جعل رایانه‌ای در بستر تجارت الکترونیکی

دکتر علی‌مراد حیدری*

چکیده: جعل رایانه‌ای موضوع ماده ۶۸ قانون تجارت الکترونیکی است. از حیث رکن مادی، ورود، تغییر، محو و توقف داده‌پیام و مداخله در پردازش داده‌پیام و مداخله در پردازش داده‌پیام و سیستم‌های رایانه‌ای، و یا استفاده از وسایل کاربردی سیستم‌های رمزنگاری تولید امضاء- مثل کلید اختصاصی- بدون مجوز امضاء کننده و یا تولید امضای فاقد سابقه ثبت در فهرست دفاتر اسناد الکترونیکی ویا عدم انطباق آن وسایل با نام دارنده در فهرست مزبور و اخذ گواهی مجعول و نظایر آن رفتارهای فیزیکی و داده‌پیام دارای ارزش مالی و اثباتی موضوع جرم و قابلیت استناد در مراجع اداری، مالی و قضایی نتیجه جرم است که در صورتی که متهم با آگاهی و اراده و به قصد استناد در مراجع گفته شده رفتارهای مذکور را انجام دهد جاعل رایانه‌ای محسوب و به یک تا سه سال حبس و پرداخت جزای نقدی به میزان پنجاه میلیون ریال محکوم می شود. با وجود تصویب قانون جرایم رایانه‌ای و اختصاص ماده ۶ این قانون به جعل رایانه ای، جعل رایانه‌ای در بستر مبادلات الکترونیکی به جهت موضوع خاص خود هم چنان مشمول ماده ۶۷ قانون تجارت الکترونیکی است.

واژگان کلیدی: جعل، جعل رایانه ای، مبادلات الکترونیکی، تجارت الکترونیکی

*. استادیار دانشگاه حضرت معصومه علیها السلام E mail: Heydarilaw@gmail.com

مقدمه

جعل در مفهوم سنتی خود، بزهی بر ضد اصالت و صحت اسناد و نوشته‌هاست و بر خلاف کلاه برداری به منظور تحصیل مال یا امتیاز مالی ارتکاب نمی یابد بلکه غالباً با هدف دست کاری در اسناد و ادله قضایی و به منظور تغییر در مدارک و اسناد و تقلب در آن به کار می‌رود. در محیط رایانه و فضای سایبری نیز این بزه، با حفظ ماهیت وجودی سنتی خود، "اصالت" و "صحت" داده‌ها و سامانه‌های رایانه‌ای را نشانه گرفته است. از این روی جرم مذکور در فصل دوم قانون جرایم رایانه‌ای ذیل عنوان " جرایم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی" درج گردیده است؛ در مورد عنوان فصل مذکور باید دانست گرچه صحت و تمامیت به اندازه‌ای با هم همسان هستند که در کنار یکدیگر به عنوان یک اصل بنیادین برای امنیت رایانه بکار رفته اند، لکن این دو واژه معنای واحدی ندارند و اصل صحت برای پشتیبانی از ناب‌مندی (اصالت و قابلیت استناد) است ولی تمامیت برای هست‌مندی (موجودیت) و نیز صحت بیشتر ویژگی داده است ولی تمامیت هم بر داده روی می‌کند و هم بر سا

مانه. از سوی دیگر تفاوت این دو با اصل محرمانگی در این است که ارزش صحت و تمامیت برای خود داده و سامانه است ولی ارزش محرمانگی برای دارنده آنها؛ از این روی، محرمانگی داده و سامانه، ارزشی پسینی در سنجش با صحت و تمامیت آنهاست (عالی پور، ۱۳۹۰، ص ۱۹۷)

در مقام مقایسه جعل سنتی با جعل رایانه‌ای باید در نظر داشت که آن چه جعل رایانه‌ای را از جعل سنتی متمایز می‌کند وقوع آن در بستر فضای سایبر است و نه صرف استفاده از رایانه به عنوان وسیله ارتکاب جرم. بنابراین، رفتارهای موضوع جعل رایانه‌ای ضرورتاً باید از رهگذر کنش‌های رایانه‌ای و در بستر رایانه و مخابرات انجام شود. از این روی، اگر کسی داده رایانه‌ای موجود در محیط ورد را چاپ کند و سپس بر روی مطالب کاغذ چاپ شده، تغییری پدید آورد، جعل رایانه‌ای نخواهد بود. در نقطه مقابل، اگر کسی سندی مکتوب ساخته یا آن را تغییر

دهد و سپس با اسکن نمودن و تبدیل آن به داده رایانه‌ای آن را به اشـخاص حقیقـی یا حقوقی ارائه نموده و به آن استناد نماید باز هم جعل انجام شده، سنتی خواهد بود چرا که عمل ساخت یا دگرگـونی از رهگـذر کـنش و پـردازش رایانـه‌ای صـورت نپذیرفته است.

در این نوشتار مطلـق جعـل رایانـه‌ای مـد نظـر نیـست بلکـه بررسـی جـرم جعـل رایانه‌ای در بستر مبادلات الکترونیکی مورد توجه نگارنده است کـه دامنـه موضـوع آن حتی محدودتر از جعل رایانه‌ای است. بدین منظور و به پیـروی از شـیوه متـداول نوشته‌های حقوق جزایی و هماننـد مقالـه "کـلاه بـرداری رایانـه ای" کـه در شـماره پیشین همین نشریه به چاپ رسید، بررسی جـرم "جعـل رایانـه‌ای در بـستر مبـادلات الکترونیکی" نیز به عنوان بخشی از طـرح کلـی "جـرایم تجـارت الکترونیکـی" در قالب ارکان سه گانه صورت می گیرد.

مبحث اول: رکن قانونی

مبنای قـانونی جعـل رایانـه‌ای در تجـارت الکترونیکـی مـاده ۶۸ قـانون تجـارت الکترونیکـی مـصوب ۱۳۸۲/۱۰/۱۷ اسـت کـه در مبحـث دوم از بـاب جـرایم و مجازات‌ها تحت عنـوان جعـل کـامپیوتری مقـرر داشـته اسـت: "هـر کـس در بـستر مبادلات الکترونیکی، از طریق ورود، تغییـر، محـو و توقـف داده پیـام و مداخلـه در پردازش داده پیام و سیستم های رایانه ای، و یا اسـتفاده از وسـایل کـاربردی سیـستم های رمز نگاری تولید امضاء -مثل کلید اختصاصی- بدون مجوز امضاء کننـده و یـا تولید امضای فاقد سابقه ثبت در فهرست دفاتر اسناد الکترونیکـی و یـا عـدم انطبـاق آن وسایل با نام دارنده در فهرست مزبور و اخذ گواهی مجعول و نظایر آن اقدام بـه جعل داده پیام های دارای ارزش مالی و اثباتی نماید تا با ارائه آن بـه مراجـع اداری، قضائی، مالی و غیره به عنوان داده پیام های معتبر استفاده نمایـد، جاعـل محـسوب و به مجازات حبس از یک تا سه سال و پرداخت جزای نقدی به میـزان پنجـاه میلیـون (۵۰/۰۰۰/۰۰۰) ریال محکوم می شود.

تبصره – مجازات شروع به این جرم حداقل مجـازات در ایـن مـاده مـی باشـد." (روزنامه رسمی،۱۳۸۲، ش۱۷۱۶۷)

در مورد ماده ۶۸ باید دانست که شورای عالی انفورماتیک در "گزارش توجیهی طرح قانونی جرایم کامپیوتری"(وزارت بازرگانی، ۱۳۸۰، ص۱۰۳) که بعداً مبنای تدوین ماده ۶۸ قرار گرفت، منابع اصلی این ماده را بدین شرح اعلام کرده است:

الف) ماده پیشنهادی در فهرست حداقل شورای اروپا بدین عبارت که: "جعل کامپیوتری ورود، تغییر، پاک کردن یا متوقف سازی داده‌های کامپیوتری یا برنامه‌های کامپیوتری یا هر گونه مداخله دیگر در پردازش داده‌ها به شیوه یا تحت شرایطی همان طور که در قوانین ملی تشریح شده است جرم جعل را تشکیل می‌دهد، مشروط بر این که با توجه به هدف مرسوم، چنین جرمی ارتکاب یافته باشد."

ب) ماده ۲۶۹ کد جزایی آلمان بدین مضمون که: "هر کس به قصد تقلب در یک عمل قضایی داده‌های دارای ارزش اثباتی را ذخیره کند یا تغییر دهد، به گونه‌ای که سند دروغین و جعلی تلقی شود، یا چنین داده‌های ذخیره یا تغییر داده شده‌ای را استفاده کند، به حبس تا ۵ سال یا جزای نقدی محکوم خواهد شد. شروع به این جرم نیز قابل مجازات است."

همان گونه که مشاهده می‌گردد در ماده پیش نهادی شورای اروپا نوع داده موضوع جرم تعیین نشده است و اعمال یاد شده نسبت به هر داده‌ای که ارتکاب یابد جرم تلقی می‌شود. در قانون جزای آلمان نیز قلمرو شمول ماده به داده‌های دارای ارزش اثباتی در مبادلات قضایی محدود شده است. اما در ماده ۶۸ ق.ت.ا. داده‌ها و اطلاعات دارای ارزش مالی و قابل اثبات و استناد در مراجع اداری، قضایی و مالی موضوع جرم قرار گرفته یعنی چنان چه داده موضوع جعل دارای ارزش اثباتی نزد مراجع قضایی باشد اما ارزش مالی نداشته باشد، بزه جعل تحقق نیافته است (جاویدنیا،۱۳۸۷،ص ۲۹۰)

از سوی دیگر ماده ۶ قانون جرایم رایانه‌ای مصوب ۱۳۸۸/۳/۵ مجلس شورای اسلامی نیز مبنای قانونی عام جعل رایانه‌ای است. در فصل دوم این قانون زیر عنوان جرائم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی مقرر گردیده: "هر کس به طور غیرمجاز مرتکب اعمال زیر شود، جاعل محسوب و به

حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون (۲۰,۰۰۰,۰۰۰) ریال تا یکصد میلیون (۱۰۰,۰۰۰,۰۰۰) ریال یا هر دو مجازات محکوم خواهدشد:

الف) تغییر یا ایجاد داده‌های قابل استناد یا ایجاد یا واردکردن متقلبانهٔ داده به آنها؛

ب) تغییر داده‌ها یا علائم موجود در کارتهای حافظه یا قابل پردازش در سامانه‌های رایانه‌ای یا مخابراتی یا تراشه‌ها یا ایجاد یا وارد کردن متقلبانهٔ داده‌ها یا علائم به آنها.

ماده۷ـ هرکس با علم به مجعول بودن داده‌ها یا کارتها یا تراشه‌ها از آنها استفاده کند، به مجازات مندرج در ماده فوق محکوم خواهدشد." (روزنامه رسمی،۱۳۸۸، ش۱۸۷۴۲)

این ماده با عنایت به ماده ۷ کنوانسیون جرایم سایبری ۲۳ نوامبر ۲۰۰۱ بوداپست شورای اروپا تدوین یافته که زیر عنوان جرایم مرتبط با رایانه چنین آورده است: "هر یک از اعضا باید به گونه‌ای اقدام به وضع قوانین و مقررات نماید که در صورت لزوم براساس حقوق داخلی خود، هر نوع وارد کردن، تغییر، حذف یا قطع عمدی و غیرحق داده‌های رایانه‌ای را که منجر به ایجاد داده‌های غیر معتبر می‌شود با همان قصدی که از آن انتظار می‌رفت یا در راستای اهداف غیرقانونی به عنوان داده‌هایی که از اعتبار کافی برخوردارند، به کار گرفته می‌شوند، چه این داده‌ها به طور مستقیم قابل درک و خواندن باشند چه نباشند، جرم انگاری نماید. عضو مورد نظر مقرر دارد که وجود قصد فریب یا دیگر مقاصد ناروا پیش از اتصاف مسؤولیت کیفری لازم و ضروری است."

در مورد رابطه این دو ماده و اعتبار ماده ۶۸ ق.ت.ا. باید دانست که در ماده ۵۶ قانون جرایم رایانه‌ای اعلام شده که قوانین و مقررات مغایر با این قانون ملغی است. در نسخه اولیه این قانون بطور خاص تصریح شده بود که مواد ۶۷ و ۶۸ قانون تجارت الکترونیکی در مورد کلاه برداری و جعل کامپیوتری نسخ شده است لکن در متن نهایی فقط به نسخ عام ماده ۵۶ اکتفاء شد و این عمل موجب شد در مورد اعتبار مواد ۶۷ و ۶۸ قانون تجارت الکترونیکی بین محققان اختلاف نظر پیش آید؛ به گونه‌ای که بعضی معتقدند ماده ۶۸ نسخ شده است چون این ماده عملاً درباره

همه جعل‌های رایانه‌ای است، افزون بر این تعبیرهای به کـار رفتـه در مـاده ۶۸ ماننـد بستر مبادلات الکترونیکی و جعل کامپیوتری نشان دهنده این اسـت کـه یـک مـاده کلی بوده و بنابراین با تصویب ماده ۶ قانون جرایم رایانه‌ای نسخ شده است. جـدا از این با کشف دیدگاه قانون گذار نیز می‌توان نسخ صریح ماده‌های ۶۷ و ۶۸ پـی بـرد و آن این که نسخ این دو به روشنی در متن لایحه بوده و برداشـتن آن در گـام‌هـای پسینی نه بـه جهـت نپـذیرفتن آن کـه بـه جهـت بـس بـودن تعبیـر نـسخ کلـی بـوده است(عالی پور، ۱۳۹۰، ص ۳۹۰)

از دید نگارنده قول به نسخ مواد ۶۷ و ۶۸ ق.ت. ا. درست نیست و گرچه قـانون جرایم رایانه‌ای از حیث زمان تصویب مؤخر بـر قـانون تجـارت الکترونیکـی اسـت، لکن از حیث دامنه شمول دو ماده با هم متفاوتند و همان گونه که در هر دو ماده ۶۷ و ۶۸ تصریح شده، وقوع جرایم کلاه برداری و جعل در قانون تجارت الکترونیکـی – بر خلاف آن چه گفته شده–، نه یک ماده کلی، بلکه محدود بـه "بـستر مبـادلات الکترونیکی" و در فضای تجارت الکترونیکی است در حالی که قلمرو شـمول مـاده ۶ قانون جرایم رایانه‌ای مطلق داده‌ها و سامانه‌های رایانه‌ای و مخابراتی اسـت اعـم از این که در بستر مبادلات الکترونیکی بین تامین کننده و مصرف کننده واقع شـود یـا در عملیات غیر تجاری در فضای سایبر یا در فضای خارج از سایبر و در یک شـبکه داخلی یا یک سیستم رایانه‌ای منفرد. به بیان دیگر قانون تجارت الکترونیکی خـاص و قانون جرایم رایانه‌ای عام است و پر واضح اسـت کـه در چنـین مـواردی، خـاص مقدم به اعتبار خود باقی و عام موخر را تخصیص می‌زنـد و بـه نظـر مـی‌رسـد عـدم تصریح به نسخ مواد ۶۷ و ۶۸ قانون تجارت الکترونیکی در متن نهایی قـانون جـرایم رایانه‌ای و به بیان بهتر حذف تصریح به نسخ این دو ماده به جهت بقای اعتبـار مـواد دو گانه در قلمرو خاص خود بوده است و نه به جهت بـس بـودن تعبیـر نـسخ کلـی! بنابراین، رکن قانون جرم جعل رایانـه‌ای در بـستر مبـادلات الکترونیکـی، هـم چنـان ماده ۶۸ قانون تجارت الکترونیکی است. با وجود ایـن، در مـوارد لازم مقایـسه بـین ماده ۶۸ ق.ت.ا. و ماده ۶ ق.ج.ر. از یاد نخواهد رفت.

یادآوری این مطلب نیز ضروری است که بطور کلی اولـین مـتن قـانونی کـه در کشور ما ارتکاب جرایم رایانه‌ای را مـورد توجـه قـرار داد، قـانون مجـازات جـرایم

نیروهای مسلح مصوب ۱۰/۹/ ۱۳۸۲ بود. ماده۱۳۱ این قانون مقرر نموده است: "هرگونه تغییر یا حذف اطلاعات ، الحاق ، تقدیم یا تاخیر تاریخ نسبت به تاریخ حقیقی و نظایر آن که به طور غیرمجاز توسط نظامیان در سیستم رایانه و نرم افزارهای مربوط صورت گیرد و همچنین اقداماتی از قبیل تسلیم اطلاعات طبقه بندی شده رایانه ای به دشمن یا افرادی که صلاحیت دسترسی به آن اطلاعات را ندارند، افشاء غیرمجاز اطلاعات، سرقت اشیاء دارای ارزش اطلاعاتی مانند سی دی یا دیسکتهای حاوی اطلاعات یا معدوم کردن آنها یا سوء استفاده های مالی که نظامیان به وسیله رایانه مرتکب شوند جرم محسوب و حسب مورد مشمول مجازاتهای مندرج در مواد مربوط به این قانون می باشند." هر چند ماده ۳۱ انواع مصادیق جرایم رایانه‌ای را از هم تفکیک نکرده با این حال "تغییر یا حذف اطلاعات ، الحاق ، تقدیم یا تاخیر تاریخ نسبت به تاریخ حقیقی و نظایر آن" شامل جعل رایانه‌ای و "سوء استفاده های مالی" ناظر به کلاه برداری رایانه‌ای است (حیدری، ۱۳۹۰، ص ۶۷)

مبحث دوم: رکن مادی

اجزای رکن مادی جعل رایانه‌ای – شامل رفتار مادی، موضوع جرم و نتیجه[۱]- به شرح زیر مورد بررسی قرار می گیرد:

رفتار مادی

مصادیقی که در ماده ۶۸ به عنوان رفتارهای محقق جعل مورد تصریح قرار گرفته عبارتند از:

ورود داده پیام: جعل از طریق وارد کردن داده‌ها به سیستم رایانه ای، شایع ترین روش جعل و تنها رفتار ویژه جعل رایانه‌ای است که در جعل سنتی پیش بینی نشده

۱- . در مورد جزء دیگر رکن مادی یعنی مرتکب جرم یادآوری می‌شود که مرتکب جرم جعل رایانه ای نیز همانند کلاه برداری رایانه ای "هر کس" است که در مورد مسئولیت کیفری شخص حقیقی و حقوقی در مقاله پیشین مطالبی بیان شد که به جهت مشترک بودن این بحث از تکرار آن خودداری شده و خواننده محترم به مطالعه مقاله نگارنده در شماره قبلی این مجله در مورد کلاه برداری رایانه ای توصیه می‌شود.

است. سهولت ارتکاب جعل رایانه‌ای از طریق وارد کردن داده بدین جهت است که سخت افزار رایانه با توجه به برنامه‌های منطقی از پیش طراحی و معرفی شده بطور خودکار هر گونه اطلاعات دریافتی را مطابق همان نظم منطقی تعریف شده و بدون توجه به واردکننده داده و صرف نظر از پیامدهای آن پردازش می‌کند. در قلمرو مبادلات الکترونیکی نیز یکی از رایج ترین شیوه‌های جعل رایانه ای، جعل نامه‌های الکترونیکی است که ارسال آن از طریق پست الکترونیکی در بسیاری از موارد منتهی به کلاه برداری نیز می‌شود. این موضوع به این دلیل است که رایانه‌های مورد اعتماد بسیاری در اینترنت وجود دارند که به اشخاص امکان می‌دهند که به آن‌ها وصل شده و پست الکترونیکی جعلی ایجاد کنند. بسیاری از سوداگران این حقیقت را دریافته اند و با بازپخش پست الکترونیکی ناخواسته ی بی استفاده، از این سیستم‌ها سوء استفاده می‌کنند. این پست الکترونیکی بی استفاده هرزنامه[1] نامیده شده است. برای درک فرایند جعل پیام الکترونیکی، دانستن چگونگی استفاده از تل نت[2] و درک چگونگی تبادل پیام با ام تی ای‌ها سودمند است. تل نت پیمان ساده ولی قدرت مندی است که به اشخاص امکان می‌دهد که به یک میزبان راه دور وصل شده و فرمان هایی را تایپ کنند گویی که صفحه کلید آنان به طور مستقیم به آن سیستم متصل شده و از آن سوء استفاده کنند، مشروط بر آن که از زبان مورد استفاده ان آگاهی داشته باشند. (کیسی،۱۳۸۶، ص۱۸۳) هم چنین انقلاب دیجیتال به تبهکاران امکان جعل شماره کارت‌های اعتباری به واسطه برنامه هایی را داده است که شماره کارت‌های یک بانک معین را با تجهیز کامپیوتر به عدد خاص بانکِ صادر کننده کارت، جعل می‌نماید. به علاوه امکان دریافت این شماره‌ها از طریق شَبکه‌های بازِ اینترنت و به کارگیری آن به شیوه‌ای غیرقانونی در عملیات خرید از خلال شبکه را می‌دهد به گونه‌ای که قیمت کالا از مشتریان قانونی این کارت‌ها کم می‌شود. (صغیر: ۱۹۹۹، ص۳۷)

تغییر داده پیام: تغییر نسبت به داده‌ای است که موجود است و محتوای آن دگرگون می‌شود. از این رو جدایی میان تخریب و جعل رایانه‌ای، جدا از خواست

1- Spam.
2- Tel Net.

مرتکب در انجام جعل و تخریب، در این است که تخریب نسبت به کل یا جزء داده انجام می‌شود و جعل نسبت به جزء داده و نیز جعل برای دگرگونی در محتوای داده است ولی تخریب جزئی برای دگرگونی در ظاهر یا پیکره داده؛ از سوی دیگر، هر چند دگرگونی نسبت به داده‌های پدید آورنده، افزون بر جعل می‌تواند موضوع بزه‌های ضد مالکیت معنوی به ویژه حق نویسندگی و برگردانی (تالیف و ترجمه) گردد. به سخن دیگر، در جعل رایانه‌ای، محوریت با دارا یا متصرف بودن داده و در نقض حق مالکیت فکری، محوریت با پدید آوردن اثر یا چیزی است. (عالی پور، ۱۳۹۰، ص ۱۹۷)

محو داده پیام: محو داده پیام، در حقیقت رفتاری بر ضد صحت و تمامیت داده و سامانه است و با جعل سنخیتی کم تری دارد. این مطلب به معنای عدم امکان تحقق جعل از طریق محو داده پیام نیست چرا که گاه ممکن است مجرم رایانه‌ای تمام یا بخشی از داده‌های موجود در یک سند رایانه‌ای را از بین ببرد به گونه‌ای که آن چه باقی می‌ماند چیزی خلاف حقیقت اولیه است. از این روی، در ماده ۶۸ به عنوان یکی از رفتارهای مجرمانه جعل رایانه‌ای معرفی شده و تحقق آن بدین صورت ممکن است که مثلاً یکی از مشتریان یک شرکت با ورود به رایانه شرکت تولیدکننده و محو اطلاعات مربوط به خود از لیست فروش شرکت مورد نظر خود را بری الذمه نشان دهد.

توقف داده پیام: گاهی ممکن است داده نادرست با متوقف کردن بخشی از داده‌های در حال انتقال ایجاد گردد. به این صورت که جاعل با ورود به یک سیستم رایانه ای، مانع از انتقال بخشی از داده‌های در حال انتقال در شبکه شده به گونه‌ای که داده‌ای که به کاربر مجاز می‌رسد یک داده ناقص و مبهم یا حتی غیر صحیح خواهد بود. متوقف کردن دادهای در حال انتقال در سیستم کارتِ پرداختِ الکترونیکی به راحتی امکان پذیر است. این سیستم بر عملیات انتقال الکترونیکی از حساب کارت مشتریِ بانکِ صادر کننده کارت به حساب بانکی فروشنده مبتنی است و به وسیله بانکی صورت می‌گیرد که حساب فروشنده در آن قرار دارد و از خلال شبکه باز پرداخت الکترونیکی گروه‌های بین المللی به انجام می‌رسد . (مانند گروه ویزا کارت و گروه ماستر کارت). کارت پرداخت الکترونیکی این حق را به

مشتری می‌دهد که از خلال شبکه اینترنت و از طریق اعلان کتبی یا تلفنی و با کم کردن قیمت از حساب کارت پرداخت الکترونیکی مخصوص به او به کالاها و خدماتی دست یابد و این کار سفارش‌ای میلی تلفنی[1] نامیده می‌شود.(شوابکه، ۲۰۰۹، ص۱۹۳) برای اجرای این عملیات کافی است مشتری به پایگاه الکترونیکی فروشنده در شبکه اطلاعاتی وارد شود و کالایی که قصد خرید آن را دارد انتخاب نماید و عملیات خرید و فروش پس از پر کردن نمونه الکترونیکی ـ که بر صفحه کامپیوتر ظاهر می‌شود ـ با اطلاعات کارت اعتباری مخصوص مشتری و آدرس او به انجام می‌رسد. پس از آن، فروشگاه قیمت کالا را از کارت پرداخت الکترونیکی کم می‌کند و آن را به آدرس مشتری ارسال می‌دارد. در این فرایند امکان ورود جاعل به سیستم بانک و متوقف کردن دادهای مربوط به انتقال الکترونیکی پول از حساب مشتری به حساب فروشنده وجود دارد.

مداخله در پردازش داده پیام و سیستم رایانه ای: یکی دیگر از مصادیق رفتارهای مجرمانه جعل رایانه‌ای مذکور در ماده ۶۸ ق.ت.ا. مداخله در پردازش داده پیام و سیستم رایانه ای است. رایج ترین شیوه مداخله در پردازش سیستم رایانه ای، روش "سالامی"[2] (سوسیس ایتالیایی) است که در آن یک برنامه مبالغ کوچکی را از حساب‌ها در حین پردازش گروهی با کسر خرده گرد کرده و وجوه به دست آمده را در یک حساب مخفی متعلق به متقلب قرار می‌دهد.(وایلدینگ: ۱۳۷۹، ص۲۹)

استفاده از وسایل کاربردی سیستم‌های رمزنگاری تولید امضاء:

تولید متقلبانه امضای الکترونیکی رفتار مجرمانه‌ای است که در واقع مصداقی از وارد کردن داده است.[3] این عمل از طریق علم رمزنگاری[1] و زمانی اتفاق می‌افتد

1- Mail Phone order

2- Salami

۳- از این روی گفته شده استفاده از وسایل کاربردی سیستم‌های رمزنگاری تولید امضاء از جهت چیستی، جعل رایانه ای نیست و همسان با حالت استفاده از مهر دیگری بدون اجازه دارنده آن که در ماده ۵۲۳ قانون مجازات اسلامی است می‌باشد؛ زیرا بهره گیری از افزارهای رمز نگاری تولید امضاء به تنهایی سبب جعل نمی گردد مگر این که رفتارهایی مانند وارد کردن یا پدید آوردن داده انجام شود.(عالی پور، ۱۳۹۰، ص۲۱۲)

که جاعل با در اختیار گرفتن کلید خصوصی کاربر اقدام به امضای الکترونیکی نماید. در صورت موفقیت جاعل در تولید امضای الکترونیکی تشخیص جعلی بودن امضاء بسیار دشوار بوده و وی خواهد توانست اسناد جعلی و قراردادهای ساختگی را منتسب به دیگری نموده و هم چون استفاده از مهر دیگری در جعل سنتی اقدامات بعدی را به سهولت انجام دهد.

تولید امضای الکترونیکی از این جهت است که در تجارت الکترونیکی بر خلاف تجارت سنتی تایید اسناد و قراردادها نه از طریق امضای دستی بلکه با "امضای الکترونیکی"[2] صورت گرفته و این نوع از امضاء است که کار انتساب اسناد به اشخاص را انجام می‌دهد. از این روی در ماده ۷ قانون تجارت الکترونیکی تصریح شده که هر گاه قانون، وجود امضاء را لازم بداند امضای الکترونیکی مکفی است. در این قانون دو نوع امضای الکترونیکی به رسمیت شناخته شده است: برابر بند "ی" ماده ۲ این قانون، امضای الکترونیکی عبارت از هر نوع علامت منضم شده یا به نحو منطقی متصل شده به «داده‌پیام» است که برای شناسائی امضا کننده مورد استفاده قرار می‌گیرد. این تعریف برگرفته از دستورالعمل شماره CE/۹۳/۱۹۹۹ پارلمان و شورای اروپا مورخ ۱۳ دسامبر ۱۹۹۹ است که به موجب آن امضای الکترونیکی، داده‌ای الکترونیکی است که به سایر داده‌های الکترونیکی متصل یا منطقاً مرتبط بوده، روشی برای احراز اصالت به شمار می‌رود(زرکلام، ۱۳۸۴، ص۲۸۸) امضای الکترونیکی در شکل ساده، همان امضای محیط کاغذی است که از رهگذر رو گرفت (اسکن)، در فضای سایبر نیز به کار می‌آید و در این حالت، برای کسان نیاز نیست تا همچون سپهر بیرونی،، برای هر بار گواهی دهی یا پاسخ دهی، کاغذی را دستینه کنند، بلکه امضای الکترونیکی را با کمک فرمان‌ها و برنامه‌های رایانه‌ای، بر روی متنی که آن را داده می‌نامیم، می‌گذارد.[3] امضای

1- Cryptography

2- Electronic Signature

۳- در امضای الکترونیکی وقتی امضایی به شکل خطوط (گرافیکی) صورت می‌گیرد (با قلم الکترونیکی یا اسکن امضاء و مهر) ابتدا به صورت او (O) و سپس به صورت اختلاف ولتاژ وارد رایانه شده در حافظه آن تأثیر می‌گذارد و باقی می‌ماند . سپس این اثر به طریق اولیه (گرافیکی) در صفحه نمایش یا کاغذ چاپ آشکار می‌گردد . بدین ترتیب آنچه منتقل می‌شود نسخه ای از

الکترونیکی، خود داده به شمار می‌آید و هر کس که آن را دگرگون کند، جعل رایانه‌ای انجام داده است. امضای الکترونیکی می‌تواند هر گونه نشانه یا علامتی باشد که شناساننده دارنده آن باشد.(عالی پور، ۱۳۹۰، ص۲۱۱)

نوع دیگر امضای الکترونیکی، "امضای الکترونیکی مطمئن"[1] است که برابر بند "ک" ماده ۲ قانون مورد بحث هر امضای الکترونیکی است که مطابق با ماده (۱۰) این قانون باشد. و در ماده اخیرالذکر آمده است: امضای الکترونیکی مطمئن باید دارای شرایط زیر باشد :الف- نسبت به امضاء کننده منحصر به فرد باشد .ب- هویت امضاء کننده «داده‌پیام» را معلوم نماید. ج- به وسیله امضاءکننده و یا تحت اراده انحصاری وی صادر شده باشد. د- به نحوی به یک «داده‌پیام» متصل شود که هر تغییری در آن «داده‌پیام» قابل تشخیص و کشف باشد.[2]

امضای الکترونیکی مطمئن به لحاظ فنی یا یک امضای رقمی[3] است و یا یک فرایند تجاری معقول که طرف‌ها آن را به رسمیت شناخته اند. امضای رقمی یک فرایند رمزنگاری است که از یک جفت کلید موسوم به کلید اختصاصی و کلید عمومی تشکیل می‌شود.[4] کلید اختصاصی[5] به دارنده آن اختصاص دارد و کلید عمومی[6] در اختیار دریافت کننده(مخاطب) فرضی قرار می‌گیرد. این دو کلید از

امضاء اولیه است که ابتدا به نحو مزبور تحول یافته سپس به صورت اولیه باز می‌گردد.

1- Secure Electronic Signature

۲- برابر ماده ۱۵ قانون تجارت الکترونیکی نسبت به امضای الکترونیکی مطمئن انکار و تردید مسموع نیست و تنها می‌توان ادعای جعلیت به» داده‌پیام» مزبور وارد و یا ثابت نمود که «داده‌پیام» مزبور به جهتی از جهات قانونی از اعتبار افتاده است.

3- Digital Signature

٤- در رمزنگاری، زیرساخت کلید عمومی (PKI) مقدمه‌ای است برای الصاق کلید عمومی به هویت کاربر، که با استفاده از یک مرکز صدور گواهی Certificate Authority (CA) انجام می‌گیرد. هویت کاربر باید برای هر CA یکتا باشد. نسبت دادن کلید عمومی به هویت افراد مطابق یک روند ثبت و صدور انجام می‌شود، که بر اساس سطح تضمین لازم ممکن است توسط یک نرم‌افزار در CA انجام شود و یا با نظارت انسان باشد. مسئولیت تضمین درستی در PKI بر عهده مرکز ثبت نام یا RA است. برای هر کاربر گواهی کلید عمومی حاوی هویت فرد، کلید عمومی، ترکیب هویت و کلید، شرایط اعتبار سند و مشخصه‌های دیگر، به طور غیر قابل جعل شدن توسط CA صادر می‌شود.

5- Private Key

6- Public Key

نظر ریاضی کاملاً به هم مرتبط و پیوسته بوده و در جهان خارج به طور کامل تک اند. یکی از آن دو کلید(کلید اختصاصی) برای امضای رقمی و دیگری(کلید عمومی) برای تطبیق و سنجش کلید اختصاصی به کار می‌رود. امضای الکترونیکی یک فناوری رمزنگاری نامتقارن است یعنی در آن از دو کلید متفاوت برای رمز و کشف رمز پیام استفاده می‌شود(زرکلام، ۱۳۸۴، ص ۲۹۰)

در واقع این موضوع که پیغام های الکترونیکی موجی از اطلاعات دیجیتال است، استفاده از تکنیک های رمزگشایی را برای اعتبار بخشیدن به سند امکان پذیر می سازد. این امر به وسیله اجرای عملکردهای ریاضی بر روی محتوای پیام‌ها یا بخشی از آن بدست می آید که می تواند تنها به وسیله ارسال کننده تحت تاثیر قرار گیرد. ارزش اثباتی رمزگشایی مبتنی بر مفهوم کارایی رایانه ای"[1] است، به این معنی که اگر چه رمزگشایی در نظر و در مرحله تئوریک می تواند مجدداً رمزگذاری شود – و بنابراین ذخیره ی پیام، جایگزین آن شود –، لکن مقدار زمانی که این امر در آن انجام می شود به قدری زیاد است که در جهت اهداف رمزگشایی، عملی امن تلقی می گردد. برای اینکه این امر موثر باشد، نسخه ی رمزگشایی شده باید به وسیله ارسال کننده مجدداً قابل تولید باشد و هر تلاشی برای تغییر محتوای پیام و رمزگشایی مجدد آن غیر ممکن باشد. روش های رمزگشایی، بخش اساسی تکنولوژی امضاء های الکترونیک است. کلید اصلی نظام های رمزگشایی مانند RSA برای روابط سرّی تهیه شد، ویژه ی مواردی که لازم نیست طرفین بر روش رمزگشایی توافق کنند. در قراردادهای تجارت الکترونیکی وقتی طرفین توافقی قبلی در مورد سندیت نکرده اند، این کلیدها مناسب اند و مبنایی برای تکنولوژی های امضاء های الکترونیکی می‌باشند. نشانه های رمزی RSA سه عدد نیاز دارند: N، kp (که برای رمزگشایی استفاده می شود) و ks (کلید رمزی که برای رمزگشایی مجدد استفاده می شود). کلیدهای N و kp کلیدهای اصلی دریافت کننده اند ولی ks سرّی نگه داشته می شود. ارسال کننده ی پیام با به دست آوردن شکل دیجیتال پیام از طریق kp، آن را رمزگشایی می کند. رمزگشایی مجدد دریافت کننده با استفاده از ks صورت می گیرد. از آنجا که فرمول

1- Computational Infeasibility

رمزگشایی یکسان است امکان دارد با استفاده از ks ، کلید خصوصی ارسال کننـد، و رمز گشایی آن با kp پیام رمزگشایی شود و بنابراین بر امضاء الکترونیکی اثر بگذارد. ارسال کننده پیامش را با استفاده از ks رمزگشایی می کند. وقتی پیام دریافت می شود، دریافت کننده مجدداً پیام را رمزگشایی می کند؛ حال اگر هر دو پیام به دادگاه ارائه شوند، قاضی می تواند هویت ارسال کننده را به وسیله رمزگشایی مجدد پیام و بررسی آن در برابر پیام دیگر تشخیص دهد. (رید، ۲۰۰۷، ص۲۱۹)

تولید امضای فاقد سابقه ثبت در فهرست دفاتر اسناد الکترونیکی: در تجارت سنتی سازگاری امضای پدیده آمده بر روی اسناد و قراردادها با همان امضایی که از یک شخص وجود داشته یا به آن شناخته شده تضمین کننده انتساب امضاء به شخص امضاء کننده است که با توجه به میزان فشار دست در نقاط مختلف خطوطی که به عنوان امضاء کشیده می‌شود کارشناسان قادر به شناسایی و تشخیص اصالت یا جعلی بودن امضاء خواهند بود اما در تجارت الکترونیکی به جهت الکترونیکی بودن اسناد و انعقاد قرارداد در فضای مجازی، ویژگی گفته شد منتفی است و از این روی تشخیص غیرجعلی بودن نامه‌های الکترونیکی دارای اهمیت فراوانی است. بدیهی است یک سند الکترونیکی برای معتبر بودن در یک محکمه قضایی به‌عنوان یک سند نیازمند امضاست، اما امکان اسکن و جعل کردن امضای افراد این اعتبار را زیر سؤال می‌برد و تنها دیجیتالی کردن، امضاست که می‌تواند این اعتبار را به اسناد الکترونیکی ببخشد چرا که با دیجیتالی شدن امضاء در فضای الکترونیکی تبدیل به یک کد شده و بدین ترتیب با امضای دیجیتال اطمینان در تجارت الکترونیکی حاصل می‌شود. این فرایند(یعنی تبدیل امضاء به اعداد و ارقام) باید در مراجعی صورت گیرد که بتواند اعتماد کاربران و فعالان عرصه تجارت الکترونیکی را جلب نماید و این مراجع همان دفاتر خدمات صدور گواهی الکترونیکی هستند.[1] از این روی قانون گذار تجارت الکترونیکی دفاتر خدمات

۱- به گفته مسوولان به‌منظور خدمت‌رسانی برای توسعه این خدمت الکترونیکی بیش از شش هزار دفتر ثبت اسناد رسمی در ۲۵ استان کشور آماده ارائه گواهی امضای الکترونیک به متقاضیان هستند(غضنفری، ۱۳۹۰،ص ۲)

صدور گواهی الکترونیکی را مأمور صدور امضای الکترونیکی نموده و در ماده ۳۱ مقرر داشته است: "دفاتر خدمات صدور گواهی الکترونیکی واحدهائی هستند که برای ارائه خدمات صدور امضای الکترونیکی در کشور تأسیس میشوند. این خدمات شامل تولید، صدور، ذخیره، ارسال، تأیید، ابطال و به روز نگهداری گواهی‌های اصالت) امضای)الکترونیکی می باشد." و بدین صورت بر صلاحیت انحصاری دفاتر مذکور در صدور این نوع از امضاء تاکید کرده و تخطی از این امر و تولید امضایی بدون سابقه ثبت در فهرست دفاتر اسناد الکترونیکی را به عنوان جعل شناسایی و ضمانت اجرای کیفری آین عمل را در ماده ۶۸ ق.ت.ا. اعلام داشته است.[۱]

عدم انطباق وسایل کاربردی سیستم‌های رمز نگاری تولید امضاء با نام دارنده در فهرست مزبور: ارتکاب جعل بدین شیوه ناظر به مواردی است که مرتکب از کلید خصوصی ثبت شده به نام یک فرد خاص استفاده و یک امضای دیجیتال به نام خود یا شخص ثالثی ایجاد می‌نماید. پس از مراجعه به فهرست مرجع گواهی معلوم می‌شود نام فردی که امضای دیجیتال منضم به سند الکترونیکی منتسب به اوست و به عبارتی از کلید خصوصی مربوطه به نام او استفاده شده، با دارنده کلید عمومی مرتبط با آن کلید خصوصی مندرج در فهرست مطابقت ندارد. (جاویدنیا، ۱۳۸۷،ص۲۹۴) از حیث عملیاتی، در حال حاضر افرادی که در ایجاد و ایمنی امضای دیجیتالی مداخله می‌کنند عبارتند از: الف) امضا کننده اصلی: یعنی شخصی که امضای دیجیتالی را برای استفاده از آن در تایید مدرکی ایجاد می‌کند؛ ب) دفتر خدمات گواهی الکترونیکی: مکانیسم لازم را برای ایمنی و اطمینان امضا فراهم می‌سازد. با گواهی این مرجع، امضا کننده مجاز به استناد به مدارک گواهی شده می‌شود و کلیدهای اختصاص یافته به او به نام او ذخیره شده و به شخص دیگری

۱- با وجود این گفته شده که تولید امضای فاقد سابقه ثبت در فهرست دفاتر اسناد الکترونیکی نباید جعل به شمار آید،زیرا سابقه ثبت الکترونیکی امضا تنها درباره رفتارهای مشخص مانند تجارت الکترونیکی که دارندگان آن در پی شناخته شدن و اطمینان از طرف قرارداد هستند، سازگاری دارد. از این رو این بخش از ماده ۶۸ قانون تجارت الکترونیکی، تنها بر برخی مبادلات الکترونیکی یعنی تجارت الکترونیکی گواهی می‌دهد وگرنه در مقام پشتیبانی کیفری از امضای شهروندان، نیازی به پیشینه ثبت نیست.(عالی پور، ۱۳۹۰، ص۲۱۲)

تعلق نمی گیرد؛ ج) دفاتر ثبت: بر خلاف مورد قبل که ایمنی و اطمینان امضا را از جنبه فنی تامین می کند، سردفتر به عنوان شخص ثالث قابل اعتماد به تصدیق مدارک و تایید هویت امضا کننده اقدام می کند. به طور کلی، اطلاعات تهیه شده توسط دفاتر خدمات گواهی از جمله عواملی است که زمینه اعتماد سردفتر را به امضای ایجاد شده فراهم می سازد، اگر چه او نیز موظف است تا بررسی های متعارف را به عمل آورد؛ د) طرف اعتماد کننده: شخصی است که با بررسی کلید عمومی به اصالت و صحت امضای دیجیتالی اعتماد کرده و آن را به عنوان معیاری برای تنفیذ تعهد صاحب امضا در قبال خود می‌پذیرد. این فرد اگر چه در فرایند ایجاد و امنیت امضا نقشی ندارد، ولی قبول وی از آن جهت که به امضای دیجیتالی اعبار عملی می‌بخشد، بسیار ارزشمند محسوب می‌شود، زیرا تقریباً در تمام قوانین راجع به امضای دیجیتالی به افراد این اختیار داده شده که از پذیرش امضا و مدارک الکترونیکی در روابط تجاری و مالی خود با دیگران امتناع نموده و امضای دستی و مدارک کاغذی مطالبه کنند که این امر با توجه به مسایل متعددی چون ضعف امنیت و اعتماد در فضای مجازی قابل توجیه است. اما مطلبی که باید مورد توجه قرار گیرد این است که از آن جا که بدون وجود سابقه ثبتی و مدارک دقیق علمی، امضای دیجیتالی هیچ دلالتی بر دخالت یک فرد در محتوای سندی که امضا در آن به کار گرفته شده، ندارد، عدم دخالت دفاتر ثبت اسناد از ساختار شکل گیری، ایمنی و تصدیق این گونه از امضاها موجب سلب اعتماد و کاهش اعتبار این نوع از امضاء است. از سوی دیگر، از آن جهت که در قوانین داخلی کشورمان، حضور امضا کننده نزد سردفتر واجد شرایط به منظور ثبت امضا پیش بینی نشده و نیازی به طی تشریفات مقرر در قانون ثبت برای تشخیص هویت امضا کننده وجود ندارد، این امر امکان صدور امضا از سوی اشخاص خیالی را افزایش می‌دهد و امضا کننده می‌تواند از این طریق حقوق و تعهداتی برای خویش در قرارداد با دیگران ایجاد نماید، در حالی که تعهدات وی به دلیل فقدان شخصیت حقیقی برای او قابل گریز است. (http://www.bih.ir/)

أخذ گواهی مجعول: أخذ گواهی در روال تأیید امضای دیجیتال و از ناحیه کسی انجام می گیرد که می‌خواهد صحت و سقم امضاء را تشخیص دهد: پس از

وصول تقاضای صدور گواهی به دفتر خدمات مربوطه آن دفتر تأییدیه را بصورت برخط برای متقاضی ارسال می‌کند بنابراین اخذ گواهی جعل معنا ندارد. اما چنانچه متصدیان دفتر خدمات الکترونیکی گواهی جعل کنند یا یک گواهی جعل شده و به دفتر خدمات الکترونیکی خاص منسوب گردد یا یک ایمیل به دروغ به دفتر خدمات معرفی شده و متقاضی فریب بخورد و اقدام به أخذ گواهی از آن کند اینها همگی صدور گواهی جعل است و نه أخذ گواهی جعل! از این روی گفته شده که اخذ گواهی مجعول دنباله حالت استفاده از وسایل کاربردی سیستم‌های رمزنگاری تولید امضاء است و نمی بایست با واژه "یا" جدا می‌شد، بلکه باید از نشانه "و" بهره گرفته می‌شد.

و نظایر آن: رفتارهای چهارگانه مذکور در صدر ماده ۶۷ یعنی ورود، تغییر، محو و توقیف داده پیام به اندازه کافی از جامعیت برخوردار بوده و در برگیرنده هر نوع عملی است که منتهی به وقوع جعل شود و با ذکر آن نیازی به تصریح به موارد دیگر نیست از این روی در ماده ۷ کنوانسیون جرایم سایبری هم فقط چهار عمل پیش گفته بصورت حصری ذکر شده است.[1] با وجود این مقنن در ماده ۶۷ قانون تجارت با ذکر عبارت و نظایر آن، بر تمثیلی بودن مصادیق نام برده شده در این ماده تاکید نموده است. تمثیلی بودن مصادیق ماده ۶۸ از این مزیت برخوردار است که امکان برخورد با هر گونه رفتارهای جدید و پیچیده جعل رایانه‌ای در فضای مبادلات الکترونیکی را برای دادگاه فراهم می‌سازد و مانع عقب ماندگی قانونی در برابر پیشرفت‌های فنی ابزارهای مورد استفاده در جعل است. چرا که امروزه قابلیت‌های تصاویر پیشرفته نرم افزاری جدید مخزنی از ابزارهای نو را در اختیار گذاشته است که به کمک آنها می‌توان اسناد مورد استفاده در تجارت را جعل کرد. با در دسترس قرار گرفتن ماشین‌های فتوکپی رنگی لیزری و کامپیوتری، نسل جدیدی از تغییر و جا به جایی متقلبانه و یا جعل نیز بوجود آمده است. این ماشین‌ها

۱- برابر ماده ۶ قانون جرایم رایانه ای مصوب ۱۳۸۸/۳/۵ هر کس به طور غیرمجاز مرتکب اعمال زیر شود، جاعل محسوب ... خواهد شد:
الف) تغییر یا ایجاد داده‌های قابل استناد یا ایجاد یا واردکردن متقلبانهٔ داده به آنها.
ب) تغییر داده‌ها یا علائم موجود در کارتهای حافظه یا قابل پردازش در سامانه‌های رایانه‌ای یا مخابراتی یا تراشه‌ها یا ایجاد یا وارد کردن متقلبانهٔ داده‌ها یا علائم به آنها.

قادر به کپی برداری با وضوح بالا، اصلاح اسناد و حتی ایجاد اسناد جعلی بدون استفاده از نسخه اصلی هستند (خداقلی،۱۳۸۳،ص ۱۵۰)

به هر حال، در محیط سایبر، یک مرتکب جرم یا قصد دارد امتیازات جدیدی را بر اساس اعتبارات اشتباه ایجاد کند؛ یا از رهگذر استفاده از اطلاعات به دست آمده از منابع، از امتیازات بهره گیری کند. چنین اطلاعاتی ممکن است از طریق خودِ زیان دیده، به وسیله استفاده از تکنیک های مهندسی اجتماعی، که مبتنی بر روابط بشری است، به دست آید؛ روابطی که مردم را مجبور به افشای اطلاعاتی می کند که باعث غلبه بر مکانیسم های امنیت اطلاعاتی می گردد. بر عکس، شخص ممکن است اطلاعات مشتریان و یک سایت تجارت الکترونیکی را هک کند تا مشخصات کارت اعتباری و اطلاعات مربوط به هویت صاحبان آنها را به دست آورد. هر دو نوعِ این اقدامات، جرم جعل را به موجب «قانون جعل و تقلب» ۱۹۸۱ تشکیل می دهد. بخش ۱ قانون جعل و تقلب ۱۹۸۱ ابراز می دارد: «شخصی که سندی اشتباه را با قصد این که خودش یا دیگری برای مجبور کردن فردی دیگر به پذیرفتن آن، از سند استفاده کننده تهیه کند، مرتکب جرم جعل شده است.»

طبق قانونگذاری اخیر، شخص می تواند انتظار داشته باشد که قانون از مداخله در مسائلی که با استفاده از فناوری رایانه ای در ارتباط با کلاهبرداری به وجود می آید، جلوگیری کند. با این حال، قضیه انگلیسی جاری در مورد استفاده از رایانه‌ها برای ارتکاب جعل - دعوای آر علیه شیفرین - نشان می دهد مشکلات مستمری بر سر راه قانونگذاران قرار دارد. در قضیه ی گلد، متهمان دسترسی غیر مجازی به خدمت Prestel شرکت BT داشتند و رمز عبورهای ایمیل های مختلف، مثلاً دوک ادینبرگ را پیدا کردند. متهمین طبق قانون مصوّب ۱۹۸۱، به دلیل ایجاد یک سند تقلبی از جهت وارد کردنِ کدهای مشتریان برای دستیابی به سامانه، تحت تعقیب قرار گرفتند.(والدن،۲۰۰۷، ص ۵۶۰)

موضوع جرم: مقنن در ماده ۶۸ ق.ت.ا. "داده پیام، سیستم‌های رایانه‌ای و وسایل کاربردی سیستم‌های رمزنگاری تولید امضاء" را موضوع این جرم دانسته است. در مورد داده پیام و سیستم‌های رایانه‌ای در شماره پیشین این اثر و در مقاله کلاه برداری رایانه‌ای توضیحاتی داده شد و از تکرار آن خودداری می کنیم اما تفاوتی

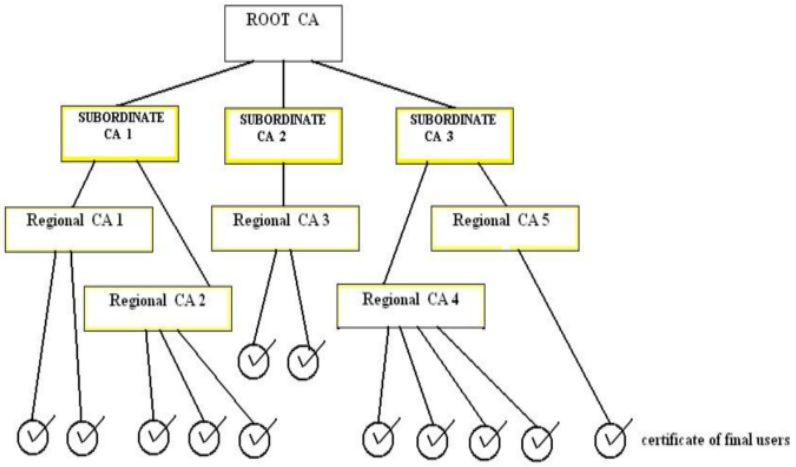
که در مورد موضوع جرم در دو جرم کلاه برداری و جعل رایانه‌ای وجود دارد این است که تصریح مقنن در ماده ۶۸ ق.ت.ا. به این که "...اقدام به جعل داده‌پیام دارای ارزش مالی و اثباتی[1] نماید تا با ارائه آن به مراجع اداری، قضایی، مالی و غیره به عنوان «داده‌پیام»های معتبر استفاده نماید..." برخورداری از ارزش مالی و اثباتی را شرط داده پیام موضوع جرم دانسته است. این در حالی است که در جعل رایانه‌ای، ارزش مالی داشتن داده، برجستگی ندارد؛ زیرا نه به این شرط برای استنادپذیری نیاز هست و نه جعل رایانه‌ای، بزهی بر ضد مال یا ارزش مالی داده است، بلکه این رفتار بر روی داده‌هایی رخ می‌دهد که همچون سند یا نوشته، به اندازه‌ای اهمیت دارند که بتوان از آنها برای استناد در نهادهای عمومی و دولتی بهره جست(عالی پور، ۱۳۹۰، ص ۲۱۱) این مطلب از این جهت قابل تایید است که در اسناد مصوب شورای همکاری و توسعه اقتصادی، شورای اروپا و نیز در کنوانسیون جرایم سایبری صرفاً جعل داده‌ها و پیام‌های رایانه‌ای موضوع جعل شناخته شده و به ارزش مال داشتن داده شرط دانسته نشده است.

با وجود این و با توجه به ظاهر ماده ۶۸ داده پیام‌های فاقد ارزش مالی مثل داده‌های مربوط به یک ویروس رایانه‌ای که تولید آن جرم است یا حتی داده پیام‌های دارای ارزش اثباتی در مراجع قضایی اما فاقد ارزش مالی موضوع جعل ماده ۶۸ ق.ت.ا. نیست(جاویدنیا،۱۳۸۷، ص۲۹۶)

اما در مورد موضوع سوم در جرم جعل مذکور در ماده ۶۸ یعنی وسایل کاربردی سیستم‌های رمزنگاری تولید امضاء بابد دانست از آن جا که امروزه هر کس می‌تواند بسته به نوع نیازش یک یا چندین گواهینامه دیجیتال دریافت و ثبت کند، به منظور اینکه صدور گواهی به درستی مدیریت شده و در عمل با ایجاد یک مرکز صدور گواهی، یک نقطه حساس به خرابی ایجاد نشود که کل امنیت اینترنت بدان وابسته است، باید شیوه‌ای مناسب اتخاذ گردد. شیوه‌ها و سیستم‌های کاربردی رمزنگاری متعددی برای تولید امضای الکترونیکی وجود دارد لکن در حال حاضر بهترین رویکرد برای صدور گواهینامه‌های دیجیتالی روشی است که به زیرساخت

۱- گفته شده احتمالاً مقصود قانون گذار این بوده که از عبارت دارای ارزش مالی یا اثباتی استفاده کند ولی دچار اشتباه شده است(اصلانی،۱۳۸۴، ص۱۹۷

کلید عمومی[1] شهرت یافته و یک الگوی سلسله مراتبی (درختی) به شمار می‌رود.



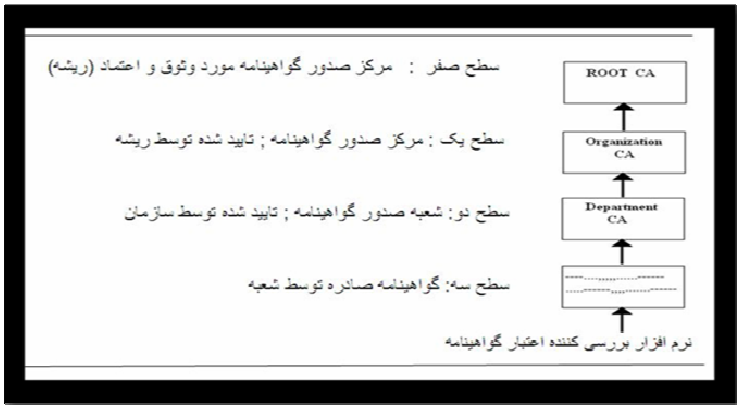
الگوی سلسله مراتبی PKI در صدور گواهینامه

در شکل فوق فرض را بر این بگذارید که یک مرکز جهانی و مورد وثوق همگان وجود دارد که در عالیترین سطح برای سطح دوم گواهینامه صادر می‌کند. این مرکز جهانی (که می‌تواند بیش از یکی باشد) ریشه[2] نام دارد که بر اساس ضوابط و توافقات بین المللی اداره می‌گردد. این مرکز برای شعبات خود در کشورهای مختلف گواهینامه دیجیتالی صادر کرده و درون این گواهینامه ، کلید عمومی آنها را تایید می‌کند. تمام این مراکز میانی ، زوج کلید عمومی و خصوصی خود را به دلخواه انتخاب کرده و کلید عمومی خود را به کمک یک گواهینامه X.۵۰۹ که توسط ریشه امضاء شده در اختیار همه قرار می‌دهند. این مراکز را شعبات مجاز صدور گواهی[3] ، در کشورهای مختلف تلقی کنید. این شعبات نیز خودشان در ایالات و استانها و شهرهای بزرگ شعبه خواهند داشت. بدین ترتیب در سطح سوم مراکز مجاز منطقه ای[4] بوجود می‌آیند. مراکز منطقه‌ای خود از مراکز استانی ، گواهینامه در یافت کرده و کلیدهای عمومی خود را درون آنها تایید می‌کنند. این مراکز می‌توانند مستقیما برای کاربران گواهینامه صادر کنند و یا

1- PKI (Publik Key Infrastructure)
2- Root
3- Subordinate Certificate Authority
4- Regional Certificate Authority

مـی‌تواننـد خـود در شـهرهای کوچـک و منـاطق مختلـف، شـعباتی تاسـیس و گواهینامه‌های این شعبات را امضاء کننـد. بـه هـر حـال در آخـرین سـطح، کـاربران معمولی با مراجعه به یکی از این مراکز مجـاز و طـی تـشریفات پـیش بینـی شـده در قـانون، گواهینامـه‌ای دریافـت و کلیـد عمـومی خـود رادرون آن درج و گـواهی می‌کنند. حال سؤال این است که گواهینامه صادر شده در سطح آخر چگونـه دارای اعتبار و هویت می‌شود؟ بدیهی است که به غیر از مرکز جهانی (ریـشه) هیچکـدام از شعبات کشوری ،استانی یا شهری ،برای عموم مردم شـناخته شـده و مـورد اعتنـاد نیستند. لذا صرفا فرض را برآن می‌گذاریم که عموم کاربران و نرم افزارهـای جهـان فقط وفقط ریشه را می‌شناسند و کلید عمومی این مرکـز را در اختیـار دارنـد. روش تایید اعتبار یک گواهینامه صادره در آخرین سـطح طبـق روال شـکل زیـر صـورت می‌گیرد:

الف) نرم افزار بررسی کننده اعتبار گواهینامه ،کارش را بـا دریافـت گواهینامـه X.۵۰۹ متعلـق بـه یـک کـاربر فرضـی آغـاز مـی‌کنـد. گواهینامـه بـاب گذشـته از مشخصات کلی او ، کلید عمومی او را نیز شامل شده و همچنین هویت مرکزی کـه این گواهینامه را صـادر کـرده درون آن مـشخص اسـت. در اولـین گـام بایـد کلیـد عمومی مرکـز صـادر کننـده گواهینامـه بدسـت آیـد تـا ضـمن رمزگـشایی امـضای گواهینامه و مقایسه آن با چکیده محتوای آن، جعلی نبـودن گواهینامـه احـراز شـود. بدین ترتیب نرم افزار بررسی کننده اعتبار، کار را نیمه تمام باقی گـذارده تـا قبـل از هر چیز ، گواهینامـه مرکـز صـدور گـواهی را بدسـت آورد و کلیـد عمـومی آن را مشخص کند.



ب) گواهینامه شعبه صادر کننده گواهینامه توسط شخص کاربر و یا از طریق یک سیستم دایرکتوری دریافت می‌شود. مجددا برای آنکه جعلی نبودن همین گواهینامه اثبات شود به کلید عمومی شعبه صدور در سطح بالاتر نیاز است. گواهینامه صادر کننده سطح بالاتر نیز دریافت و همین فرآیند تکرار می‌شود تا زنجیره گواهینامه‌ها به ریشه ختم شود. وقتی زنجیره گواهینامه‌ها ب ریشه رسید شرایط برای تایید گواهینامه‌ها مهیاست زیرا فرض بر آن است که همه افراد کلید عمومی ریشه را می‌دانند.

ج) با کلید عمومی ریشه، گواهینامه مرکز سطح یک، پردازش و در صورت احراز اصالت آن، کلید عمومی آن مرکز استخراج می‌شود تا به کمک آن گواهینامه مرکز سطح دو پردازش و تایید شود. این روند به صورت بازگشتی ادامه می‌یابد تا تمام گواهینامه‌ها احراز هویت شوند. بدین ترتیب کاربر نهایی تایید و کلید عمومی او برای ادامه کار از درون گواهینامه استخراج می‌شود. (http://nsecure.ir)

نتیجه

جعل سنتی جرمی مقید به نتیجه نبوده و ضرر بالفعل شرط وقوع آن نیست. با وجود این، ضرر بالقوه یا به بیان دیگر قابلیت اضرار شرط است و اگر نوشته‌ای ساخته شود که امکان هیچ گونه ضرری با آن قابل تصور نباشد جرم جعل محقق نخواهد بود. در جعل رایانه‌ای موضوع ماده ۶۸ قانون تجارت الکترونیکی هم ایراد ضرر بصورت بالفعل شرط وقوع جرم نیست بلکه آن چه اهمیت دارد این است که جاعل بتواند با انجام رفتارهای گفته شده در ماده "داده‌پیام دارای ارزش مالی و اثباتی ایجاد نماید تا با ارائه آن به مراجع اداری، قضایی، مالی و غیره به عنوان داده‌پیام‌های معتبر استفاده نماید" به بیان دیگر داده‌های ایجاد شده باید امکان استفاده و استناد در مراجع اداری، قضایی، مالی و نهادهای مشابه را داشته باشد بنابراین اگر در جعل سنتی "قابلیت اضرار" برای تحقق جرم لازم است، در جعل رایانه‌ای "قابلیت استناد" شرط است و از آن جا که ضرر اعم از ضرر مادی و معنوی است و استناد به سند در مقام دعوی یا دفاع در درون خود با اثبات حق بر ضرر غیر یا نفی حق ادعایی غیر ملازمه دارد، از این رو قابلیت استناد به معنای

قابلیت اضرار خواهد بود[1] و بدین ترتیب مشاهده می‌شود که جعل سنتی و رایانه‌ای از حیث نتیجه مشابه یکدیگر بوده و قابلیت اضرار در وقوع آن شرط است.

در تبصره ماده ۶۸ ق.ت.ا. شروع به جعل نیز جرم تلقی و مجازات آن حداقل مجازات جعل رایانه‌ای در نظر گرفته شده است. هر چند به جهت سرعت بالای عملیات رایانه‌ای تصور وقوع شروع به جرم و امکان تفکیک مرحله شروع از مرحله جرم تام چندان آسان نیست با وجود این، می‌توان موردی را تصور کرد که کارمند دفتر خدمات صدور گواهی الکترونیکی با اسکن امضای شخص موهوم در حال تخصیص و ایجاد ارتباط بین کلید عمومی و اختصاصی برای صدور یک امضای الکترونیکی جعلی است که به جهت عدم مهارت مدت زمانی غیرمتعارف برای این کار صرف کرده و این موضوع موجب مشکوک شدن و نهایتاً کشف قضیه می‌گردد.

مبحث سوم رکن معنوی

رکن معنوی جعل رایانه‌ای از دو جزء سوء نیت عام و خاص تشکیل شده است. برای احراز سوئ نیت عام از یک سو جاعل باید علم به ماهیت عمل خود داشته و به غیر قانونی و غیر مجاز بودن رفتار خویش آگاه باشد و بداند که اعمال و رفتارهایش در ورود، تغییر، محو و توقف داده‌پیام و مداخله در پردازش داده‌پیام و مداخله در پردازش داده‌پیام و سیستم‌های رایانه‌ای، و یا استفاده از وسایل کاربردی سیستم‌های رمزنگاری تولید امضاء و یا تولید امضای فاقد سابقه ثبت در فهرست دفاتر اسناد الکترونیکی و اعمال مشابه دیگر غیرمجاز و یا بدون مجوز امضاء کننده بوده و در نهایت منتهی به جعل داده‌های دارای ارزش مالی و اثباتی خواهد بود و از سوی دیگر با اراده و اختیار خود و نه با اجبار و اکراه یا از روی سهل انگاری و فقدان مهارت و دانش رایانه‌ای دست به چنین اعمالی زده باشد.

هم چنین برای احراز سوء نیت خاص باید قصد جاعل مبنی بر ارائه داده پیام‌های جعلی به مراجع اداری، قضایی، مالی و... و استفاده از آن به عنوان داده پیام‌های معتبر اثبات گردد. عبارت قانون گذار در ماده ۶۸ مبنی بر این که " تا با

۱- بنابراین، این گفته که "داده‌های موضوع جعل رایانه‌ای باید قابلیت استناد داشته باشند و به جهت همین شرط بنیادین است که دیگر نیازی به پیش کشیدن زیان چه بالقوه و چه بالفعل نیست" عبارت درستی به نظر نمی رسد چه این که امکان استناد به معنای احتمال اضرار است.

ارائه آن به مراجع اداری، قضایی، مالی و غیره به عنوان داده‌پیام‌های معتبر استفاده نماید " مؤید این مطلب است. بنابراین، اگر به عنوان نمونه کسی یک امضای الکترونیکی را جعل و در رایانه‌اش ذخیره کند ولی قصد ارائه آن به جای علامت اصلی و استناد به آن در مراجع اداری، مالی و قضایی و سایر مراجع دولتی را نداشته باشد مرتکب جرم جعل نشده است.

مجازات

مرتکب جرم جعل رایانه‌ای در بستر مبادلات الکترونیکی قانوناً در معرض اعمال دو مجازات قرار دارد: مجازات حبس از یک تا سه سال و نیز پرداخت جزای نقدی به میزان پنجاه میلیون (۵۰/۰۰۰/۰۰۰) ریال. در مورد کیفر حبس، بازه دوساله ناشی از تفاوت بین حداقل و حداکثر مجازات، به قاضی امکان فردی سازی و ایجاد تناسب بین مجازات با نوع و درجه شدت جرم و شخصیت مجرم را خواهد داد ولی مبلغ ثابت جزای نقدی دارای دو اشکال است؛ از یک سو فاقد انعطاف و امکان فردی سازی مجازات است و از سوی دیگر همانند سایر موارد تعیین جزای نقدی، تورم و کاهش ارزش پول موجب سلب قدرت بازدارندگی مجازات خواهد شد. از سوی دیگر برابر ماده۶ قانون جرایم رایانه ای، مجازات جعل رایانه‌ای حبس از یک تا پنج سال یا جزای نقدی از ۲۰,۰۰۰,۰۰۰ تا ۱۰۰,۰۰۰,۰۰۰ ریال یا هر دو مجازات تعیین شده است که در مورد جعل رایانه‌ای در خارج از فضای مبادلات الکترونیکی است. تفاوت مجازات جعل رایانه‌ای در حیطه مبادلات الکترونیکی با غیر آن در این است که افزون بر تفاوت در میزان حبس و جزای نقدی در دو مقرره، در قانون تجارت الکترونیکی همواه هر دو کیفر حبس و جزای نقدی باید مورد حکم قرار گیرد ولی در قانون جرایم رایانه‌ای یکی از دو مجازات هم می‌تواند حکم داده شود!

نکته دیگر این است که برابر تبصره ماده ۷ قانون جرایم رایانه ای، "هرکس با علم به مجعول بودن داده‌ها یا کارتها یا تراشه‌ها از آنها استفاده کند، به مجازات مندرج در ماده فوق محکوم خواهدشد." مشابه چنین حکمی در قانون تجارت الکترونیکی وجود ندارد اما از آن جا که قانون جرایم رایانه‌ای حکمی عام و قانون تجارت الکترونیکی قانونی خاص است، در مواردی که قانون خاص نسبت به موضوعی ساکت باشد می‌توان به قانون عام مراجعه و به آن استناد نمود بنابراین در

صورتی که شخصی در خلال تجارت الکترونیکی اقدام به استفاده آگاهانه از داده پیام جعلی نماید برابر ماده ۷ قانون جرایم رایانه‌ای قابل مجازات خواهد بود.

نتیجه:

مزایای تجارت الکترونیکی نظیر کم هزینه بودن، سهولت، سرعت، تنوع انتخاب، بازاریابی گسترده و ... عواملی است که روی آوردن به این روش نوین از مبادلات را در دنیای امروز امری ضرورت و گریزناپذیر نموده است. از سوی دیگر قابلیت‌های فنی و ابزارهای پردازش رایانه‌ای امکان مداخلات متقلبانه رایانه‌ای را برای مجرمان بوجود آورده است. یکی از مهم ترین اقداماتی که موجب سلب اعتبار اسناد الکترونکی و در نتیجه کاهش اعتماد کاربران به تجارت الکترونیکی شده جعل رایانه‌ای است. از این رو قانون گذار در ماده ۶۷ قانون تجارت الکترونیکی جعل رایانه‌ای در بستر مبادلات الکترونیکی را جرم تلقی و برای ان مجازات حبس و جزای نقدی در نظر گرفته است. از آن جا که اعتبار اسناد و قراردادها به امکان انتساب آن به شخص حقیقی یا حقوقی منتسب الیه است که با امضای و تایید آن بدست می‌آید، در اسناد و قراردادهای الکترونیکی که رکن اساسی تجارت الکترونیکی است نیز امضای الکترونیکی که نشانه انتساب سند الکترونیکی به امضاء کننده است دارای اهمیت اساسی است. از سوی دیگر ایجاد مراجع معتبری که بتوانند با صدور امضای الکترونیکی تایید کننده اصالت و اعتبار امضای الکترونیکی باشد امری ضروری است. خوشبختانه این مهم نیز در قانون تجارت الکترونیکی پیش بینی شده و به موجب ماده ۳۱ این قانون دفاتر خدمات گواهی الکترونیکی عهده دار چنین کاری شده اند. اما این امر به تنهایی کافی نیست و آن چه اهمیت بیشتری دارد تمایل و رغبت مردم به تجارت الکترونیکی است که بخشی از آن ناشی از نبود اطمینان و اعتماد به فضای مجازی و دنیای اینترنت است. بدیهی است بکارگیری روش‌های فنی دقیق و سیستم‌های کاربردی مطمئن و امن در صدور امضای الکترونیکی از یک سو و الزام تجار و بلکه اختصاص عمومی امضای الکترونیکی برای همه مردم و درج آن در کارت هویت ملی دیجیتالی در کنار آموزش و تشویق مردم به استفاده از این نوع امضاء در فعالیت‌های مالی و اداری می‌تواند کمک شایانی به پذیرش امضای الکترونیکی به عنوان نشانه معتبر انتساب به اشخاص و در نتیجه گسترش تجارت الکترونیکی نماید.

منابع:

۱) خداقلی، زهرا، جرایم کامپیوتری، چاپ اول، انتشار ات آریان، تهران، ۱۳۸۳

۲) اصلانی، حمیدرضا، حقوق فناوری اطلاعات، چاپ اول، نشر میزان، تهران، ۱۳۸۴

۳) باستانی، برومند ، جرایم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری، تهران، بهنامی، چاپ دوم، ۱۳۸۶

۴) بای، حسینعلی و پورقهرمانی، بابک، بررسی فقهی حقوقی جرایم رایانه ای، قم، پژوهشگاه علوم و فرهنگ اسلامی، چاپ اول ۱۳۸۸

۵) پنلوپ، لارنس، کاربرد اینترنت در حقوق،ترجمه سید قاسم زمانی و مهناز بهراملو، تهران، نشر میزان،چاپ اول،۱۳۸۳

۶) جاویدنیا، جواد، جرایم تجارت الکترونیکی، تهران،خرسندی، چاپ اول،۱۳۸۷

۷) حیدری، علی مراد، شناخت جرایم رایانه‌ای از منظر اسناد بین المللی و قوانین داخلی، دو فصلنامه فقه و حقوق ارتباطات، سال اول، پیش شماره۱، بهار و تابستان ۱۳۸۹

۸) خرم آبادی، عبدالصمد ، تاریخچه، تعریف و طبقه بندی جرم‌های رایانه‌ای، مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات، قوه قضائیه، معاونت حقوقی و توسعه قضایی، قم، سلسبیل، ۱۳۸۴

۹) وزارت بازرگانی، کمیته ملی ادیفاکت؛ ۱- گزارش توجیهی. ۲- پیش نویس. ۳- منابع قانون تجارت الکترونیکی(ویرایش تکمیلی)، پاییز ۱۳۸۰

۱۰) کیسی، اوئن(۱۳۸۳) دلایل دیجیتالی و جرم رایانه ای(علم قانونی، رایانه‌ها و اینترنت)، ترجمه امیرحسین جلالی فراهانی و علی شایان، قم، سلسبیل.

۱۱) محمدامین الشوابکه، جرائم الحاسوب والإنترنت،عمان، دارالثقافه، الطبعه الاولی/ الاصدارالثالث،۲۰۰۹

۱۲) صغیر، جمیل، الحمایه الجنائیه والمدنیه لبطاقات الائتمان الممغنطه(دراسه

تطبیقیه فی القضاء الفرنسی والمصری)، الطبعه الاولی، دارالنهضه العربیه، القاهره، ۱۹۹۹.

۱۳) زرکلام، ستار، قانون تجارت الکترونیکی و الفبای الکترونیکی،مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات، معاونت حقوقی و توسعه قضایی قوه قضائیه، قم، سلسبیل، چاپ نخست، ۱۳۸۴

۱۴) قاجار قیونلو، سیامک، مقدمه‌ای بر زیر ساخت کلید عمومی / PKI : http://www. Irannamaye.ir

۱۵) تارنمای گسترش آنلاین، ۱۱ مهر ۱۳۹۰

۱۶) Ian Walden, Computer Crime And Information Misuse, Computer Law, Oxford University Press, Six Edition, Edited By: Chris Reed and John Angel,۲۰۰۷

۱۷) Chris Reed, ELECTRONIC COMMERCE, Computer Law, Oxford University Press, Six Edition, Edited By: Chris Reed and J