجاد امضای الکترونیکی [۳] صورت گرفته باشد. [۴]

مطابق ماده ۳ قانون مذکور، ابزار ایجاد امضای الکترونیکی، زمانی ایمن تلقی می‌شوند که محرمانگی داده‌های مورد نیاز برای ایجاد امضا و حمایت از آنها را در برابر هرگونه تغییر و تحریف تضمین نماید. که از جمله آنها می‌توان به موارد ذیل اشاره نمود:

۱- شناسایی این امضا از طریق به کارگیری یک گواهی الکترونیکی حایز شرایط صورت گرفته [۵] باشد.

۲- نسبت به امضا کننده، منحصر به فرد باشد. بدین مفهوم که نباید امضای الکترونیکی یک شخص قابل انتساب به شخص دیگر باشد. لازمه این امر، برخورداری از داده‌هایی اختصاصی (مانند کلید خصوصی در امضای دیجیتال) برای تولید امضا است.

۳- امضا کننده بایستی ابزار ایجاد امضا را تحت کنترل انحصاری خود داشته باشد. اعم از اینکه او امضاء را ایجاد کند و یا دیگران با مسئولیت وی امضاء را تولید نمایند.

بنابراین سخت افزار و نرم‌افزار به کار رفته جهت امضای الکترونیکی باید تحت کنترل انحصاری امضا کننده باشند.

۴- با سندی که بدان منضم شده است چنان رابطه‌ای داشته باشد که هرگونه تغییر آتی ایجاد شده در سند، قابل شناسایی باشد.

---

[1]- Decret no 2001 du 3. Mars 2001 pris pour lapplication larticle 1316-4: du code et relative a la signature electronoque.

[2]- Signature ElectroniqueSecurisee

[3]- DispisitifSecurisee de creation de signature electrionoque

[4] - De Lamberterie, Isaballe et Blanchette, Jean- Francois. Le decret du relatif a la signature electronique, lecture critique, technique etjuridique, 3 mars 2001, Pp. 5-7.

[5]- Certificatelectroniquequelifie

مقررات فوق الذکر به طور کلی از دستورالعمل امضاهای الکترونیکی اتحادیه اروپا اقتباس شده است.

بنابراین در ذیل به این دستورالعمل نیز اشاره می‌کنیم.

۴-۲-۲- دستورالعمل امضاهای الکترونیکی اتحادیه اروپا

این دستورالعمل پس از ارایه تعریفی کلی از امضای الکترونیکی (در بند ۱ ماده ۲) نوع خاصی از امضاهای الکترونیکی را معرفی کرده است.

مطابق بند دوم از ماده ۲ دستورالعمل، امضای الکترونیکی پیشرفته[1] عبارت است از امضای الکترونیکی که شرایط ذیل را داشته باشد:

۱- به صورت انحصاری با امضاء کننده مرتبط باشد؛

۲-امکان شناسایی امضاءکننده را فراهم آورد؛

۳-با استفاده از ابزاری ایجاد شده باشد که امضاءکننده بتواند آنها را تحت کنترل انحصاری خود در آورد؛

۴- با داده‌هایی که به آنها مربوط می‌شود به گونه‌ای مرتبط باشد که هرگونه تغییر بعدی داده‌ها قابل کشف باشد.

ماده ۵ دستورالعمل تحت عنوان آثار قانونی امضاهای الکترونیکی شامل دو بند است:

۱-کشورهای عضو، تضمین می‌نمایند که امضاهای الکترونیکی پیشرفته مبتنی بر گواهی‌های حائز شرایط که از طریق ابزاری ایمن ایجاد می‌شوند:

الف- در رابطه با داده‌های الکترونیکی، شرایط وجود امضاء را محقق می‌نمایند، درست به همان طریقی که امضای دستی، این شرایط را در رابطه با داده‌های مبتنی بر کاغذ تأمین می‌کند.

ب- به عنوان دلیل در دادرسی‌های قانونی پذیرفته می‌شوند.

در بند دوم این ماده آمده است:

۲- کشورهای عضو تضمین می‌نمایند که اثر قانونی و قابلیت پذیرش امضاهای الکترونیکی به عنوان دلیل در دادرسی‌های قانونی صرفاً به علل زیر رد نخواهد شد:

الف- به دلیل الکترونیکی بودن ب- به دلیل عدم برخورداری از یک گواهی حائز شرایط و ...

[1]- Advanced Electrionic Signature

با دقت در ماده ۵ در می‌یابیم که بند ۱ این ماده در واقع امضای الکترونیکی پیشرفته را به امضای سنتی تشبیه نموده بدین معنی که هرگاه امضای الکترونیکی شرایط معین مذکور در تعریف امضای الکترونیکی پیشرفته را در برداشته باشد، باید آن را به عنوان دلیل در دادرسی‌ها پذیرفته و همچنین همان قدرت اثباتی معادل امضای سنتی را برای آن قائل شد. به همین دلیل به بند مذکور عنوان بند تشبیه[۱] اطلاق می‌شود. بدیهی است که بند تشبیه صرفاً در خصوص امضاهای پیشرفته قابل اجرا است.

هر گاه شرایط اجرای بند تشبیه (بند ۱ ماده ۵) موجود نباشند، بند دوم این ماده اعمال خواهد شد. این بند به بند عدم تبعیض[۲] مشهور شده است که به موجب آن دادگاه نمی‌تواند صرفاً به دلیل عدم تحقق شرایط بند ۱، از پذیرش امضای الکترونیکی امتناع ورزد.

اصل منعکس شده در بند دوم ماده ۵ را در واقع باید اصل کلی قابلیت پذیرش[۳] امضاهای الکترونیکی دانست، بدین معنی که قاضی ملزم است امضای الکترونیکی را به عنوان دلیل پذیرفته و آن را مورد بررسی قرار دهد. هر چند که ممکن است پس از مطالعه دقیق، امضای ارایه شده را فاقد هرگونه قدرت اثباتی بداند.

ایرادی که در رابطه با طرز تنظیم ماده ۵ دستورالعمل مطرح می‌شود آن است که ماده مذکور ابتدا ارزش اثباتی نوع خاصی از امضاهای الکترونیکی را بیان کرده و پس از آن اصل کلی پذیرش امضاهای الکترونیکی را ذکر نموده است. در حالی که اصولاً باید در ابتدا گفته شود که امضاهای الکترونیکی در دادگاه پذیرفته می‌شوند و سپس از قدرت اثبات منحصر به فرد آنها سخن به میان آید.[۴]

۴-۲-۳- قانون تجارت الکترونیکی جمهوری اسلامی ایران

قانون تجارت الکترونیکی جمهوری اسلامی ایران مقرر می‌دارد:

«هرگاه قانون وجود امضاء را لازم بداند امضای الکترونیکی مکفی است».

در این ماده به طور کلی امضاهای الکترونیکی به عنوان معادلی برای امضای سنتی پذیرفته شده است اما ماده ۱۰ همین قانون مقرر می‌دارد:

---

1. Assimilation Clause
2. Non – discrimination clause
3. Principle of Admissibikity

۴- نظیر قانون مدنی فرانسه و قانون تجارت الکترونیکی جمهوری اسلامی ایران

«امضای الکترونیکی مطمئن باید دارای شرایط زیر باشد:

۱- نسبت به امضاءکننده منحصر به فرد باشد.

۲- هویت امضاءکننده داده پیام را معلوم نماید.

۳- به وسیله امضاءکننده و یا تحت اراده انحصاری وی صادر شده باشد

۴- به نحوی به یک داده پیام متصل شود که هر تغییری در آن داده پیام قابل تشخیص و کشف باشد».

ماده ۱۵ قانون مذکور اعتبار ویژه‌ای را برای این نوع امضاء پیش‌بینی کرده است:

«نسبت به داده پیام مطمئن، سوابق الکترونیکی مطمئن و امضای الکترونیکی مطمئن انکار و تردید مسموع نیست و تنها می‌توان ادعای جعلیت به داده پیام مزبور وارد و یا ثابت نمود که داده پیام مزبور به جهتی از جهات قانونی از اعتبار افتاده است».

با آنکه در بسیاری از قوانینی که آماره‌هایی قانونی را برای دسته خاصی از امضاهای الکترونیکی (تحت عنوان امضای الکترونیکی مطمئن، ایمن، پیشرفته و ...) در نظر گرفته‌اند. صرفاً معیارهای اجرای این امارات بیان شده و فناوری معینی مورد اشاره قرار نگرفته است.[۱](بی طرفی علمی یا تکنولوژیک) مع ذلک در حال حاضر امضاهای دیجیتال از معیارهای مذکور در قوانین مورد بحث برخوردار هستند.[۲]

نتیجه گیری

پس از بررسی اهم قوانین مرتبط با امضاهای الکترونیکی، نتایج حاصل از این پژوهش بدین بیان است:

امضای الکترونیکی عبارت از داده‌ای است که در بستر الکترونیکی و به قصد التزام به مندرجات و مفاد داده پیام، به آن منضم یا متصل می‌شود و بیانگر رضایت ممضی به مفاد و مندرجات آن داده پیام بوده و موجبات شناسایی ایشان را فراهم می‌کند.

در بسیاری از قوانین مصوب، در خصوص نقش مسائل امنیتی سخنی به میان نیامده است این قوانین صرفاً استفاده از امضاهای الکترونیکی به جای امضای سنتی را مجاز می‌دانند.

---

[۱]- زرکلام، ستار، امضای الکترونیکی و جایگاه آن در نظام ادله اثبات دعوی. مجله مدرس، شماره ۱، ۱۳۸۲.

[۲]- مظاهری کوهانستانی، رسول، مطالعه تطبیقی امضای الکترونیکی در حقوق ایران و مقررات آنسیترال ، انتشارات جنگل، ۱۳۹۳، ص ۷۵.

این رویکرد توسط قانون یکنواخت مبادلات و قانون امضاهای الکترونیکی ایالات متحده امریکا اتخاذ شده است..

دستورالعمل اتحادیه اروپا بر خلاف قانون مدنی فرانسه و قانون تجارت الکترونیکی جمهوری اسلامی ایران ابتدا اثر قانونی ویژه امضاهای الکترونیکی پیشرفته را بیان نموده و سپس به طور کلی مقرر شده که امضاهای الکترونیکی باید در دادگاه‌ها به عنوان امضاء پذیرفته شوند.

قوانین مورد بحث اگرچه صریحاً امنیت را به عنوان پیش شرط قابل اجرا بودن مبادلات الکترونیکی اعلام نکرده‌اند، منتها به منظور تشویق اشخاص به اتخاذ تدابیر امنیتی مناسب، اماره-ای قانونی به سود کسانی که از امضاهای الکترونیکی معینی استفاده می‌کنند به وجود آورده‌اند. در بسیاری از قوانین، صرفا اماره‌های قانونی را برای دسته خاصی از امضاهای الکترونیکی (تحت عنوان امضای الکترونیکی مطمئن، ایمن، پیشرفته و ...) در نظر گرفته‌اند و هیچ اشاره ای به فناوری‌های لازم جهت اعمال این امارات نشده است.

برخلاف دستورالعمل اروپا، که مسائل فنی امضای الکترونیکی را نیز بیان نموده، قانون ۱۳ مارس ۲۰۰۰ فرانسه در مورد تطبیق حقوق ادله با فناوریهای اطلاعات و مرتبط با امضای الکترونیکی، که قانون مدنی فرانسه را کامل نمود، وارد هیچ ملاحظه فنی نشده است.

پی نوشتها

[1] UNCITRA Model Law on Electronic Commerce Guide to Enactment with 1996

[2] UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001

[3] United Nations Convention on the Use of Electronic Communications in International Contracts

[4]DIRECTIVE 2000/31/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)

[5] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures

[6] Art2.(a) "Electronic signature" means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message;

[7] Art2.(c) "Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy;

[8]"Article 2 – Definitions Aux fins de la presented directive, on entend par: «signature electronique», undone sous formeelectronique, qui estjointeouliéelo giquement a dautresdonneeselectroniques et qui sert de methoded' authentification;"

[9] Art2-3 'signatory' means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents;

[10]Art2-4 'signature-creation data' means unique data, such as codes or private cryp to graphic keys, which are used by the signatory to create an electronic signature;

[11] Law adapting evidence to information technology and relating to electronic signature, March ,2000

[12] Art. 1316-4. - La signature necessaire a la perfection d'un actejuridiqueidentifiecelui qui l'appose. Elle manifeste le consentement des parties aux obligations qui decoulent de cetacte.

Quandelleestapposee par un officier public, elleconferel'authenticite a l'acte.

« Lorsqu' elleestélectronique, elleconsiste en l'usage d'un procedefiabled'identificationgarantissant son lien avec l'acteauquelelles' attache. La fiabilite de ceprocedeestprésumee, jusquapreuve contraire, lorsque la signature

electroniqueestcreee, l' identite du signataireassuree et l' integrite de l' actegarantie, dans des conditions fixes par decret en Conseild' Etat.»

[13] « Art. 1316. - La preuvelitterale, oupreuve par ecrit, resulted une suite de lettres, de caracteres, de chiffresou de tousautressignesousymbolesdotesd'une signification intelligible, quelsquesoientleur support et leursmodalites de transmission.

[14]«Art. 1316-1. - Lecrit sous formeelectroniqueestadmis en preuve au memetitrequel'ecritsur support papier, sous reservequepuisseetredumentidentifiee la personnedontilémane et qu' ilsoitetabli et conservedans des conditions de nature a en garantirl' integrite.

منابع فارسی

کتب

- حمیدرضا ریاحی و همکاران(۱۳۸۶)، **ترجمه فناوری اطلاعات در مدیریت: دگرگونی سازمان‌ها در اقتصاد دیجیتالی (جلد دوم)**، تهران: انتشارات پیام نور
- جعفری لنگرودی، محمد جعفر(۱۳۸۱)، **مبسوط در ترمینولوژی حقوق (جلد اول)**، تهران: نشر گنج دانش
- دهخدا، علی اکبر(۱۳۸۵)، **فرهنگ متوسط دهخدا**، تهران: موسسه انتشارات و چاپ دانشگاه تهران
- قلی زاده نوری، فرهاد **(۱۳۷۹)، فرهنگ تشریحی اصطلاحات کامپیوتری مایکروسافت (ترجمه)**، تهران: انتشارات کانون نشر علوم
- کاتوزیان، ناصر(۱۳۸۰)، **اثبات و دلیل اثبات (جلد اول)**، تهران: نشر میزان
- کی نیا، محمد(۱۳۸۸)، **امضای الکترونیک منطبق با حقوق فرانسه**، تهران، انتشارات بنیاد حقوقی میزان
- مظاهری کوهانستانی، رسول(۱۳۹۳)، **مطالعه تطبیقی امضای الکترونیکی در حقوق ایران و مقررات آنسیترال**، تهران: انتشارات جنگل
- معین، محمد(۱۳۷۵)، **فرهنگ فارسی معین (جلد دوم)**، تهران، انتشارات امیرکبیر

مقالات

- حیدری، محمد (شهریور۱۳۸۸)، **ارزیابی تهدید امنیتی در عرصه تجارت الکترونیک**، سومین کنفرانس انجمن رمز ایران
- زرکلام، ستار(۱۳۸۲)، **امضای الکترونیکی و جایگاه آن در نظام ادله اثبات دعوی**، مجله مدرس، شماره ۱
- سیامک نوری، محمد حسین فتحیان و ناهید تیتکانلو (آذر۱۳۸۶)، **بررسی نقش عوامل سوم در ایجاد اعتماد در تراکنش‌های تجارت الکترونیک**، چهارمین همایش ملی تجارت الکترونیک
- کریمی،روح الله (اردیبهشت۱۳۸۸)، **تحلیل و ارزیابی روش‌های تولید امضای دیجیتال**، اولین کنفرانس ملی مهندسی نرم افزار ایران

- محمد اصفهانی و مسعود اخوانی فرد (بهمن۱۳۸۷)، **مفهوم اعتماد مشتریان در تجارت الکترونیک و انواع تکنولوژی‌های مربوط**، پنجمین کنفرانس بین‌المللی مدیریت فناوری اطلاعات و ارتباطات

منابع انگلیسی

-Decret no (2001) du 3. Mars 2001 pris pour l application larticle 1316-4: du code et relative a la signature electronoque

-Michael Chissik, AlisterKelman,(2001) **Electronic Commerce: Law and practice,** 3-De Lamberterie, Isaballe et Blanchette, Jean- Francois. Le decret du relatif a la signature electronique, lecture critique, technique etjuridique, 3 Mars

-DIRECTIVE (1999/93/)EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures

-DIRECTIVE (2000/31/)EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)

-Garner, A, Brayan.(2000). Black's Law Dictionary. Tehran: Dadgostar.

-KAINIYA, Mohammad. (2008).**LA SIGNATURE ELECTRONIQUE, Mémoire pour le master 2 de droitnotariat**. Université Jean-Moulin Lyon III

-KAINIYA, Mohammad.(2011**). La dématérialisation des acteset conventions** (de l'expériencefrancaise à saréception par le droitiranien?), Thèse de doctorat. Université Jean-Moulin Lyon3.

-Turban, Efraim(2008), Leidner, McLean, Dorothy , Ephraim , Wetherbe, James, **Information Technology for Management: Transforming Organizations in the Digital Economy**, Wiley, 6th Edition

- Floyd, Brian (2007),**The Information Security Writers group**, The Changing Face of Network Security Threats" (http://www.infosecwriters .com/text_ resources/pdf/ Network_Security_Threats_BFloyd.pdf)

-Information_security(2010), available at: http://en.wikipedia.org/wiki/Info-rmation security, March

-MehrnooshTorabi, KareshnaZamani(2010), **Mobile Banking and its security issues,** 5th international Conference on e-Commerce in Developing Countries: with focus on export, September

-Venter, H.S., Eloff, J.H.P.,(2003), **A taxonomy for information security technologies,** Elsevier, p.300, 0167-4048/03

-Piotr Bilski (2010), **Wiesław Winiecki, Multi-core implementation of the symmetric cryptography algorithms in the measurement system**,Measurement,43, 1050- 1051
-Lopeza Javier (2004), **Oppliger Rolf, Pernul Gunther, Authentication and authorization infrastructures** (AAIs): a comparative survey, Computers & Security, vol. 23
-Srivastava, A.,(2009), **Electronic signatures and security issues: An empirical study,** Computer law and security review 25, 442-445
-Description of Symmetric and Asymmetric Encryption, Revision: 1.3, October 26, 2007.(http://support.microsoft.com/kb/246071)
-Shoup, Victor (2004), **FCD 18033-2 Encryption algorithms-Part 2: Asymmetric ciphers**,Instructor of New York University, Faculty of computer science ,December 6.(http://www.shoup.net/iso/std6.pdf)
-Hardjono, Thomas(2005), **Dondeti, Lakshminath R., Security In Wireless LANS And MANS**, Artech House
-Torrubia, Andres, Mora, Francisco J., Marti, Luis(2001), **Cryptography Regulations for E-commerce and Digital Rights Management**, Computers & Security Vol.20, No.8