رمزنگاری نامتقارن گواهی امضای الکترونیکی معبر تجارت الکترونیک

امیر جهانگرد محبوب[۱]

اشاره:

شتاب روزافزون تولید فن‌آوری‌های پیشرفته موجب سرعت و افزایش حجم مبادلات تجاری و فشردگی رقابت‌ها شده است و در بستر شبکه جهانی اینترنت، حجم عظیم آبشار هول‌انگیز اطلاعات هویتی و تبادلات جدید مالی را به اقیانوس بیکران داده‌های پیشین فرو می‌ریزد. از سوی دیگر، توسعه این تبادلات نو، در فضایی امن و ایمن، امکان جعل، تزویر و کلاهبرداری را به شدت کاهش داده است. معضلاتی که چگونگی مواجهه با آن‌ها پاشنه آشیل عمده نظامات حقوقی پیشین به‌شمار می‌رفت و تنظیم روابط چالش برانگیز اشخاص به خصوص آنجا که حوزه مالکیت‌ها و تعهدات چون کوه یخی سر بر می‌آورد همواره دغدغه اندیشمندان بوده است.

هویت و مالکیت

از آن روی که هویت و مالکیت، این دو بال مرغ حق، هرگز از گزند بداندیشان و مجرمان در امان نمانده‌اند، قانون‌گذار، طی مواد ۹۹۲ ق.م. و ۳۶ ق.ث. شناسنامه را ملاک

۱. سردفتر دفتر اسناد رسمی شماره ۱۲۴۷ تهران.

تعیین هویت اشخاص معرفی نموده و با تبیین علاقه‌های اشخاص نسبت به اموال در ماده ۲۹ ق.م. (مالکیت بر عیون و منافع، حقوق عینی تبعی، حق انتفاع و حق ارتفاق به ملک غیر) همت خود را معطوف بر تعریف مالکیت گمارده بود.

اما در دنیای مدرن، هنگامی که چرخه‌های بازرگانی (موسوم به PESA) تکرار می‌شوند، مبادله الکترونیکی داده‌ها موجب کاهش هزینه‌ها، ریسک معاملات، بهبود کیفیت مبادله و افزایش سرعت تولید می‌گردد. در بخش تولیدی، تولید به‌هنگام (***Just In Time***) و در بخش خدماتی، سرعت، ایمنی و گسترش خدمات بانکی و حاکمیتی را فراهم می‌آورد و هویت با شتاب و امنیت بالا، تعیین و شناسایی و مالکیت منتقل می‌گردند.

مشارکت در بهره‌برداری از اطلاعات، بیع و شراء، تبلیغ، بازاریابی و سنجش بازار از طریق رایانه را تجارت الکترونیک می‌نامند که ابزار، روش، اعتبارات، اصطلاحات و بالتبع نظام حقوقی خود را دارا است، بنابراین توسعه تجارت الکترونیکی صرفاً تحت تأثیر گسترش فن‌آوری نیست و کاملاً به توسعه و تبیین ابعاد حقوقی آن وابسته است. امری که در مقررات متحدالشکل جهانی نظیر استاندارد ISOx ۰۹۰۵ برای مراجع تصدیق و استاندارد جهانی پرداخت (***Secure Electronic Trasuction***) مورد توجه قرار گرفته است. وجود ضمانت اجرا و حمایت‌های حرفه‌ای برای واسطه‌های دیجیتالی (***Intermediary Digital***) در قوانین مربوطه، شناسایی دارایی مادی الکترونیکی نظیر چک الکترونیکی (***Netcheque***)، پول الکترونیکی (***Cybercash***)، کارت اعتباری (***Creditcard***) و کیف پول الکترونیکی (***Digital Wallet***) و نیز شناسایی دارایی‌های معنوی الکترونیکی و پذیرش اسناد الکترونیکی در مراجع قضایی منوط به تعیین مراجع احراز هویت و صدور گواهی امضای دیجیتالی می‌باشد.

پیشینه حقوق تجارت الکترونیک در ایران

اوایل اردی‌بهشت ماه سال ۱۳۸۲، قانون تجارت الکترونیکی از تصویب مجلس شورای اسلامی گذشت. این قانون مشتمل بر ۷۹ ماده و شش باب اصلی بود که عبارتند از: ۱ ـ مقررات عمومی ۲ ـ دفاتر خدمات صدور گواهی الکترونیکی ۳ ـ قواعد مختلفه

۴ ـ جرایم و مجازات‌ها ۵ ـ جبران خسارت ۶ ـ متفرقه. پیش‌تر در ۲۹ مرداد ماه ۱۳۸۱ دولت جمهوری اسلامی ایران به استناد اصل ۱۳۸ ق.ا.، سیاست تجارت الکترونیکی را تصویب و وظایف مربوط به پیگیری مسایل آن را به وزارت‌خانه‌های بازرگانی، علوم، تحقیقات و فن‌آوری و هم‌چنین ارتباطات و فن‌آوری اطلاعات واگذار نمود. تبصره ۸ ماده ۳ سیاست تجارت الکترونیکی ج.ا.ا. اعلام می‌دارد؛ کلیه وزارت‌خانه‌ها، سازمان‌ها و شرکت‌های دولتی موظف‌اند نسبت به راه‌اندازی سیستم تجارت الکترونیکی در مبادلات خارجی خود اقدام کنند و تا پایان برنامه توسعه سوم حداقل نیمی از مبادلات خارجی خود را به این روش انجام دهند. هم‌چنین تبصره ۳ ـ ۴ ماده ۳ سیاست‌نامه مذکور، وزارت بازرگانی را در محدوده زمانی برنامه توسعه سوم موظف به ایجاد مراجع صدور گواهی دیجیتال در کشور مطابق با استانداردهای مقبول جهانی نموده است.

مراجع تصدیق

وقتی گواهی تولد و گواهی فوت از سوی بیمارستان یا دیگر مراجع ذی‌ربط صادر می‌گردد، سازمان ثبت احوال اقدام به اصدار یا ابطال شناسنامه هویت می‌نماید. بنابراین موجودیت ثبت می‌شود و تا زوال امتداد آن، معتبر می‌ماند. هنگامی‌که متعاملین معاملهٔ ملکی یا طرفین قرارداد اقدام به تنظیم و ثبت آن در دفتر اسناد رسمی می‌نمایند، سند رسمی صادر می‌شود که قابل انکار یا تردید نخواهد بود. دفاتر اسناد رسمی، سازمان ثبت اسناد و املاک کشور و سازمان ثبت احوال مراجع تصدیق حاکمیتی برای هویت و مالکیت‌اند که مدارک صادره توسط ایشان دراین‌باره قابل استناد و استعلام و پایدار می‌باشد، اما همواره امکان ارائه اطلاعات نادرست و جعلی به این مراجع تصدیق وجود دارد. وظیفه مرجع تصدیق در محیط مجازی و داد و ستد رایانه‌ای یا مراجع صدور گواهی دیجیتال (***Certification Service Provider***) صدور گواهی امضای الکترونیکی است. چنان‌که ماده ۳۱ قانون تجارت الکترونیکی CSP را واحدهایی تعریف می‌کند که برای صدور امضای الکترونیکی در کشور تأسیس می‌شود. این خدمات در هفت مورد بر شمرده می‌شود: ۱ و ۲: تولید و صدور ۳ و ۴: ذخیره و ارسال ۵ و ۶: تأیید و ابطال ۷: به روز

نگهداری گواهی‌های اصالت امضای الکترونیکی. در شمای کلی، مرجع اصلی توسط دولت ایجاد می‌شود. این مرجع بنیادی (***Root Certification Authority***) می‌تواند ده‌ها زیرمجموعه (***Authority Sub Certification***) داشته باشد که به دنبال آن هزاران مرجع وابسته (***Registration Authority***) را پوشش دهد.

تفاهم‌نامه منعقده میان وزارت بازرگانی و کانون سردفتران و دفتریاران در این مسیر، امکان اخذ گواهی امضای الکترونیکی را برای دفاتر اسناد رسمی فراهم می‌سازد.

امضای الکترونیکی مطمئن

امضای الکترونیکی مطمئن (***Secure Electronic Signature***) از دو کلید عمومی و خصوصی تشکیل شده است. این دو کلید را می‌توان به دو رشته DNA (اسید دزوکسی ریبو نوکلئیک) تشبیه نمود. دو رشته اسیدهای DNA که بازهای آلی آدنین، گوانین، تیمین و سیتوزین، آن دو را به هم پیوند می‌دهند مانند دو کلید متشکل از حروفی که دو به دو با هم متناظرند، یک بسته اطلاعات ژنتیکی را می‌سازند که مبین خصوصیات مختلف جسمی و روانی فرد می‌باشند. الگوریتم کلید عمومی در نقطه مقابل، ترتیب رمز کلید خصوصی است. چنانچه واژه حق را متناظر دو عدد قرار دهیم یعنی ح=۱ و قاف=۲ ترتیب ۱ و ۲ ما را به عبارت حق می‌رساند و بالعکس. چنین اتفاقی در فرآیند رمزنگاری (***Cryptography***) رخ می‌دهد. رمزنگاری یا فرآیند ایجاد کلید عمومی و خصوصی به دو روش متقارن و نامتقارن صورت می‌پذیرد.

رمزنگاری متقارن

در روش متقارن طرفین رمزی را به‌عنوان کلید مشترک میان خود انتخاب و ضمیمه داده پیام خود می‌نمایند. بند ،"الف" ماده ۲ از فصل دوم ق.ت.ا. داده پیام (***Data Masage***) را هر نمادی از واقعه، اطلاعات یا مفهوم تعریف می‌کند که با وسایل الکترونیکی، نوری یا فن‌آوری‌های جدید اطلاعات، تولید، ارسال، دریافت یا پردازش می‌شود. در رمزنگاری متقارن، هر شخص در ارتباط با بی‌نهایت اشخاص باید بی‌نهایت کلید مشترک لحاظ کند و صحت امضا در نهایت منوط به شناخت قبلی طرفین از یکدیگر

است و راهی به اطلاعات حقیقی افراد بدون شناخت قبلی نمی‌گشاید. علاوه‌بر آن همواره این مسأله وجود دارد که در صورت فاش شدن کلمه رمز، اطلاعات سند برای هرکس قابل استفاده و تغییرات آن قابل تأیید باشد.

رمزنگاری نامتقارن

روش معمول و معقول رمزنگاری که ایرادات روش قبل را ندارد، رمزنگاری نامتقارن است. در رمزنگاری نامتقارن، مرجع تصدیقی وارد عمل می‌شود که مورد قبول طرفین است و فرآیند رمزنگاری و بهره‌برداری از آن را با طراحی و ایجاد زیرساخت کلید عمومی (***Public Key Infrastructure***) و خدمات مراجع وابسته به خود سامان می‌دهد تا اشخاص هنگامی که قصد ارسال داده پیامی را دارند بتوانند با کلید خصوصی خود آن را رمز (***Encrypt***) نموده و دریافت‌کننده به وسیله کلید عمومی آن را رمزگشایی (***Decrypt***) نماید. روش‌های مختلف این‌گونه رمزنگاری (چون ***RFA، CHA، RCA، TLS***) از امنیت، سرعت و سهولت بالاتری نسبت به روش سنتی امضای اسناد برخوردار هستند و امکان جعل، اگرچه غیرممکن نیست اما تاکنون ممکن نشده است.

اقامتگاه

بند "ز" ماده ۲ فصل ۲ ق.ت.ا. سیستم اطلاعاتی (***Information System***) را سیستمی برای تولید، ارسال، دریافت، ذخیره یا پردازش داده پیام تعریف می‌نماید. اگرچه هنوز تا شکل‌گیری و استقبال لازم از تجارت الکترونیک در کشور راهی طولانی پیش رو است و اکنون ایجاد خدمات الکترونیک حاکمیتی به مردم در اولویت دست‌اندرکاران است، اما توجه به برخی ابعاد حقوقی این تجارت مانند مسأله اقامتگاه امری ضروری به‌نظر می‌رسد. چرا که سیستم‌های اطلاعاتی ممکن است ثابت یا متحرک باشند. بنابراین در تجارت الکترونیکی، قانون باید اقامتگاه را به شکلی متفاوت با روش‌های سنتی تعریف نماید. چنان‌که قانون تجارت الکترونیک عنوان می‌نماید اگر محل استقرار سیستم اطلاعاتی با محل استقرار دریافت داده پیام یکسان باشد، آن محل اقامتگاه مخاطب محسوب می‌شود. اما اگر این دو متفاوت باشند، محل تجاری یا کاری اصل‌ساز اقامتگاه محسوب می‌شود.

بند "ب" ماده ۲ فصل ۲ ق.ت.ا.، اصل‌ساز (***Originator***) را منشأ اصلی تولید و ارسال‌کننده پیام الکترونیکی عنوان می‌نماید. و محل دریافت متقابل را نیز همان اصل‌ساز تعیین می‌نماید. اگر اصل‌ساز یا مخاطب فاقد محل کاری و تجاری معین باشند، مطابق ماده ۲۹ ق.ت.ا. اقامتگاه قانونی آن‌ها ملاک عمل خواهد بود.

خاتمه

برابر ماده ۴۹ ق.ث.ا. مصوب ۱۳۱۰/۱۲/۲۶، مرجع صدور گواهی صحت امضا و سواد مصدق و ثبت اسناد در ایران، نهادهای حاکمیتی دفاتر اسناد رسمی هستند که اکنون در بازاری که به گستردگی کره خاکی است به‌عنوان مرجع ارائه خدمات گواهی امضای الکترونیکی وارد عرصه‌ای نوین می‌شوند. آینده، از آن کشورهایی است که با قدرت دانش و دوراندیشی نظام حقوقی خود، اعتماد و اعتبار بیشتری را در این بازار گسترده فراهم کنند. چنان‌که ماده ۳ از فصل ۳ قانون تجارت الکترونیکی ایران اشعار می‌دارد؛ در تفسیر این قانون، همواره باید به خصوصیت بین‌المللی، ضرورت هماهنگی بین کشورها در کاربرد آن و رعایت لزوم حسن نیت توجه کرد.

منابع:

۱ ـ ***مجموعه مقالات اولین همایش آینده اینترنت و تجارت الکترونیکی در ایران***، اسفندماه ۱۳۷۹، دانشگاه صنعتی شریف.

۲ ـ بنی فیضی چکاب، غلام، ***وضعیت حقوقی و قانونی تجارت الکترونیکی در جهان و ایران***، دانشگاه علامه طباطبایی.

۳ ـ سیاست تجارت الکترونیکی جمهوری اسلامی ایران، جلسه مورخ ۱۳۸۱/۲/۲۹، هیئت وزیران و گزارش توجیهی سیاست تجارت الکترونیکی مصوب کمیسیون تخصصی اطلاع‌رسانی اقتصادی، بازرگانی و تجارت الکترونیکی.

۴ ـ نوری، محمدعلی؛ نخجوانی، رضا، ***حقوق تجارت الکترونیکی***، گنج‌دانش، ۱۳۸۲، با همکاری کمیته مطالعات و فن‌آوری وابسته به دفتر همکاری فناوری ریاست جمهوری.

۵ ـ نیک بخش تهرانی، محمدحسن؛ آذر صابری، مهدی، ***تجارت الکترونیکی و زیرساخت‌های آن***، انیستیتو ایز ایران، ۱۳۸۰.

۶ ـ ***قانون تجارت الکترونیک***، مصوب ۱۳۸۲/۱۰/۱۷.

۷ ـ ***قانون مدنی***.