جعل در بستر فناوریهای اطلاعات و ارتباطات*

□ فاطمه قنّاد[۱]

چکیده

ورود به عصر فناوری اطلاعات و ارتباطات، چالشهای فراوانی را فراروی جوامع بشری گسترده است. همزمان با تحول ابزارها و روشهای زندگی اجتماعی، با تحولات چشمگیری در عرصهٔ ارتکاب جرایم روبه‌رو هستیم. امروزه با گونه‌های نوینی از جرم جعل در رایاسپهر[۲] مواجهیم که با استفاده از راهکارهای فنی از سوی متخصصان بزهکار ارتکاب می‌یابد و مبارزه با آن نیازمند کسب مهارتهای علمی و عملی بی‌شماری است. اوصاف و ارکان جعل رایانه‌ای، ابتدا در سال ۱۳۸۲ به موجب مادهٔ ۶۸ قانون تجارت الکترونیکی مطرح گردید و سپس با تصویب مادهٔ ۶ قانون جرایم رایانه‌ای در سال ۱۳۸۸، به عنوان یکی از جرایم قابل ارتکاب در فضای مجازی به قانون مجازات

* تاریخ دریافت: ۱۳۹۱/۱/۲۷ ـ تاریخ پذیرش: ۱۳۹۱/۳/۲۵.

۱. استادیار دانشگاه علم و فرهنگ (ghanad@gmail.com).

۲. رایاسپهر، معادل واژهٔ بیگانه (cyber space) است که به تصویب فرهنگستان زبان و ادبیات فارسی رسیده است. اصطلاح فضای مجازی نیز امروزه رواج عرفی دارد و تا کنون چندین مقالهٔ پژوهشی با بهره‌گیری از این اصطلاح به چاپ رسیده است.

اسلامی ملحق شد. این جرم در بستر فناوری اطلاعات و ارتباطات و با بهره‌گیری از روشهای فناورانه تحقق می‌یابد و در نتیجهٔ آن صحت و تمامیتِ داده‌پیام به عنوان بنیادی‌ترین رکن جامعهٔ اطلاعاتی مخدوش می گردد. هدف این مقاله تبیین و شناسایی ماهیت این جرم در مقایسه با جعل سنتی و بیان خصوصیات و چگونگی روشها و فنونی است که به عنوان عملیات اجرایی جرم مزبور از سوی بزهکاران قابل ارتکابند و آشنایی با آن جامعهٔ حقوقی را در تحلیل صورتهای علمی و فنی ارتکاب این جرم یاری خواهد کرد.

واژگان کلیدی: فناوری اطلاعات، رایاسپهر/ فضای مجازی، داده‌پیام، جعل رایانه‌ای.

مقدمه

ارتکاب جعل در جریان تراکنشها و ارتباطات الکترونیکی از جرایمی است که با پیشرفتهای حاصل از فناوری اطلاعات و ارتباطات[1] پیوستگی و ارتباط تنگاتنگی دارد و جرمی مبتنی بر فناوری برتر به شمار می‌رود. از این رو، در اسناد بین‌المللی (کنوانسیون بوداپست، ۲۰۰۱: مادهٔ ۶؛ گزارش بانکوک، ۲۰۰۵: بند ف، مادهٔ ۳۲۷) در دسته‌بندی جرایم مرتبط با رایانه قرار می گیرد و علت انتخاب عنوان جعل رایانه‌ای،[2] در متن

۱. فناوری عبارت است از کلیهٔ فعالیتهای تولیدی و خدماتی که هدف آن کسب سود یا منفعت است یا در نهایت به آن منجر می‌شود و بالا بردن توان رقابتی، ارتقای رفاه عمومی، افزایش قابلیت دفاعی، بهره‌برداری صحیح از منابع طبیعی، حفظ محیط زیست و ارتقای فرهنگ، روابط و ساختارهای اجتماعی از کاربردهای آن است (کاستلز، ۱۳۸۰: ۲۵۹). فناوری اطلاعات، مجموع ابزارها، ماشینها، دانش فنی، روشها و مهارتهای استفاده از آنها در تولید، داد و گرفت، پردازش، انباشت، بازیافت، جابه‌جایی، انتقال و مصرف اطلاعات، از ساده‌ترین تا پیچیده‌ترین و از ابتدایی‌ترین تا پیشرفته‌ترین مراحل اطلاعاتی است. در یک تعریف فنی‌تر، فناوری اطلاعات عبارت است از: کاربرد رایانه (سخت‌افزار و نرم‌افزار)، مخابرات، رادیو و تلویزیون و الکترونیک نوری (فیبرهای نوری و انتقال لیزری) و ریزالکترونیک (مدار یک‌پارچه، تراشه‌ها، ریزپردازنده‌ها، رایانه‌های شخصی و نظایر آن) برای تبادل اطلاعات.

۲. قانون، عنوان جعل رایانه‌ای را انتخاب کرده است. این عنوان، دقیق به نظر نمی‌رسد؛ زیرا این جرم صرفاً از طریق رایانه ارتکاب نمی‌یابد بلکه کلیهٔ ابزارها و واسطه‌های الکترونیکی در بستر فناوریهای اطلاعات و ارتباطات، امکان تحقق جرم جعل در فضای مجازی را فراهم می کنند. لذا عنوان جعل الکترونیکی به مقصود نزدیک‌تر است. در کنوانسیون جرایم قابل ارتکاب در فضای مجازی، عنوان کلی جعل مرتبط با رایانه انتخاب شده است که خود زیرمجموعهٔ جرایم قابل ارتکاب در فضای ←

قانون تجارت الکترونیکی ۱۳۸۲ و قانون جرایم رایانه‌ای ۱۳۸۸ نیز الگوبرداری از ادبیات بین‌المللی در این مورد است. این دو قانون در حوزهٔ جعل رایانه‌ای مکمل یکدیگر محسوب می‌شوند و عنصر قانونی این جرم را باید در متن هر دو قانون جستجو و تحلیل کرد.

بسیاری از اعمال مجرمانه‌ای که در فضای فیزیکی و ملموس قابل تحقق هستند، در فضای مجازی نیز امکان‌پذیرند. ارتکاب جرایم در فضای مجازی، با تکیه بر ابزارهای ناشی از پیشرفت علوم و فناوریهای اطلاعات و ارتباطات امکان‌پذیر است و شبکه‌های اطلاع‌رسانی رایانه‌ای مانند اینترنت یا شبکه‌های محلی تلفن همراه، بستر مناسبی را برای بسیاری از فعالیتهای مجرمانه، به ویژه انواع سازمان‌یافتهٔ آن فراهم کرده است. ارتکاب جرایم در این فضا، از برخی جهات آسان‌تر و فرار از پیامدهای قضایی آن به مراتب امکان‌پذیرتر است. جرایم اقتصادی و مالی یکی از انواع این

← مجازی یا جرایم سایبر است. این عنوان، نسبت به عنوان جعل رایانه‌ای دقیق‌تر است، زیرا این جرم در فضای مجازی و در بستر مبادلات الکترونیکی، به نوعی در ارتباط با رایانه نیز قرار می‌گیرد. در این جرم، اطلاعات، نرم‌افزارها، سیستم‌های رایانه‌ای و عملکرد آن، از جمله چیزهایی است که مورد توجه و سوء استفادهٔ جاعل قرار می‌گیرد. برخی نویسندگان معتقدند که اصطلاح جرم رایانه‌ای در مقایسه با اصطلاحاتی نظیر جرم اینترنتی، سایبری، شبکه‌ای و نرم‌افزاری، مناسب‌تر به نظر می‌رسد و کلیهٔ جرایمی را که اینترنت در آن نقش ایفا می‌کند، در بر می‌گیرد و از آنجا که اینترنت متشکل از شبکه‌های محلی و منطقه‌ای است که کاملاً وابسته به رایانه و سیستمهای رایانه‌ای هستند، جرم رایانه‌ای، کلیهٔ اشکال جرایم فضاهای فوق را در بر می‌گیرد و از این منظر جعل رایانه‌ای نیز اصطلاح قابل توجیهی است (عالی‌پور، ۱۳۸۳: ۲۰۶ـ۲۰۸). ولی به عقیدهٔ نگارنده، از آنجا که عنصر مادی این جرم، در بستر مبادلات الکترونیکی رخ می‌دهد و برنامه‌ها و سیستمهای رایانه‌ای در کنار وسایل ارتباط از راه دور، همگی از ابزارهای ارتکاب جرم هستند، عنوان جعل الکترونیکی مفهوم عام‌تری است که تمامی این حوزه‌ها را در بر می‌گیرد و نسبت به سایر اصطلاحها مناسب‌تر است. اتحادیهٔ اروپا نیز در گزارش توجیهی توصیه‌نامهٔ شمارهٔ R-95 مصوب ۱۹۹۵ خود، اصطلاح جرم فناوری اطلاعات را به‌کار برده است که با یک سیستم رایانه‌ای قابل ارتکاب است (خرم‌آبادی، ۱۳۸۴: ۵۴ـ۵۵؛ پاکزاد، ۱۳۸۴: ۸۴ـ۸۶). این سیستم می‌تواند هدف یا بستر ارتکاب جرم باشد و یا دلایل ارتکاب جرم از این محیط قابل جمع‌آوری باشد. در گزارش یازدهمین کنگرهٔ پنج‌سالانه پیشگیری از جرم و عدالت کیفری سازمان ملل متحد نیز این جرم در دسته‌بندی جرایم مرتبط با رایانه قرار گرفته است (گزارش کنگرهٔ یازدهم بانکوک، ۲۰۰۵: مادهٔ ۳۲۷). فایدهٔ این بحث بیشتر از جنبهٔ نظری است و قانون تجارت الکترونیکی مصوب ۱۳۸۲ و قانون جرایم رایانه‌ای مصوب ۱۳۸۸ اصطلاح جعل رایانه‌ای را برگزیده است.

جرایم تلقی می‌شوند و موضوع رشتهٔ مطالعاتی مستقلی را تحت عنوان حقوق کیفری اقتصادی تشکیل می‌دهند.[۱] ارزشهایی که مورد حمایت این حقوق قرار می‌گیرند، غالباً ماهیتی فنی دارند. ضمانت اجرای این جرایم نیز عمدتاً جنبهٔ مالی دارد و در قالب جریمه متبلور می‌شود (Ruggiero, 2007: 8-11).

این جرایم که اصطلاحاً جرایم «یقه‌سفیدی» نامیده می‌شوند، ویژگیهای خاصی دارند که ناشی از طبقهٔ اجتماعی و وضعیت بزهکاران آن است (Croall, 2009: 8). بیشتر این جرایم در فضای محرمانه و خلوت کاری افراد اتفاق می‌افتند و به ندرت کشف می‌شوند؛ زیرا حضور فرد تاجر در صحنهٔ جرم کاملاً قانونی و مشروع است (Clarke, 2007: 21) و رویداد جرم در جریان فعالیت حرفه‌ای وی با تکیه بر تجربه و دانش حرفه‌ای، علمی یا توان مالی بزهکار (Croall, 2009: 8) و سوء استفاده از اطمینان بزه‌دیده صورت می‌پذیرد (Shapiros, 1990: 55/346-365).

به گزارش یازدهمین کنگرهٔ پنج سالانهٔ پیشگیری از جرم و عدالت کیفری سازمان ملل متحد در سال ۲۰۰۵، جرایم اقتصادی و مالی که به پیشرفتهای فناوری اطلاعات و پدیدهٔ جهانی شدن متکی هستند (Ruggiero, 2007: 9)، آثار منفی کوتاه‌مدتی بر اقتصاد و درازمدتی بر حاکمیت مطلوب می‌گذارند (گزارش بانکوک، ۲۰۰۵: بند ۱۷۸). جرایم اقتصادی و مالی در عصر فناوریهای اطلاعات و ارتباطات، یکی از عناوین این گزارش را تشکیل داده است (Ruggiero, 2007: 9). با آنکه جرم جعل، بیشتر با هدف کسب منافع مالی انجام می‌شود و در بسیاری موارد به بردن مال بزه‌دیده منجر می‌گردد، در زمرهٔ جرایم علیه آسایش عمومی قرار دارد (میرمحمدصادقی، ۱۳۸۵: ۲۴۰)، زیرا ارتکاب آن علاوه بر زیانهای مالی که بر افراد جامعه تحمیل می‌کند، موجب سلب آسایش عمومی شده و اعتماد شهروندان به بنیانهای اقتصادی، اداری و قضایی جامعه را متزلزل می‌سازد (همان: ۱۲).

۱. بخش دیگر از اعمال مجرمانه‌ای که ذیل این عنوان، مورد بررسی قرار می‌گیرند، ناظر بر حیات اقتصادی جامعه هستند. جرایم مربوط به تخلفات شرکتها و تقلّبهای مالیاتی در این زمره‌اند. دستهٔ سوم از این جرایم، ناظر بر نظم اقتصادی جامعه هستند. جرایم رشا و ارتشا، ربا، نقض حقوق مصرف‌کنندگان، نقض حقوق رقابتی و قواعد تبلیغات تجاری و تبلیغات خلاف واقع، در این دسته‌بندی جای می‌گیرند.

علی‌رغم تفاوتهایی که در روشهای ارتکاب عنصر مادی، میان جعل سنتی و جعل مبتنی بر فناوریهای اطلاعات و ارتباطات (حاج فتحعلیها، ۱۳۷۲: ۴۶؛ Tanaka, 2005: 5) وجود دارد، شباهتهایی نیز میان جعل مرتبط با رایانه و جعل در مفهوم سنتی آن وجود دارد که یکی از آنها قلب حقیقت و مخدوش کردن و تغییر دادن واقعیت است تا به وسیلهٔ آن، امر خلاف واقعی را حقیقی قلمداد و در مراجع مختلف به عنوان یک امر معتبر، مورد استفاده قرار گیرد (میرمحمدصادقی، ۱۳۸۵: ۲۴۲ـ۲۴۳). به علاوه بسته به اینکه دگرگون‌سازی حقیقت، در بُعد مادی و محسوس قابل رؤیت باشد یا به صورت قلب حقیقت در مفاد و شرایط و محتوای موضوع جعل، بدون هرگونه خدشهٔ ظاهریِ قابل رؤیت، انجام شده باشد، جرم جعل مادی یا مفادی تحقق می‌یابد (همان: ۲۶۴ـ۲۹۰).

و بالاخره آخرین شباهت در عنصر مادی، مربوط به رکن ضرری هر دو جرم است. به عبارت دیگر، همچون جعل در مفهوم سنتی کلمه، زمانی جرم جعل مرتبط با رایانه محقّق می‌شود که علاوه بر قلب حقیقت، به یکی از روشهای مندرج در قانون، داده‌پیامِ تولیدشده قابلیت بالقوه و امکان اضرار به اشخاص حقیقی یا حقوقی را داشته باشد (همان: ۲۹۶)، هرچند عملاً ضرر ایجاد نشده و صرفاً امکان تحقق آن در آینده وجود داشته باشد و اعم از اینکه ضرر مادی یا معنوی (همان: ۳۰۳)، نسبت به اشخاص حقیقی یا حقوقیِ دولتی یا غیر دولتی قابل تحقق باشد.[۱] پس ایراد ضرر بالفعل، در تحقق هر دو جرم شرط نیست (همان: ۲۹۳ـ۳۱۴؛ گلدوزیان، بی‌تا: ۳۹۱ـ۴۱۰؛ ولیدی، بی‌تا: ۲۱۴ـ۲۷۳).

دربارهٔ عنصر روانی این جرم نیز باید گفت که لازم است جاعل، سوء نیت عامِ انجامِ فعل مجرمانه و قلب حقیقت را همراه با سوء نیت خاصِ فریب اشخاص داشته باشد. سوء نیت خاص اینکه محصول جرم را به عنوان شیء اصلی قلمداد و از این راه به ضرر خود عمل نمایند (میرمحمدصادقی، ۱۳۸۵: ۳۱۲). از آنجا که سوء نیت خاص با رکن نتیجه ملازمه دارد، در این جرم، قصد ایراد هر نوع ضرر به غیر به عنوان سوء

۱. رأی شمارهٔ ۵۱۳ مورخ ۱۳۲۶/۴/۹ و رأی شمارهٔ ۱۳۰۵ مورخ ۱۳۱۸/۶/۶ شعبهٔ دوم دیوان عالی کشور.

نیتِ خاصِ جرم جعل کفایت می‌کند (همان: ۳۱۳). تحقّق ضرر یا امکان ایراد ضرر مادی یا معنوی به اشخاص حقیقی یا حقوقی، دو رکن اساسی عنصر روانی این جرم به‌شمار می‌رود و مسلماً احراز آن با دادگاه خواهد بود. با وجود شباهتهایی که بیان شد، بررسی عناصر قانونی این دو جرم مبیّن تفاوتهایی است که به تفاوت در ساختار و روش ارتکاب جرم منجر می‌شود. هدف اصلی مطالب مندرج در این نوشتار تبیین روشهای عملی و فنی ارتکاب جعل در رایاسپهر و شناسایی آن به جامعهٔ حقوقی است.

الف) مقایسهٔ ساختاری جعل سنتی و جعل رایانه‌ای

در مقام مقایسه میان دو جرم باید خاطرنشان کرد که جعل رایانه‌ای چند ویژگی اساسی دارد که آن را از جعل سنتی متمایز می‌سازد. نخست اینکه بستر ارتکاب این جرم، مبادلات الکترونیکی است؛ یعنی بزهکار با بهره‌گیری از فناوریهای اطلاعات و ارتباطات و ابزارهای متنوع آن، نظیر برنامه‌ها و سیستمهای رایانه‌ای و وسایل کاربردیِ سیستمهای رمزنگاریِ تولید امضا (قناد، ۱۳۸۵: ۵۹ـ۶۷) اسباب تحقق این جرم را فراهم می‌سازد و دوم اینکه روشهای ارتکاب این جرم نیز همچون بستر ارتکاب آن الکترونیکی است و با ارتکاب افعالی نظیر ورود، تغییر، محو و توقف داده‌پیام و سیستمهای رایانه‌ای یا استفاده از وسایل کاربردیِ سیستمهای رمزنگاریِ تولید امضا و نظایر آن، که همگی بر فناوریهای اطلاعات و ارتباطات مبتنی هستند، عملی می‌شود و محصول مجرمانهٔ حاصل از به کارگیری ابزارها و انجام اقدامات فوق نیز ایجاد پیام غیر واقعی است که دارای ارزش مالی و اثباتی است و مرتکب می‌تواند با ارائهٔ آن به مراجع مختلف، از به کارگیری آن به عنوان داده‌پیام معتبر بهره‌مند شود. به عبارت دیگر، این جرم در زمرهٔ جرایم مبتنی بر فناوری برتر قرار دارد و بدون استفاده از فناوریهای اطلاعات و ارتباطات و ابزارهای متنوع آن ظهور خارجی نمی‌یابد.

به موجب مادهٔ ۶۸ قانون تجارت الکترونیکی:

هر کس در بستر مبادلات الکترونیکی، از طریق ورود، تغییر، محو و توقف

داده‌پیام و مداخله در پردازش داده‌پیام و سیستمهای رایانه‌ای و یا استفاده از وسایل کاربردی سیستمهای رمزنگاری تولید امضا ـ مثل کلید اختصاصی ـ بدون مجوز امضاکننده و یا تولید امضای فاقد سابقهٔ ثبت در فهرست دفاتر اسناد الکترونیکی و یا عدم انطباق آن وسایل، با نام دارنده در فهرست مزبور و اخذ گواهی مجعول و نظایر آن اقدام به جعل داده‌پیامهای دارای ارزش مالی و اثباتی نماید تا با ارائهٔ آن به مراجع اداری، قضایی، مالی و غیره به عنوان داده‌پیامهای معتبر استفاده نماید، جاعل محسوب و به مجازات حبس از یک تا سه سال و پرداخت جزای نقدی به میزان پنجاه میلیون (۵۰/۰۰۰/۰۰۰) ریال محکوم می‌شود.

تبصره ـ مجازات شروع به این جرم حداقلِ مجازات مقرر در این ماده می‌باشد.

مادهٔ ۶ قانون جرایم رایانه‌ای که از بسیاری جهات مکمل قانون تجارت الکترونیکی تلقی می‌شود در تعریف جعل رایانه‌ای چنین مقرر می‌دارد:

هر کس به طور غیر مجاز 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 وارد کردن متقلبانهٔ داده به آنها.

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

ملاحظه می‌شود که عنصر مادی این جرم در بخشی از مواد مذکور تولید یا تغییر داده‌پیام است. بنابراین در این صورت و نیز در مواردی که بزهکار اقدام به تغییر علایم موجود در کارتهای حافظه یا سامانه‌های رایانه‌ای و مخابراتی یا تراشه‌ها نموده است با توجه به تاریخ تصویب قانون جرایم رایانه‌ای و نیز مادهٔ ۵۵ آن، عمل وی تحت شمول قانون اخیر قرار می‌گیرد. مجازات مندرج در این قانون، یک تا پنج سال حبس یا جزای نقدی است و در صورت صلاحدید قاضی ممکن است حکم به هر دو مجازات داده شود. در مواردی نظیر مداخله در پردازش سیستمهای رایانه‌ای و ارتباطی، تولید امضای جعلی اشخاص و صدور گواهی مجعولِ صحت امضای الکترونیکی که مستنبط از متون قانونی، عمل مرتکب تحت شمول قانون تجارت

الکترونیکی قرار می‌گیرد، همزمان مشمول حبس و جزای نقدی خواهد بود که البته با توجه به ابعاد وسیع این جرم و نتایج زیانباری که در سطحی گسترده به بار می‌آورد، نسبت به بیشتر مجازاتهای مندرج در فصل پنجم قانون مجازات اسلامی، در خصوص جعل و تزویر، مجازات خفیف‌تری به شمار می‌رود. مجازات اصلی این اعمال مجرمانه ترکیبی از حبس و جزای نقدی اعلام شده است که توأماً مورد حکم قرار می‌گیرد. مرتکب جرم جعل علاوه بر پرداخت جزای نقدی به مبلغ پنجاه میلیون ریال جزای نقدی ثابت، به یک تا سه سال حبس نیز محکوم می‌گردد. به علاوه در هر دو صورت، دادگاه می‌تواند حسب شدت جرم و خصوصیات مجرم، نسبت به صدور مجازاتهای تتمیمی موضوع مادهٔ ۱۹ قانون مجازات اسلامی، اقدام نماید.

ملاحظه می‌شود که مجازات این جرم در مقایسه با جعل در مفهوم سنتی، ملایم‌تر تعیین شده است، ولی رویکرد قانون‌گذار همچنان بر تعیین مجازات سالب آزادی در خصوص جرم استوار است که نشانگر شدت جرم و اهمیت حمایت از جامعه در برابر ارتکاب چنین جرایمی است. به نظر می‌رسد قانون‌گذار امیدوار است تا با بهره‌گیری از ارعاب ناشی از اِعمال مجازات سالب آزادی، با گسترش روزافزون این پدیدهٔ مجرمانه مبارزه نماید.

شروع به این جرم، صرفاً در مواردی که عمل مرتکب تحت شمول قانون تجارت الکترونیکی قرار می‌گیرد قابل مجازات است و دادگاه می‌تواند مرتکب را به حداقل مجازات حبس مقرر در مادهٔ ۶۸ قانون تجارت الکترونیکی محکوم نماید و برای مدت یک سال از وی سلب آزادی نماید.

معیارهای شروع به جرم جعل رایانه‌ای نیز همچون جعل در مفهوم سنتی است. از این رو، چنانچه مرتکب عملیات اجرایی جرم را آغاز کرده و اقدام به تحریف و قلب حقیقت نماید، اما پیش از اتمام کار و ایجاد داده‌پیام مجعول، به علل غیر ارادی، از دستیابی به جرم تام و تحصیل داده‌پیام مجعول محروم بماند، این مقدار از انجام عملیات اجرایی و عدم انصراف ارادی وی، شروع به جرم را محقّق می‌سازد، مانند موردی که شخصی به منظور تحریف حقیقت، اطلاعات نادرستی را در متن داده‌پیام وارد کند و شروع به پردازش داده‌پیام نماید، ولی پیش از اتمام پردازش و

دستیابی به داده‌پیام مجعول، به عللی خارج از ارادهٔ وی، عملیات پردازش متوقف و مرتکب دستگیر شود. از آنجا که مرتکب، بیشترِ مسیر ارتکاب جرم را طی کرده و اگر این مانع نمی‌رسید، جرم تام محقّق می‌شد، این مقدار از عملیات اجراییِ انجام‌شده، وی را مشمول مجازات شروع به جرم قرار می‌دهد.

ب) روشهای فنی و عملی ارتکاب جعل رایانه‌ای

آن گونه که از مادهٔ ۶ قانون جرایم رایانه‌ای و مادهٔ ۶۸ قانون تجارت الکترونیکی استنباط می‌شود، عنصر مادی این جرم عبارت از قلب حقیقت و مخدوش کردن واقعیت از طریق ارتکاب یک سلسله عملیات فنی است. شناخت مصادیق عملی و فنی ارتکاب جعل، امکان درک بیشتر ماهیت جرم را فراهم می‌سازد و برای شناخت و تحلیل مفاد قانون و آشنایی با شرایط تحقق جرم جعل رایانه‌ای لازم است مورد بررسی قرار گیرد.

۱. قلب و مخدوش کردن حقیقت داده‌پیام

قلب حقیقت در هر دو بُعد مادی و مفادی، اصلی‌ترین جزء عنصر مادی این جرم است. منظور از آن، دگرگون کردن و تحریف واقعیت به گونه‌ای است که حقی را تضییع یا ناحقی را اثبات نماید، اعم از اینکه آثار تحریف حقیقت، از طریق فعل مادی بر روی داده‌پیام باقی و مشهود باشد، مانند موردی که داده‌پیامِ خلافِ واقعی ایجاد کرده یا داده‌پیام موجود را از طریق ارتکاب اعمالی نظیر ورود، محو و توقف با تغییرات اساسی همراه نماید و از این طریق داده‌پیامی را که دارای ارزش مالی و اثباتی است جعل مادی کند یا اینکه عمل مرتکب، بدون هیچ گونه آثار خارجی انجام شود، یعنی بی‌آنکه تغییری در ظاهر داده‌پیام ایجاد گردد و تحریف مادی صورت پذیرد، مفاد و شرایط آن تحریف شده و امر باطلی صحیح یا صحیحی باطل جلوه داده شود، همچون موردی که مأموران مالیاتی یا متصدیان دفاتر رسمی، هنگام انجام وظایف خود در خصوص وارد کردن اطلاعات مربوط به داده‌پیام، مرتکب جعل شده و مطالب خلاف واقعی را در متن داده‌پیامهایی که حسب قانون

مکلّف به ایجاد آن هستند وارد نموده و مورد پردازش قرار دهند یا بخشی از حقایق موجود را حذف و داده‌ها را از مسیر پردازش خارج نمایند و به وسیلهٔ آن حقی را تضییع یا ناحقی را اثبات نمایند. در چنین صورتی عمل مرتکب جعل مفادی تلقی و مشمول مجازات خواهد بود.[۱] قلب حقیقت، به شیوه‌های زیر انجام می‌شود:

۱ـ۱. ورود، تغییر، محو و توقف داده‌پیام

این اَعمال باید حقیقت و واقعیت را دگرگون کرده و منجر به تولید،[۲] ذخیره و در موارد مقتضی ارسال[۳] داده‌پیامی شود که با استفاده از آن در مراجع مختلف، بتوان اموالی تحصیل یا ناحقی را اثبات کرد. از این رو، چنانچه در نتیجهٔ اَعمال یادشده، چنین داده‌پیامی ایجاد نشود، عمل مرتکب مشمول مجازات نخواهد بود.

منظور از ورود، وارد کردن اطلاعات ناصحیح و خلاف حقیقت به رایانه یا کارتهای حافظه یا سامانه‌های مخابراتی یا تراشه‌های رایانه‌ای جهت پردازش[۴] اطلاعات[۵] یا مفاهیم، اعم از متن، صدا و تصویر برای ایجاد داده‌های قابل استناد یا واردکردن متقلبانهٔ داده به داده‌های موجود در آنهاست. اعم از اینکه با ورود اطلاعات و پردازش نهایی توسط رایانه، تحریف و جعل حقایق در داده‌پیام محسوس و رؤیت‌پذیر باشد یا اینکه بدون هیچ تغییری در ظاهر داده‌پیام، مفاد و شرایط آن تحریف شده و امر باطلی صحیح یا صحیحی باطل جلوه داده شود، عمل

۱. قانون‌گذار از عبارت کلّیِ جعل استفاده کرده و تمامی اَعمال فوق را مشمول مجازات قرار داده است و فایدهٔ این بحث فقط از جهات نظری است.

۲. تولید: ایجاد فایلهای متشکل از داده به شکل متن، اعداد یا گرافیک، نگهداری و ذخیرهٔ اطلاعات از طریق رسانه‌های فیزیکی، مانند لوحهای نوری، نوارهای مغناطیسی و نرم‌افزارهایی که چنین امکانی را فراهم می‌سازند (لاودن، ۱۳۸۶: ۹).

۳. ارسال: انتقال الکترونیکی اطلاعات از دستگاه ارسال‌کننده به دستگاه دریافت‌کننده (همان).

۴. پردازش: کسب، ذخیره‌سازی، دستکاری، تجزیه و تحلیل و ارائهٔ داده با ابزارهای الکترونیکی (همان).

۵. اطلاعات: داده‌هایی هستند که به شکلی معنادار و مفید سازماندهی شده و قابل درک هستند. منظور از داده، مجموعه‌ای از واقعیات خام است که هنوز به شکلی سازماندهی و منسجم نشده که افراد آن را درک و مورد استفاده قرار دهند. سیستم اطلاعاتی مجموعه‌ای از اجزای وابسته به هم می‌باشد که اطلاعات را جمع‌آوری، پردازش، ذخیره و توزیع می‌کند و آن را قابل استفاده می‌نماید. یک سیستم اطلاعاتی از فناوریهای اطلاعات بهره می‌گیرد تا به هدف برسد (همان: ۶).

مرتکب در هر دو صورت، مشمول عنوان مجرمانهٔ جعل خواهد بود.

در مادهٔ ۷ کنوانسیون جرایم قابل ارتکاب در فضای مجازی نیز ورود هرگونه اطلاعات رایانه‌ای چنانچه به تولید داده‌پیام جعلی و ناصحیح منجر شود، عمل مجرمانه تلقی می‌شود. صِرف ایجاد داده‌پیام جعلی که به عنوان داده‌پیام معتبر قابل بهره‌برداری باشد، صرف نظر از اینکه مستقلاً قابل خواندن و درک باشد یا خیر، عمل مرتکب را مشمول عنوان مجرمانه قرار می‌دهد.

تغییر در داده‌پیام نیز مشتمل بر انجام اقداماتی به منظور دگرگون‌سازی داده‌پیام و روند پردازش آن است، به گونه‌ای که در نتیجهٔ اقدامات انجام‌شده، داده‌پیامی متفاوت از داده‌پیام اصل و حقیقی ایجاد شود که البته قابل بهره‌برداری به عنوان داده‌پیام معتبر باشد. به عبارت دیگر، ایجاد تغییر و دگرگونی در ماهیت یا مفاد و شرایط داده‌پیام باید به گونه‌ای باشد که داده‌پیام را از حیّز انتفاع ساقط نکرده و نتیجهٔ عمل، ایجاد داده‌پیامی قابل مقایسه با داده‌پیام معتبر بوده و قابل استفاده در مراجع مختلف باشد.[۱] تغییر داده‌ها یا علایم موجود در کارتهای حافظه یا داده‌های قابل پردازش در سامانه‌های رایانه‌ای یا مخابراتی یا تراشه‌ها، یکی دیگر از مصادیق این جرم تلقی می‌شود که در مادهٔ ۶ قانون جرایم رایانه‌ای احصا گردیده است. مادهٔ ۷ کنوانسیون جرایم قابل ارتکاب در فضای مجازی نیز تغییر در اطلاعات رایانه‌ای را چنانچه به ایجاد داده‌پیام جعلی منجر شود و به عنوان داده‌پیام معتبر و قانونی قابل استفاده باشد، عملی مجرمانه تلقی کرده است.

محو داده‌پیام نیز عبارت از حذف دائمی اطلاعات است، به گونه‌ای که قابل بازسازی و بهره‌برداری مجدد نباشد. محو و حذف بخشی از داده‌پیام و پردازش مجدد آن، به تنهایی یا در کنار سایر داده‌پیام‌ها، باید منجر به ایجاد وضعیتی شود که در نتیجهٔ آن، ناحقی اثبات یا حقی تضییع شود و عنوان تغییر داده‌پیام بر آن صدق کند که در این صورت، مشمول مادهٔ ۶ قانون جرایم رایانه‌ای می‌گردد.

از این رو، در موردی که شخص با محو بخشی از داده‌پیامی که برائت ذمهٔ

---

۱. برای مقایسه با تغییر (Alteration) در جرم جعل در مفهوم سنتی کلمه، ر.ک: گلدوزیان، بی‌تا: ۴۰۵؛ ولیدی، بی‌تا: ۲۴۰؛ میرمحمدصادقی، ۱۳۸۵: ۲۵۸ـ۲۵۹.

شخص ثالثی را گواهی می‌کند، داده‌پیام ظاهراً معتبری ایجاد می‌نماید و خود را مجدداً طلبکار نشان می‌دهد، مرتکب عمل جعل شده است.[1]

در مادهٔ ۷ کنوانسیون جرایم قابل ارتکاب در فضای مجازی نیز محو داده‌پیام چنانچه به ایجاد داده‌پیام جعلی با ظاهری معتبر منجر شود، به عنوان عمل مجرمانه اعلام گردیده است.

منظور از توقف داده‌پیام، اختفای تمام یا بخشی از داده‌ها به گونه‌ای است که عمل پردازش را از مسیر عادی خارج و مانع از عملکرد صحیح سیستمها و پردازش دقیق اطلاعات شود. پردازش چنین اطلاعاتی منجر به حصول نتایج غیر واقعی شده و داده‌پیام ایجادشده از این طریق، هیچ گونه انطباقی با واقعیت نخواهد داشت، ولی چنانچه به عنوان داده‌پیام معتبر قابل استفاده باشد، داده‌پیام مجعول تلقی می‌شود. از این رو، مثلاً در مواردی که مرتکب با موقوف‌سازی بخشی از اجزای داده‌پیامهای تجاری، در خصوص مشخصات کالاها، خدمات، مشخصات واحد بازرگانی یا تاجر و مسئول بنگاه تجاری، داده‌های تفصیلی را از مسیر پردازش خارج و از این طریق، داده‌پیام ظاهراً معتبری ایجاد می‌نماید، مرتکب جعل شده است. در مادهٔ ۷ کنوانسیون جرایم قابل ارتکاب در فضای مجازی نیز موقوف‌سازی داده‌پیام به عنوان عنصر مادی جرم جعل شناسایی شده است.

۲ـ۱. مداخله در پردازش داده‌پیام و سیستم رایانه‌ای

سیستم رایانه‌ای مجموعه‌ای از عناصر سخت‌افزاری و نرم‌افزاری است که برای انجام کار خاصی از جمله فعالیتهای مخابراتی یا سامانه‌های پردازشگری با هم کار می‌کنند. هرگونه مداخله در عملکرد سیستم سخت‌افزاری یا عملیات پردازش داده‌پیام و سیستمهای نرم‌افزاری رایانه‌ای می‌تواند رایانه را از مسیر پردازش صحیح داده‌پیام خارج کند و کارکردهای اساسی سیستم سخت‌افزاری رایانه را مختل نماید. این عمل، مداخله در عملکرد سیستم رایانه‌ای و پردازش داده‌پیام تلقی می‌شود. این امر در مادهٔ ۵

۱. برای مقایسه با محو در سند یا نوشته و ارتکاب عنصر مادی جرم جعل در مفهوم سنتی، ر.ک: گلدوزیان، بی‌تا: ۴۰۷؛ ولیدی، بی‌تا: ۲۳۳.

کنوانسیون جرایم قابل ارتکاب در فضای مجازی نیز مورد اشاره قرار گرفته است.

مداخله در پردازش داده‌پیام و سیستم رایانه‌ای، چنانچه منتهی به ایجاد داده‌پیام جعلی شود و امکان استفاده از آن به عنوان داده‌پیام معتبر وجود داشته باشد، عمل مرتکب را مشمول مجازات قرار می‌دهد.

۳ـ۱. صدور و تولید جعلی امضای اشخاص

استفاده از وسایل کاربردی سیستمهای رمزنگاری تولید امضا ـمثل کلید اختصاصی‌ـ بدون مجوز امضاکننده، عین عبارت قانون در مقام بیان یکی از مصادیق عنصر مادی جعل رایانه‌ای است. طبق بند ی مادهٔ ۲ قانون تجارت الکترونیکی مصوب ۱۳۸۲، امضای الکترونیکی عبارت از هر نوع علامت متصل به داده‌پیام است که برای شناسایی امضاکننده مورد استفاده قرار می‌گیرد[۱] (زرکلام، ۱۳۸۵: ۲۸۹؛ Brazell, 2008: 77-78) و اگر دارای برخی اوصاف و شرایط قانونی و فنی خاص باشد، امضای الکترونیکی مطمئن نامیده می‌شود و از این نظر با امضای دست‌نویس که زیر اسناد کاغذی درج می‌گردد و در دفاتر اسناد رسمی گواهی می‌شود، تفاوت چندانی ندارد.

امضای الکترونیکی باید دارای اوصاف و عملکردهای خاصی باشد. نخست آنکه مشخص‌کنندهٔ هویت امضاکننده باشد و سایر اشخاص امکان استفاده از آن را نداشته باشند. دوم اینکه عمل مثبتی باشد که به مفهوم تصدیق صحت معامله است (Ibid.: 12) و چنانچه به گونه‌ای اعمال شود که موجب اصالت امضا و مدرک باشد و امکان انکار و تکذیب یا تغییر آن وجود نداشته باشد «امضای مسلّم الصدور» تلقی می‌شود (جعفری لنگرودی، ۱۳۷۶).

وجود امضا در زیر نوشته یا سند، جزئی از شرایط شکلی اعتبار سند است و

---

۱. این تعریف، نسبتاً با تعریف مندرج در بند یک مادهٔ ۲ دستورالعمل شمارهٔ ۹۹/۹۳ مصوب ۱۹۹۹ پارلمان و شورای وزیران اتحادیهٔ اروپا در خصوص امضای الکترونیکی و بیشتر با مادهٔ ۷ قانون نمونهٔ کمیسیون حقوق تجارت بین‌الملل سازمان ملل متحد در خصوص تجارت الکترونیکی مصوب ۱۹۹۶ و بند الف مادهٔ ۲ قانون نمونهٔ کمیسیون حقوق تجارت بین‌الملل سازمان ملل متحد دربارهٔ امضای الکترونیکی مصوب ۲۰۰۱ مطابقت دارد. تجزیه و تحلیل تعاریف فوق نشان می‌دهد که امضای الکترونیکی، داده‌ای الکترونیکی است که به سایر داده‌های الکترونیکی منضم یا به طور منطقی مرتبط شده و رابطهٔ امضاکننده را با آن داده‌ها مشخص می‌کند.

تصدیق صحت و اصالت امضا، به عنوان ابزاری جهت پیشگیری از ادعای انکار یا تردید و حتی جعل تلقی می‌شود. نتیجهٔ چنین فرایندی، ایجاد «امضای مسلم الصدور» است که هیچ گونه دعوای انکار یا تردید، علیه آن مسموع نیست (*قانون آیین دادرسی مدنی*، مادهٔ ۲۲۵). امضای الکترونیکی نیز از این امر مستثنا نبوده و برای اینکه واجد آثار حقوقی باشد و صدور آن به مفهوم شناسایی هویت امضاکننده و اصالت امضا و مدرک باشد و عملی مثبت قلمداد شود، باید از یک سلسله شرایط شکلی برخوردار باشد و چون امری مبتنی بر فناوری است، باید از قواعد فنی خاصی نیز تبعیت نماید (قناد، ۱۳۸۵: ۶۵ـ۶۶). هدف از وضع شرایط قانونی برای اعتبار بخشیدن به امضای الکترونیکی و به ویژه تولید و صدور امضای الکترونیکی مطمئن، تضمین تمامیت، دوام و امضاپذیری اسناد الکترونیکی است. بر این اساس، اسناد الکترونیکی که بدین نحو امضا شده‌اند، اعتباری همسان با اسناد کاغذی با امضای دست‌نویس دارند. هر اندازه کارایی سیستم فنی که برای صدور امضای الکترونیکی استفاده شده، بیشتر باشد، تمامیت، دوام و ارتباط سند با فایلهای امضایی که برای آن ایجاد شده بیشتر است (زرکلام، ۱۳۸۵: ۲۹۱). از این رو، امضایی که طبق شروط مقرر در قانون صادر شده باشد، «امضای الکترونیکی مطمئن» نام می‌گیرد و همچون امضای مسلّم الصدور که ذیل اسناد کاغذی درج می‌گردد، هیچ گونه دعوای انکار یا تردید علیه آن مسموع نبوده و قابل انتساب به صادرکننده است. تفاوت امضای الکترونیکی با امضای رقمی در این نکته نهفته است که در امضای الکترونیکی هر نماد الکترونیکی که به امضا متصل شود معتبر بوده و می‌توان از کلیهٔ اشکال فناوریهای الکترونیکی سطح پایین و سطح بالا برای تولید آن بهره برد. به عنوان نمونه وقتی با استفاده از قلم نوری متن یک سند امضا می‌شود (Brazell, 2008: 38) یا در موردی که شخصی امضای مکتوب خود را در رایانه «تصویربرداری» نموده و آن را به یک نوشته «منضم» می‌کند یا حتی در موردی که شخصی نام خود را ذیل یک سند الکترونیکی درج می‌کند (Ibid.: 36)، یک سند با امضای الکترونیکی تولید نموده است و لزومی به استفاده از فنون رمزنگاری در چنین امضایی وجود ندارد. چنین امضایی اگرچه قابل جعل است، امضای الکترونیکی با استفاده از فناوری سطح پایین

تلقی می‌شود (Ibid.: 37-38). در مقابل، دو روش مبتنی بر فناوری سطح بالا نیز وجود دارد. نخست، «امضای رقمی» است که محدود به فناوری زیرساختِ کلیدهای عمومی است و با استفاده از این فناوری سطح بالا، اسناد «رمزنگاری» و به عبارتی امضا می‌شوند و سپس مورد شناسایی قرار می‌گیرند (Baker, 2008: 248-249) و از آنجا که این رمزنگاری با استفاده از یک جفت کلید عمومی و اختصاصی صورت می‌پذیرد، «رمزنگاری نامتقارن» نامیده می‌شود[۱] (Ibid.: 248-249; Brazell, 2008: 51) و دوم امضای بایومتریک یا مبتنی بر «زیست‌سنجی» که با استفاده از خصوصیات زیستی هر شخص نظیر ویژگیهای شبکیه، عنبیه یا اثر انگشت وی طراحی شده و منحصر به فرد است. وسایلی که برای ثبت ویژگیهای زیستی هر فرد به کار می‌روند، امروز به صورت تجاری خرید و فروش می‌شوند و از طریق آنها، اثر انگشت، ساختار شبکیه و عنبیهٔ چشم، خطوط کف دست، شکل رگها، میزان فشار دست بر روی کاغذ در هنگام امضا و حتی ترکیب صورت قابل ثبت و اندازه‌گیری است. این دستگاهها پس از ثبت ویژگیهای زیستی هر شخص، آن را به اطلاعات عددی تبدیل می‌کنند. به این فرایند، «رقمی‌سازی» گفته می‌شود. این ارقام، مبنای شناسایی ویژگیهای زیستی شخص در مراجعات بعدی قرار می‌گیرد. ایراد این فناوری این است که ویژگیهای جسمی انسان در اثر افزایش سن، بیماری و سایر عوامل تغییر می‌کند. فشار بیش از اندازهٔ ابزار اندازه‌گیری بر عضو ممکن است باعث صاف شدن عضو و اشکال در تعیین محدودهٔ دقیق آن گردد یا در مواردی که زخم وجود دارد، اندازه‌گیری دقیق نخواهد بود. از این رو ممکن است به واسطهٔ این اندازه‌گیری غیر دقیق، شخص مجاز، غیر مجاز اعلام شود و شخص غیر مجاز تأیید گردد. این ویژگی، نقطهٔ ضعف این

۱. رمزنگاری، روشی برای انتقال داده‌ها به گونه‌ای است که محتوای اطلاعات پوشیده مانده و امکان دسترسی و استفادهٔ غیر مجاز از اشخاص ثالث سلب شود. برای رمزنگاری، از یک یا چند پارامتر محرمانه که به آن متغیرهای رمزنگاری گفته می‌شود یا از یک جفت کلید استفاده می‌شود. اگر در رمزنگاری و رمزگشایی از یک کلید خصوصی استفاده شود، رمزنگاری متقارن تلقی می‌شود و اگر یک جفت کلید به نامهای عمومی و اختصاصی مورد استفاده قرار گیرد، رمزنگاری نامتقارن خواهد بود. رمزنگاری متقارن چندان اطمینان‌بخش نیست؛ زیرا در هر معامله میان افراد مختلف یا حتی یکسان، باید کلید جدیدی ایجاد شود و امنیت هر کلید فقط برای یک بار استفاده قابل تضمین است، حال آنکه در رمزنگاری نامتقارن، کلید اختصاصی اشخاص همیشه محرمانه باقی می‌ماند.

روش به شمار می‌رود و از این رو استفاده از روشهای رمزنگاری برای تولید امضای الکترونیکی مطمئن رایج‌تر است (Brazell, 2008: 39-49; Vacca, 2009; Liu, 2010). برخی از نظامهای قانون‌گذاری[1] (Brazell, 2008: 28-31)، استفاده از فناوری «زیرساخت کلید عمومی» را شرط صحت امضای الکترونیکی اعلام کرده و به عبارتی امضای رقمی را مورد تأیید قرار داده‌اند و برخی دیگر همانند ایران، بر فناوری خاصی تأکید نداشته و تنها معیارهای لازم را برای اعتبار بخشیدن به امضای الکترونیکی بیان نموده‌اند که البته مسیری است که به امضای رقمی ختم می‌شود (Ibid.: 35) و تحقق آن با استفاده از فناوری زیرساخت کلید عمومی امکان‌پذیر است.

این ابزار تولیدکنندهٔ امضای الکترونیکی، مبتنی بر رمزنگاری بوده[2] (Baker, 2008: 4-5) و متشکّل از یک جفت کلید عمومی و اختصاصی است که مکمّل یکدیگرند و برای رمزنگاری و رمزگشایی فایلهای اطلاعاتی الکترونیکی به کار می‌روند. این رمزنگاری، امضایی تولید می‌کند که اصطلاحاً «امضای الکترونیکی مطمئن» یا «امضای رقمی» نامیده می‌شود. «کلید عمومی» شخص، فاقد وصف محرمانگی بوده و در دنیای تجارت الکترونیکی، در دسترس عموم کاربران

۱. کشورهایی نظیر بلژیک، فرانسه، آلمان، ایرلند، فنلاند، نروژ، اسپانیا، سوئد، هلند و پادشاهی متحدهٔ انگلستان از جملهٔ این کشورها هستند.

۲. فناوری‌ای که برای رمزنگاری داده‌ها مورد استفاده قرار می‌گیرد، به عملیات هش (hash function) شهرت دارد. این عملیات، اطلاعات را به یک ارزش با اندازهٔ معین تبدیل می‌کند که ارزش هش (hash value) نامیده می‌شود. الگوریتمی که به هر داده‌پیام اختصاص داده می‌شود (hash algorythm)، منحصر به فرد است. به این صورت که برای هر حرف الفبا، یک عدد مشخص و منحصر به فرد تعیین می‌شود و متن، دوباره با این اعداد بازنویسی می‌گردد. سپس کلیهٔ اعداد با هم جمع می‌شوند و حاصل جمع، به عنوان داده‌پیام به آسانی منتقل می‌شود. حتی اگر یک حرف از این متن تغییر کند، متن جدید یک ارزش هش جدید تولید می‌کند و در نتیجه، حاصل جمع تغییر می‌کند و جعلی بودن متن معلوم می‌شود. رمزگشایی نیز به این صورت است که دریافت‌کننده، کلید اختصاصی خود یا کلید عمومی فرستنده را (حسب اینکه متن با چه کلیدی رمزنگاری شده باشد) به کار می‌برد تا اصالت امضای الکترونیکی فرستنده پدیدار شود. سپس همان الگوریتم هش را به کار می‌برد تا متن رمزنگاری‌شده، قابل رؤیت شود، آنگاه با بهره‌گیری از کلید عمومی فرستنده، متن رؤیت‌شده را رمزگشایی می‌کند و از این طریق تمامیت و اصالت متن و فرستندهٔ آن اثبات می‌شود.

قرار می‌گیرد. ولی «کلید اختصاصی»، «کد رقمیِ» محرمانهٔ شخص است که همانند اثر انگشتان وی تلقی شده و باید مورد حفاظت قرار گیرد.[۱]

برای تولید امضای الکترونیکی مطمئن با استفاده از روش رمزنگاری، امضاکننده پس از تولید داده‌پیام اعم از متن، صدا و تصویر، آن را با کلید اختصاصی خود رمزنگاری نموده و برای مخاطب ارسال می‌نماید. در این مرحله، رمزگشایی داده‌پیام صرفاً از طریق کلید عمومی شخص امضاکننده که مکمل کلید اختصاصی اوست امکان‌پذیر بوده و با هیچ روش دیگری قابل رمزگشایی نمی‌باشد. ناگفته پیداست چنانچه کلید اختصاصی امضاکننده در دسترس اشخاص دیگری قرار گیرد، امکان ایجاد اسناد جعلی با امضای دارندهٔ کلید اختصاصی و هرگونه سوء استفاده وجود دارد، از این رو محافظت از آن بسیار ضروری است. این امر در مادهٔ ۸ قانون نمونهٔ امضای الکترونیکی کمیسیون حقوق تجارت بین‌الملل سازمان ملل متحد مصوب سال ۲۰۰۱ و بند ۶ مادهٔ ۹ ویرایش دوم «شیوه‌نامهٔ اتاق بازرگانی بین‌المللی در خصوص تجارت بین‌الملل با استفاده از فناوریهای رقمی»، مورد اشاره قرار گرفته و دارندهٔ ابزارهای تولید امضا مکلّف به مراقبت و نگهداری از ابزارها بوده و در مواردی که احتمال هرگونه سوء استفاده از ابزارها وجود دارد، باید مراتب را فوراً به کلیهٔ اشخاصی که ممکن است در رابطه با چنین سوء استفاده‌هایی لطمه ببینند، اعلام نماید، وگرنه مسئول جبران خسارتهای وارده خواهد بود. از سوی دیگر، چنانچه داده‌پیام با استفاده از کلید عمومی مخاطب، رمزنگاری و برای وی ارسال شود، بازگشایی آن صرفاً از طریق کلید اختصاصی شخص مخاطب امکان‌پذیر بوده و اطلاعات آن برای هیچ کس جز مخاطب قابل درک نمی‌باشد.

خدمات مربوط به کلیدهای مزبور، به موجب مادهٔ ۳۱ قانون تجارت الکترونیکی از طریق «دفاتر خدمات صدور گواهی الکترونیکی»[۲] در اختیار درخواست‌کنندگان

---

۱. برای اطلاع بیشتر، ر.ک: <http://www.itsecurity.com/products>.

۲. تصویب آیین‌نامهٔ مربوط به تأسیس و شرح وظایف این دفاتر، مشترکاً بر عهدهٔ وزارتخانه‌های بازرگانی، ارتباطات و فناوری اطلاعات، امور اقتصادی و دارایی و دادگستری و نیز سازمان مدیریت و برنامه‌ریزی کشور است و تا کنون به تصویب نرسیده است (برای اطلاعات بیشتر در خصوص ماهیت این دفاتر، ر.ک: قناد، ۱۳۸۵: ۷۸ـ۸۵).

قرار می‌گیرد. این خدمات شامل: تولید، صدور، ذخیره، ارسال، تأیید، ابطال و به‌روزنگهداریِ گواهیهای اصالت امضای الکترونیکی می‌باشد. وظیفهٔ اصلی این دفاتر، شناسایی و تأیید هویت امضاکنندگان و اصالت امضای ایشان است که با ارائهٔ کلیدهای مزبور انجام می‌شود.

به عبارت دیگر، با استفاده از این ابزارهای فناورانه، امکان جعل امضای اشخاص یا دستیابی به متن داده‌پیامهای اختصاصی ایشان در محیط الکترونیکی، جز با دستیابی به کلید اختصاصی آنها وجود ندارد. از این روست که قانون‌گذار در مواد ۱۰ و ۱۵ قانون تجارت الکترونیکی پس از تبیین کلّیِ شرایط اختصاصیِ امضای الکترونیکی مطمئن، امضای داده‌پیام به شیوه‌های مذکور را معتبر و سند حاصله را در حکم اسناد معتبر و غیر قابل انکار و تردید دانسته است و اگرچه از عباراتی مبهم و غیر دقیق استفاده نموده، برای چنین امضایی ارزش اثباتیِ معادل اسناد رسمی قائل شده است(زرکلام، ۱۳۸۵: ۹۷ـ۹۸) و تنها امکان طرح ادعای جعل در خصوص مورد یا فقدان اعتبار به جهات قانونی را ـهمچون حجر و فوت دارندهٔ کلید در زمان استفاده از آن یا ادعای سرقت یا خیانت در امانت و سوء استفاده از کلید اختصاصی که نزد امین، امانت بوده است ـ پیش‌بینی کرده و مسلماً بار اثبات دلیل نیز بر عهدهٔ مدعی خواهد بود.

پس با استفاده از سیستم کاربردی رمزنگاری نامتقارن، عملیات مربوط به رمزنگاری و متعاقباً رمزگشایی، به وسیلهٔ یک جفت کلید عمومی و اختصاصی صورت می‌پذیرد و آنچه محرمانه و استفادهٔ غیر مجاز آن مجرمانه است، کلید اختصاصی است که یک کد رقمی کاملاً انحصاری و قابل مقایسه با اثر انگشتان شخص است و در زمرهٔ اطلاعات محرمانهٔ اشخاص قرار دارد و هرگونه استفادهٔ غیر مجاز از آن برای تولید امضا، به عنوان عنصر مادی جرم جعل قابل تعقیب است.[1] از این رو، چنانچه مرتکب با دستیابی به کلید اختصاصی شخص، امضای وی را ذیل یک سند الکترونیکی یا داده‌پیامی که به عنوان گواهی یا سند الکترونیکی قابل بهره‌برداری

۱. برای مقایسهٔ شرایط و مفهوم تولید امضای اشخاص و ارتکاب جعل در مفهوم سنتی، ر.ک: گلدوزیان، بی‌تا: ۴۰۵؛ ولیدی، بی‌تا: ۲۳۰.

است، جعل کند، اقدام وی به عنوان قلب و تحریف حقیقت قابل مجازات است.

البته با توجه به شرایط مندرج در مواد ۱۰ و ۱۵ قانون تجارت الکترونیکی، بار اثبات دلیل در ادعای جعل امضا نسبت به چنین داده‌پیامی، بر عهدهٔ دارندهٔ کلید اختصاصی است که قانوناً به عنوان امضاکنندهٔ مجاز شناخته می‌شود. چنین کاری از نظر فنی دشوار و تا حد زیادی غیر ممکن است.

۴ـ۱. اخذ گواهی صحت و اصالت امضای الکترونیکی به شیوه‌های مجعول

صدور گواهی صحت و اصالت امضای الکترونیکی، از طریق دفاتر خدمات صدور گواهی الکترونیکی صورت می‌پذیرد (قناد، ۱۳۸۵: ۷۶ـ۸۳). این تأسیس حقوقی نوین که در نتیجهٔ بهره‌مندی از فناوریهای اطلاعات و ارتباطات ایجاد گردیده، یکی از اساسی‌ترین پایه‌های تجارت الکترونیکی به شمار می‌رود. این دفاتر در بستر مبادلات الکترونیکی و در فضای مجازی جایگزین سازمانهای متولّیِ ثبت حقایق مربوط به اشخاص و دفاتر صدور گواهی صحت و اصالت امضا تلقی می‌شوند و عملیات مربوط به شناسایی هویت طرفهای معاملاتی و گواهی صحت صدور و اصالت امضای اشخاص را به عهده دارند. از این رو، تحت عنوان دفاتر اسناد الکترونیکی نیز شناخته می‌شوند. وظیفهٔ این دفاتر، تأمین و تضمین منافع و حقوق اجتماع و امنیت و صحت در روابط حقوقی و معاملات الکترونیکی اشخاص است.

روش کار این دفاتر نیز به گونه‌ای است که پس از بررسی کامل و شناسایی هویت امضاکننده، یک جفت کلید جهت صدور امضای الکترونیکی، به طور کاملاً انحصاری ایجاد و در اختیار متقاضی قرار می‌دهند و در کلیهٔ مواردی که اصالت و صحت صدور این امضا در مراجع یا نزد اشخاص مورد بررسی قرار گیرد، خدمات مربوط به تأیید اصالت و تصدیق صحت امضای الکترونیکی را که با استفاده از آن کلیدها صادر شده است، به عهده دارند و مراتب را گواهی می‌نمایند (همان: ۵۹ـ۶۶). این گواهی، معتبر و هم‌پایهٔ گواهی دفاتر اسناد رسمی کنونی در خصوص صحت امضای اشخاص است. حال چنانچه گواهی صحت امضای الکترونیکی برای امضایی صادر شود که جزئیات آن قبلاً در چنین دفاتری به ثبت نرسیده و هویت صادرکنندهٔ

آن از طریق این دفاتر بررسی و شناسایی نشده است، عمل مرتکب، صدور گواهیِ مجعول تلقی می‌شود و تحت عنوان جرم جعل، قابل پیگرد قانونی خواهد بود.

به علاوه ممکن است در برخی موارد، نام دارندهٔ امضا، در فهرست این دفاتر ثبت شده و مراحل مربوط به بررسی و شناسایی هویت وی به طور کاملاً قانونی انجام شده باشد، ولی گواهی صحت و اصالت صدور امضای الکترونیکی برای امضایی صادر شده باشد که کلید اختصاصی آن، هیچ گونه انطباقی با کلید اختصاصی متعلق به نام ثبت‌شده در فهرست ندارد. به عبارت دیگر، نام در فهرست ثبت شده، ولی امضا متعلق به آن نام نیست و مرتکب با صدور گواهی مجعول، تعلق این امضا را به نامِ ثبت‌شده در فهرست، مورد تأیید و تصدیق قرار می‌دهد. در چنین موردی، صادرکنندهٔ گواهی، مرتکب جعل شده و عمل وی مشمول مجازات قرار می‌گیرد.

۲. لزوم وجود ارزش مالی و اثباتی داده‌پیام

جرم جعل تنها در صورتی محقق می‌شود که داده‌پیامِ تولیدشده دارای ارزش مالی و اثباتی بوده و به عنوان داده‌پیام ظاهراً معتبر، قابل استناد در مراجع مختلف اداری، قضایی و... باشد و بتواند در تضییع حق و اثبات ناحقی مؤثر واقع شود. در غیر این صورت، ایجاد داده‌پیامی که قابلیت به کارگیری به عنوان داده‌پیام معتبر و تأییدشده را ندارد و یا فاقد ارزش مادی و اثباتی است و مرتکب یا شخص ثالث، با استفاده از آن منتفع نمی‌شود، جعل تلقی نمی‌گردد و ایجادکنندهٔ چنین داده‌پیامی مسئولیت کیفری نخواهد داشت.

از این رو چنانچه مرتکب، از راههای پیش‌بینی‌شده در این ماده، داده‌پیام مربوط به انتقال مالکیت اموال غیر منقولِ متعلق به اشخاص ثالث را جعل نماید یا گواهی جعلی صحت امضای خود یا امضای الکترونیکی شخص ثالثی را در ذیل چنین داده‌پیامی صادر کند و همچنین در موردی که شخص، رسیدهای خلاف واقعی را در خصوص فروش مواد دارویی به مصرف‌کنندگان نهایی، به صورت داده‌پیام ایجاد کند یا امضای الکترونیکی، در ذیل این اسناد فروش، تولید و صادر می‌نماید، عمل وی مشمول عنوان مجرمانهٔ جعل قرار نمی‌گیرد؛ زیرا به موجب بندهای الف و

ب مادهٔ ۶ قانون تجارت الکترونیکی، داده‌پیامهایی که مربوط به اسناد مالکیت اموال غیر منقول یا فروش مواد دارویی به مصرف‌کنندگان نهایی است، از نظر قانون حکم نوشته را نداشته و معتبر نمی‌باشد. از این رو به فرض تولید چنین داده‌پیامی، هیچ‌گونه نفع مالی عاید مرتکب نشده و امکان اثبات ناحق یا تضییع حقی از این طریق وجود ندارد؛ زیرا داده‌پیام تولید شده را نمی‌توان به عنوان یک داده‌پیام معتبر، در مراجع اداری، قضایی، مالی و نظایر آن مورد بهره‌برداری قرار داد. مستنبط از متن ماده این است که مبنای مسئولیت کیفری و اعمال مجازات بر مرتکب، قابلیت به‌کارگیری داده‌پیامهای غیر واقعی، به جای داده‌پیام واقعی و قابلیت استناد به آن است.

۳. اضرار به غیر

از قید لزوم وجود ارزش مالی یا اثباتی در داده‌پیام تولیدشده، می‌توان نتیجه گرفت که قلب حقیقت باید متضمن ایراد ضرر به غیر باشد. اعم از اینکه ضرر به منافع خصوصی اشخاص یا منافع عمومی جامعه وارد شود. از این رو صِرف قلب و تحریف حقیقت، بدون امکان اضرار به غیر، جعل تلقی نمی‌شود. ولی در عین حال باید توجه داشت که تحقق عملی اضرار به غیر، شرط ضروری تحقق عنصر مادی جرم جعل نیست و صِرف انجام یکی از مصادیق طرح‌شده و ارتکاب عنصر مادی این جرم برای تعقیب کیفری کافی است. به عبارت دیگر، این جرم آنی است و به محض انجام اعمال مجرمانهٔ اضرارآمیز تمام می‌شود و مرتکب قابل تعقیب است، هرچند در لحظهٔ ارتکاب، قصد فریب شخص خاصی را نداشته باشد (میرمحمدصادقی، ۱۳۸۵: ۲۹۸). از این رو گرچه احتمال ورود ضرر بالقوه برای جرم دانستن عمل ضروری است، تحقق ضرر آنی، شرط اِعمال مسئولیت کیفری نیست و عمل مرتکب، در هر صورت قابل مجازات است، هرچند ضرر یا خسارت بالفعلی وارد نیامده باشد. در چنین شرایطی، ضرر مطلقِ ناشی از ایجاد داده‌پیامهای مجعول، برای تحقق جرم کافی است و مفهوم ضرر در عنصر مادی این جرم نهفته است و تصور نهایی مرتکب از انجام جرم، بخشی از عنصر روانی است که در جای خود مورد بررسی قرار می‌گیرد.

۴. احراز عنصر روانی

جعل رایانه‌ای همانند نوع سنتی آن، جرمی عمدی است و علاوه بر سوء نیت عام و آگاهی مرتکب از ارتکاب اعمال مجرمانه، سوء نیت خاص اضرار به غیر، اعم از اشخاص حقیقی و حقوقی نیز لازم است. به عبارت دیگر، اولاً باید سوء نیت عام مرتکب به تولید و پردازش داده‌پیامهای مجعول احراز و مشخص شود که با علم و آگاهی کامل و عمداً (همان: ۳۱۲) مبادرت به قلب حقیقت و تحریف حقایق نموده است و ثانیاً باید قصد خاصِ فریب دادن دیگران را داشته و آگاه باشد که اعمال وی اضرارآمیز بوده و تولیدات مجرمانهٔ وی، قابلیت اضرار به غیر را دارد و ممکن است به منافع کل جامعه یا افراد آن لطمه وارد نماید. به عبارت دیگر، مرتکب باید قصد ایراد ضرر مادی یا معنوی به غیر را داشته باشد (همان: ۳۱۳).

از این رو در مواردی که مرتکب با اعتقاد به اینکه حق ورود اطلاعات یا تغییر مندرجات داده‌پیام را دارد و یا مجاز به مداخله در سیستم یا پردازش داده‌پیام است، اقداماتی را انجام دهد و در نتیجهٔ آن، داده‌پیامی خلاف حقیقت ایجاد کند که اتفاقاً قابلیت استفاده به عنوان داده‌پیام معتبر را هم داراست، عمل مرتکب، مشمول عنوان مجرمانهٔ جعل قرار نمی‌گیرد. مانند موردی که کاربر مجاز که حق ورود به سیستم و پردازش اطلاعات را دارد، با اعتقاد به اینکه حق تغییر مندرجات داده‌پیام را دارد، بخشی از داده‌پیام را حذف و محو کند و آن را مجدداً مورد پردازش قرار دهد و در نتیجه، داده‌پیام کاملاً معتبری بر خلاف حقیقت ایجاد کند. در چنین مواردی، ایجادکنندهٔ داده‌پیام، به واسطهٔ عدم آگاهی از اینکه مرتکب قلب و تحریف واقعیت شده است، بزهکار تلقی نمی‌گردد. همچنین در مواردی که مرتکب، با علم به اینکه عمل وی قلب و تحریف حقیقت است، در داده‌پیامهای شخصی متعلق به خود، تغییراتی ایجاد و با ورود برخی اطلاعات یا حذف و محو بخشی از آن، داده‌پیام جدیدی را به ضرر خود ایجاد نماید، از آنجا که سوء نیت خاصِ اضرار به غیر، به سوء نیت عامِ قلب و تحریف حقیقت ملحق نشده است، عمل وی مشمول مجازات نخواهد بود.

همچون سایر جرایم، انگیزهٔ مرتکب در تحقق این جرم تأثیری ندارد و در

صورت تکمیل عنصر روانی، عمل مرتکب، حتی چنانچه به انگیزهٔ خیرخواهانه صورت گرفته باشد، قابل مجازات است. مانند موردی که شخصی به انگیزهٔ کمک به مدیون و رهانیدن وی از تعقیب قضایی و عواقب احتمالی آن، اطلاعات مربوط به بدهی او را از متن داده‌پیام محو و حذف نماید یا با ورود اطلاعات نادرست، او را بریء الذمه نشان دهد. از آنجا که چنین داده‌پیامی قابلیت اضرار به غیر و بهره‌برداری در مراجع قضایی را دارد، عمل مرتکب صرف نظر از انگیزهٔ دیگرخواهانه‌ای که به همراه دارد، جعل و مشمول مجازات است.

نتیجه‌گیری

بسیاری از اعمال مجرمانه‌ای که در فضای فیزیکی و ملموس قابل تحقق هستند، در فضای مجازی نیز امکان فعلیت دارند. تحقق جرایم در فضای مجازی با تکیه بر ابزارهای ناشی از پیشرفت علوم و فناوریهای اطلاعات و ارتباطات امکان‌پذیر است و شبکه‌های اطلاع‌رسانی رایانه‌ای نظیر اینترنت یا شبکه‌های محلی تلفن همراه، بستر مناسبی را برای بسیاری از فعالیتهای مجرمانه، به ویژه انواع سازمان‌یافتهٔ آن فراهم کرده است. ارتکاب جرایم در این فضا، از برخی جهات آسان‌تر و فرار از پیامدهای قضایی آن به مراتب امکان‌پذیرتر است. هر قدر استفاده از ابزارهای فناورانه در ارتکاب جرایم افزایش یابد، کشف و اثبات جرایم و تحصیل ادلهٔ قانونی دشوارتر می‌گردد. به گونه‌ای که در برخی موارد عملاً امکان استماع دعوای بزه‌دیده منتفی شده یا به موردی نادر تبدیل می‌شود.

البته علی‌رغم تفاوتهایی که در روشهای ارتکاب عنصر مادی میان جعل سنتی و جعل مبتنی بر فناوریهای اطلاعات و ارتباطات وجود دارد، شباهتهایی نیز میان جعل مرتبط با رایانه و جعل در مفهوم سنتی آن وجود دارد که یکی از آنها قلب حقیقت و مخدوش کردن و تغییر دادن واقعیت است. بررسی مقررات قانونی نشان می‌دهد که روش ارتکاب جرم جعل در فضای سنتی با فضای الکترونیکی متفاوت است.

بستر ارتکاب این جرم، مبادلات الکترونیکی است که با بهره‌گیری از فناوریهای اطلاعات و ارتباطات و ابزارهای متنوع آن محقق می‌شود. به علاوه روشهای

ارتکاب این جرم نیز همچون زمینهٔ ارتکاب آن الکترونیکی است و با ارتکاب افعالی نظیر ورود، تغییر، محو و توقف داده‌پیام و سیستمهای رایانه‌ای یا استفاده از وسایل کاربردی سیستمهای رمزنگاری تولید امضا و... که همگی بر فناوریهای اطلاعات و ارتباطات مبتنی هستند، عملی می‌شود. قلب حقیقت، در هر دو بُعد مادی و معنوی، اصلی‌ترین جزء عنصر مادی این جرم است. منظور از آن، دگرگون کردن و تحریف واقعیت به گونه‌ای است که حقی را تضییع یا ناحقی را اثبات نماید. این عمل به شیوه‌های گوناگون نظیر ورود، تغییر، محو و توقف داده‌پیام، مداخله در پردازش داده‌پیام و سیستم رایانه‌ای، صدور و تولید جعلی امضای اشخاص، اخذ گواهی صحت و اصالت امضای الکترونیکی از راههای مجعول صورت می‌پذیرد.

تولید چنین داده‌پیامی در صورتی جرم است که دارای ارزش مالی و اثباتی باشد و نیز این قابلیت را داشته باشد که در مراجع مختلف اداری، قضایی و... به عنوان داده‌پیام معتبر به کار گرفته شود و در تضییع حق و اثبات ناحقی مؤثر باشد. در غیر این صورت، ایجاد داده‌پیامی که قابلیت به کارگیری به عنوان داده‌پیام معتبر و تأییدشده را ندارد و یا فاقد ارزش مادی و اثباتی است و مرتکب یا شخص ثالث با استفاده از آن منتفع نمی‌شود، جعل به شمار نمی‌رود و ایجادکنندهٔ چنین داده‌پیامی مسئولیت کیفری نخواهد داشت. قلب حقیقت باید متضمن ایراد ضرر به غیر باشد؛ اعم از اینکه ضرر به منافع خصوصی اشخاص یا منافع عمومی جامعه وارد شود. از این رو صِرف قلب و تحریف حقیقت بدون امکان اضرار به غیر، جعل به شمار نمی‌رود. این جرم از جرایم مادی صرف نبوده و نیازمند اثبات عنصر روانی است. در نتیجه باید سوء نیت عام مرتکب به تولید و پردازش داده‌پیامهای مجعول احراز و مشخص شود که با علم و آگاهی کامل و عمداً (همان: ۳۱۲) مبادرت به قلب حقیقت و تحریف حقایق نموده است. به علاوه باید قصد خاصِ فریب دادن دیگران را داشته و آگاه باشد که اعمال وی اضرارآمیز بوده و تولیدات مجرمانهٔ وی، قابلیت اضرار به غیر را دارد و ممکن است به منافع کل جامعه یا افراد تشکیل‌دهندهٔ آن لطمه وارد نماید. همانند جعل در فضای سنتی، در این جرم نیز انگیزه اثری در تحقق آن ندارد و حداکثر ممکن است از اسباب تخفیف مجازات تلقی گردد.

کتاب‌شناسی

۱. پاکزاد، بتول، «اقدامهای سازمانهای بین‌المللی و منطقه‌ای در خصوص جرمهای رایانه‌ای»، ***مجلهٔ پژوهشهای حقوقی***، مؤسسهٔ مطالعات و پژوهشهای حقوقی شهر دانش، سال سوم، شمارهٔ ۶، ۱۳۸۳ش.

۲. جعفری لنگرودی، محمدجعفر، ***ترمینولوژی حقوق***، چاپ هشتم، تهران، کتابخانهٔ گنج دانش، ۱۳۷۶ش.

۳. حاج فتحعلیها، عباس، ***توسعهٔ تکنولوژی، بررسی مفاهیم، فرایند تصمیم‌گیریها***، تهران، دانشگاه علامه طباطبایی، ۱۳۷۲ ش.

۴. خرم‌آبادی، عبدالصمد، «تاریخچه، تعریف و طبقه‌بندی جرمهای رایانه‌ای»، ***مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات***، معاونت حقوقی و توسعهٔ قضایی قوهٔ قضاییه، تهران، سلسبیل، ۱۳۸۴ ش.

۵. زرکلام، ستار، «قانون تجارت الکترونیکی و امضای الکترونیکی»، ***مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات***، معاونت حقوقی و توسعهٔ قضایی قوهٔ قضاییه، تهران، سلسبیل، ۱۳۸۴ ش.

۶. عالی‌پور، حسن، «کلاهبرداری رایانه‌ای»، ***مجلهٔ پژوهشهای حقوقی***، مؤسسهٔ مطالعات و پژوهشهای حقوقی شهر دانش، سال سوم، شمارهٔ ۶، ۱۳۸۳ ش.

۷. قناد، فاطمه، ***ابعاد کیفری حقوق تجارت الکترونیکی***، رسالهٔ دکتری، دانشگاه شهید بهشتی، ۱۳۸۵ ش.

۸. کاستلز، مانوئل، ***عصر اطلاعات و ظهور جامعهٔ شبکه‌ای***، ترجمهٔ احمد علیقلیان، تهران طرح نو، ۱۳۸۰ ش.

۹. گلدوزیان، ایرج، ***حقوق جزای اختصاصی***، تهران، جهاد دانشگاهی، بی‌تا.

۱۰. لاودن، کنت سی. و همکاران، ***فناوری اطلاعات، مفاهیم و کاربردها***، ترجمهٔ حمید محسنی، تهران، کتابدار، ۱۳۸۶ ش.

۱۱. میرمحمدصادقی، حسین، ***جرایم علیه امنیت و آسایش عمومی***، تهران، میزان، ۱۳۸۵ ش.

۱۲. ولیدی، محمدصالح، ***حقوق جزای اختصاصی***، تهران، غروب، بی‌تا.

13. Baker, S., et al, ***The Limits of Trust Cryptography, Governments and Electronic Commerce***, Kluwer Law International, London, 2008.

14. Brazell, L., ***Electronic Signature Law and Regulations***, Sweet & Maxwell, 2008.

15. Clarke, M., ***Business Crime: Its Nature and Control***, Cambridge Polity Press, 2007.

16. ***Convention on Cybercrime***, Budapest, 23.XI. 2001, art 6.

17. Croall, H., ***Understanding White Collar Crime***, Open University Press, 2009.

18. Liu, S., et at, ***A Practical Guide to Biometric Security Technology***, 2010, available at: <http://www.computer.org/itpro/homepage/jan_feb/security3.htm>.

19. ***Report of the Eleventh United Nations Congress on Crime Prevention and Criminal Justice***, Bangkok, 18-25 April 2005.

20. Ruggiero, V., et al, ***Eurodrugs: Drug Use; Markets and Trafficking in Europe***, London University College, London Press, 2007.

21. Shapiros, S., "Collaring the Crime, not the Criminal: Re-Considering the Concept of White Collar Crime", ***American Sociological Review***, Vol. 55, 1990.
22. Tanaka, K., et al, ***Information Organization and Databases Foundations of Data Organization***, Kluwer Academic Publishers, 2005.
23. Vacca, J., ***Biometric Security Solutions***, 2009, available at: <http://www.informit.com>.