پژوهشنامه حقوق کیفری
سال نهم، شماره اول، بهار و تابستان ۱۳۹۷
شماره پیاپی ۱۷

گستره و ویژگی‌های داده‌های مجعول رایانه‌ای در حقوق ایران

دکتر محمدخلیل صالحی[۲]
ایمان محترم قلاتی[۱]✉

تاریخ دریافت: ۱۳۹۵/۱۱/۴ تاریخ پذیرش: ۱۳۹۷/۴/۱۰

چکیده

به موازات پیشرفت سریع فناوری‌های اطلاعات و ارتباطات، طیف گسترده و متنوعی از داده‌ها و اسناد الکترونیک موضوع جعل و تحریف قرار گرفته است. ماده ۶ قانون جرایم رایانه‌ای در مقام جرم‌انگاری جعل رایانه‌ای، موضوع این جرم را «داده‌های قابل استناد» عنوان کرده است. برخلاف جعل سنتی که قانون‌گذار موضوعاتش را مانند نوشته، دستخط، سند، امضا و مهر، تقریباً مشخص کرده است، نوع و ویژگی‌های داده-های موضوع جعل رایانه‌ای در ماده ۶ تعیین نگردیده است. این نقیصه در عمل ابهامات زیادی را به وجود آورده است. حجم عظیم و متنوع داده‌ها از یک سو و ابهام در مفهوم «داده قابل استناد» از سوی دیگر، تشخیص اینکه چه داده‌هایی موضوع بزه جعل رایانه‌ای هستند را دشوار کرده است. در این مقاله سعی شده با تبیین ویژگی‌های اسناد الکترونیک مجعول، به ابهامات موجود در این زمینه پاسخ داده شود.

واژگان کلیدی: جعل رایانه‌ای، داده، سند رایانه‌ای، رابطه انتساب، ارزش اثباتی

---

۱. استادیار حقوق کیفری و جرم شناسی دانشگاه قم
۲. دانشجوی دکتری حقوق کیفری و جرم شناسی دانشگاه قم (نویسنده مسئول) ✉ iman_mohtaram@yahoo.com

مقدمه

حجم گستردهٔ روابط اشخاص در فضای مجازی در کنار مزایـای بسـیار آن، محـیط مناسـبی بـرای فعالیت بزهکاران فراهم آورده است. این فضا به لحاظ ویژگی‌های منحصر به فـردی کـه نسـبت بـه دنیای مادی دارد، دارای مزیت‌ها و جذابیت‌های بیشتری برای تبهکاران است. به نحوی که در سال های اخیر ارتکاب جرم در فضای سایبر روند رو به رشد فزاینده‌ای داشته است.

جرم جعل رایانه‌ای یکی از مهم‌ترین و شایع‌ترین جرایم رایانه‌ای است. طبق آماری که سـازمان ملل در سال ۲۰۱۳ میلادی ارائه کرده، جعل و کلاهبرداری رایانـه‌ای شـایع‌تـرین جـرایم رایانـه‌ای هستند و حدود یک سوم از کل جرایم رایانه‌ای در سراسر دنیا را به خود اختصاص داده‌اند.[1]

در این جرم، «داده»[2] به‌عنوان بنیادی‌ترین رکن فضای مجازی، موضـوع جـرم قـرار مـی‌گیـرد. همان‌طور که مقنن در جعل سنتی موضوعات خاصی از جمله دسـتخط مقامـات عـالی، اسـکناس، امضا، مهر و سند را قابل جعل دانسته و تحقق جعل در مورد هر نوشـته‌ای را نپذیرفتـه[3]، در جعـل رایانه‌ای نیز هر داده‌ای را موضوع بزه جعل قرار نداده است. نظر به اینکه با گسـترش فنـاوری‌هـای نوین اطلاعات و ارتباطات گونه‌های متنوع و بسیار گسترده‌ای از داده‌هـای رایانـه‌ای از جملـه داده-های صوتی، تصویری، مکتوب و غیره به وجود آمده، اینکه چه نوع داده‌هـایی بـا چـه ویژگـی‌هـایی موضوع جرم جعل رایانه‌ای هستند یکی از مسائل مهم قابل طرح در حوزه جعل رایانه‌ای است.

قبل از تصویب قانون تجارت الکترونیک در خصوص قابل اعمال بودن مقررات سـنتی در مـورد داده‌های رایانه‌ای و این‌که چه داده‌هایی موضوع جعل محسوب می‌شود، تردیـدهـای زیـادی وجـود داشت. برای نمونه اداره حقوقی قوه قضائیه در پاسخ بـه چنـین ابهامـاتی اظهـار داشـته؛ داده‌هـای رایانه‌ای که از طریق چاپ به‌صورت نوشته قابل انعکاس بر روی کاغـذ باشـد از مصـادیق «نوشـته» مندرج در ماده ۵۲۳ محسوب می‌شود و این داده‌ها می‌توانند موضوع جرم جعل قرار گیرند[4]. لذا در آن زمان حداکثر داده‌ای که ممکن بود موضوع بزه جعل قرار گیرد، داده‌ی به شـکل نوشـته بـود و

1. United Nation Office on Drugs and Crime, Vienna, Comprehensive Study on Cybercrime, Draft—February, 2013, p 26.

2. Data.

۳. هر چند ماده ۵۲۳ ق.م.ا. مصوب۱۳۷۵ در تبیین موضوعات جرم جعل به نوشته به صورت مطلق اشـاره کـرده ولـی نظر به اینکه در این ماده مجازاتی تعیین نشده، ماده مزبور نمی‌تواند به عنوان رکن قانونی جعل مادی مورد استناد قرار گیرد. در این خصوص با مراجعه به مواد ۵۲۴ تا ۵۴۲ ق.م.ا. ۱۳۷۵ مشخص می‌شود موضوعات جعل مـادی عبارتنـد از اسناد اعم از عادی و رسمی، مهر، منگنه، علامت، دستخط مقامات عالی و غیره. بنابراین در هـیچ یـک از ایـن مقـررات «نوشته» به صورت کلی موضوع جعل مادی قرار نگرفته است.

۴. نظریه شماره ۷/۵۲۹۴ مورخ ۱۳۷۸/۱۰/۴ اداره حقوقی قوه قضائیه قابل دسترسی در سایت:
http://rooznamehrasmi.ir/laws

جعل در مورد سایر داده‌ها از جمله داده‌های به شکل صوت، رمز یا تصویر قابل تحقق نبود. اما با تصویب قانون تجارت الکترونیک و پس از آن قانون مجازات جرایم رایانه‌ای، تمامی انواع داده‌ها اعم از مکتوب، صوتی و تصویری در صورت داشتن شرایط قانونی، موضوع جرم جعل قرار گرفتند.

مقنن در سال ۱۳۸۸ با تصویب ماده ۶ قانون مجازات جرایم رایانه‌ای، جعل را در خصوص داده‌های قابل استناد قابل تحقق دانسته اما دقیقاً مشخص نکرده منظور از دادهٔ قابل استناد چیست و این چنین داده‌هایی باید دارای چه ویژگی‌ها و اوصافی باشند تا جرم جعل محقق شود. همچنین این امر مورد ابهام است که داده در چه مرحله‌ای باید قابل استناد باشد؛ قبل از ارتکاب جعل توسط مرتکب یا پس از آن.

در این نوشتار در راستای پاسخ به این پرسش‌ها نخست پیشینه قانون‌گذاری و گسترهٔ داده‌های موضوع جعل رایانه‌ای بررسی می‌شود و پس از آن اوصاف داده مجعول در جعل مادی رایانه‌ای که عبارتند از قلب رابطه انتساب و قابل استناد بودن داده، تجزیه و تحلیل می‌شود و به این موضوع خواهیم پرداخت که شرط مستند بودن داده، مربوط به داده اولیه است یا داده ثانویه (داده‌ای که در نهایت توسط جاعل تغییر یافته یا ایجاد شده) یا هر دوی آن‌ها. در مباحث بعدی نیز انواع داده‌های قابل استناد طبق قوانین دسته‌بندی و تبیین می‌شوند.

۱. پیشینه قانون‌گذاری و گسترهٔ داده‌های موضوع جعل رایانه‌ای

مسئله اصلی نوشتار حاضر، همان‌گونه که از عنوان آن پیدا است، ویژگی‌های داده موضوع جعل رایانه‌ای است. پرداختن به این امر در ابتدا مستلزم شناخت قوانین حاکم بر موضوع جعل رایانه‌ای است و این‌که بدانیم این قوانین دارای چه سوابق و پیشینه تقنینی هستند. به‌علاوه این‌که امروزه با طیف گسترده‌ای از داده‌های دیجیتالی، مغناطیسی، نوری، الکترومغناطیسی و غیره مواجهیم و بررسی ویژگی‌های داده موضوع جعل رایانه‌ای بدون تعیین گستره داده‌های موضوع این جرم امکانپذیر نیست. بنابراین در این مبحث مقدماتی به تبیین دو موضوع پیشینه قانون‌گذاری و گسترهٔ داده‌های موضوع جعل رایانه‌ای می‌پردازیم.

۱.۱. پیشینه قانون‌گذاری

داده‌های رایانه‌ای در ابتدا به دلایلی از جمله غیرملموس بودن و سهولت جعل و تغییر و همچنین دشواری شناخت هویت ایجادکننده یا فرستنده آن، قابلیت استناد نداشتند و به راحتی مورد پذیرش محاکم قضایی قرار نمی‌گرفتند. اما با توسعه استفاده از این شیوه ارتباطی، ارزش اثباتی

داده‌ها کم‌کم به رسمیت شناخته شد و در دهه‌های ۶۰ و ۷۰ قرن بیستم به‌عنوان اماره در محاکم فرانسه و بلژیک مورد استناد قرار گرفتند و در سال ۱۹۶۸ میلادی در نظام حقوقی انگلستان به‌عنوان دلیل واقعی پذیرفته شدند (عبدالهی، ۱۳۸۷: ۳).

در ایران قانون‌گذار با تصویب قانون تجارت الکترونیک مصوب ۱۳۸۲ که برگرفته از قانون نمونه کمیسیون سازمان ملل برای حقوق تجارت بین المللی (آنسیترال) ۱۹۹۶ وین[1] بود، برای برخی داده‌های الکترونیک تحت شرایط خاصی قائل به ارزش مالی و اثباتی شد و بعد از آن با تأسیس مرکز صدور گواهی الکترونیکی در سال ۱۳۸۵ قابلیت استنادپذیری داده‌های الکترونیکی را به نحو چشمگیری افزایش داد.

نخستین قانونی که به موضوع جعل رایانه‌ای پرداخته قانون مجازات جرایم نیروهای مسلح مصوب ۱۳۸۲/۱۰/۹ است. ماده ۱۳۱ این قانون بدون این‌که از عنوان جعل رایانه‌ای استفاده نماید، تغییر یا حذف اطلاعات، الحاق، تقدیم یا تأخیر تاریخ نسبت به تاریخ حقیقی و نظایر آن‌که به‌صورت غیر مجاز توسط نظامیان در سیستم رایانه و نرم افزارهای مربوط صورت گیرد، را جرم‌انگاری نموده است. این قانون مختص جرایم نظامیان بوده و همچنان دارای اعتبار است.

قانون تجارت الکترونیک مصوب ۱۳۸۲ در ماده ۶۸ جرم جعل رایانه‌ای را تبیین نموده است. این ماده در تمامی مصادیق جعل اعم از جعل داده‌های تجاری و غیرتجاری مورد استناد محاکم دادگستری قرار می‌گرفت (عالی پور، ۱۳۹۳: ۲۰۴) تا این‌که قانونگذار در ماده ۶ قانون جرایم رایانه ای جرم جعل رایانه‌ای را به شرح زیر تعریف نمود:

«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 خواهد شد:

الف) تغییر یا ایجاد داده‌های قابل استناد یا ایجاد یا وارد کردن 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».

برخی از حقوق‌دانان باتوجه به‌عنوان قانون تجارت الکترونیک، بر این باورند که ماده ۶۸ این قانون نسخ نشده و هنوز هم در خصوص داده‌های مربوط به مبادلات تجاری قابل اعمال است.

1. UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998, UNITED NATIONS PUBLICATION, ISBN 92-1-133607-4.

ایشان با این استدلال که ماده ۶۸ ق.ت.ا.[1] خاص بوده و ماده ۶ ق.ج.ر. عام است و با اتکا به قاعده‌ی قانون عام مؤخر ناسخ قانون خاص مقدم نیست، به این نتیجه رسیده‌اند که ماده ۶ ق.ج.ر. توان نسخ ماده ۶۸ ق.ت.ا. را ندارد و ماده ۶۸ قانون تجارت الکترونیک همچنان به قوت خود باقی است (زرکلام، ۱۳۸۸: ۱۵).

اما چنین برداشتی که قانون تجارت الکترونیک را از حیث تجاری بودن داده‌ها خاص می‌داند به چند دلیل اشتباه است. نخست این‌که هر چند عنوان این قانون «تجارت الکترونیک» است اما ماده یک آن در تعریف گستره حاکمیت قانون مزبور مقرر داشته: «این قانون مجموعه اصول و قواعدی است که برای مبادله آسان و ایمن اطلاعات در واسطه‌های الکترونیکی و با استفاده از سیستم‌های ارتباطی جدید به‌کار می‌رود». لذا بر این اساس، قانون مزبور تمام مبادلات اعم از تجاری و غیرتجاری[2] قابل انجام در واسطه‌های الکترونیکی و حتی سیستم‌های ارتباطی جدید را دربرمی‌گیرد (ساورایی، ۱۳۹۱: ۳۷۳)[3]. دلیل دیگر این‌که بند الف ماده ۲ ق.ت.ا. تعریفی موسع از «داده-پیام» ارائه کرده، تا حدی که این تعریف معادل واژه «داده» در مفهوم عام است و ماده ۶۸ نیز جعل کلیه داده‌پیام‌های دارای ارزش اثباتی و مالی را جرم‌انگاری نموده و موضوع جرم جعل را محدود به داده‌های مربوط به مبادلات تجاری قرار نداده است. به‌علاوه این‌که این ماده با استفاده از عبارت‌های «بستر مبادلات الکترونیک» و «جعل کامپیوتری» که عباراتی کلی است مصادیق جعل را محدود به مبادلات تجاری الکترونیک ننموده و سایر مبادلات را نیز تحت پوشش قرار داده است.

اما جعل رایانه‌ای در قانون تجارت الکترونیک از جهتی دیگر نسبت به قانون جرایم رایانه‌ای خاص است. مطابق ماده ۶۸ قانون تجارت الکترونیک صرفاً داده‌هایی موضوع این قانون قرار می‌گیرد که در بستر مبادلات الکترونیک جعل شده باشند. در صورتی‌که در ماده ۶ قانون جرایم رایانه‌ای، داده اعم از این‌که در بستر مبادلات الکترونیک باشد یا نباشد می‌تواند موضوع جرم جعل قرار گیرد. با وجود این به نظر می‌رسد مقنن ماده ۶ قانون جرایم رایانه‌ای را به‌گونه‌ای وضع نموده

---

۱. در این مقاله مخفف‌های ق.ت.ا. به جای قانون تجارت الکترونیک مصوب ۱۳۸۲ و ق.ج.ر. به جای قانون جرایم رایانه-ای مصوب ۱۳۸۸ به کار می‌رود.

۲. البته برخی هم بر این باورند که هرچند عنوان «قانون تجارت الکترونیک» این امر را به ذهن متبادر می‌کند که قانون موصوف صرفاً در خصوص فعالیت‌های تجاری به مفهوم خاص مندرج در قانون تجارت اعمال می‌گردد، اما با بررسی مواد این قانون و کاربرد عبارت «مبادلات الکترونیکی» در مواد مختلف مشخص می‌شود مقنن اصطلاح «تجارت الکترونیک» را در معنای مبادلات مالی الکترونیک به کار برده و این قانون در مورد کلیه مبادلات مالی الکترونیک اعم از اینکه ماهیتاً تجاری باشند یا خیر اعمال می‌شود (جاویدنیا، ۱۳۸۶: ۱۲۶).

۳. برای ملاحظه دلایل بیشتر مبنی بر اینکه قانون تجارت الکترونیک کلیه مبادلات اعم از تجاری و غیر تجاری را در برمی‌گیرد، بنگرید به: (ساورایی، ۱۳۹۱: ۳۷۱-۳۷۵).

که این ماده تمام مصادیق جعل اعم از این‌که داده مجعول در بستر مبادلات الکترونیک باشد یا نباشد را در برگیرد. منطق نیز این اقتضا را دارد که ماده ۶ ق.ج.ر. را در مورد جعل در بستر مبادلات الکترونیک اعمال نماییم. زیرا مجازات مندرج در ماده ۶۸ ق.ت.ا. (یک تا سه سال حبس) خفیفتر از مجازات مندرج در ماده ۶ ق.ج.ر. (یک تا پنج سال حبس) است؛ این در حالی است که قاعدتاً مجازات جعل در بستر مبادلات باید شدیدتر از جعل عادی رایانه‌ای باشد. بنابراین هر چند ماده ۶۸ ق.ت.ا.، قانون خاص محسوب می‌شود ولی با تصویب ماده ۶ ق.ج.ر. نسخ شده و در حال حاضر ماده اخیر معتبر و لازم الاجرا است (بنگرید به: عالی پور، ۱۳۹۳: ۶۴، ۳۸۹ و ۳۹۰).

در خصوص شروع به جرم جعل رایانه‌ای، در ماده ۶ ق.ج.ر. بر خلاف ماده ۶۸ ق.ت.ا.، مقرره‌ای وضع نشده است. بر همین اساس برخی نویسندگان شروع به جعل رایانه‌ای را تنها در مواردی که مورد با ماده ۶۸ ق.ت.ا. قابل تطبیق باشد قابل مجازات دانسته‌اند (قناد، ۱۳۹۰: ۷۰). ولی با عنایت به این‌که طبق ماده ۵۵ ق.ج.ر. مواد ۱ تا ۵۴ این قانون به‌عنوان مواد (۷۲۹) تا (۷۸۲) قانون مجازات اسلامی (بخش تعزیرات) و باعنوان فصل جرائم رایانه‌ای منظور گردیده است و باتوجه به این‌که ماده ۱۲۲ ق.م.ا. مصوب ۱۳۹۲، در مقام جرم‌انگاری و کیفرگذاری جدید برای شروع به کلیه جرایم بوده است، این ماده در مورد شروع به جعل رایانه‌ای مندرج در ماده ۶ ق.ج.ر. نیز اعمال می‌شود. لذا باتوجه به این‌که مجازات جعل رایانه‌ای درجه پنج است، شروع به ارتکاب جعل رایانه‌ای نیز برابر بند پ ماده ۱۲۲ حبس تعزیری یا شلاق یا جزای نقدی درجه شش خواهد بود.

۲.۱. گستره داده‌های موضوع جعل رایانه‌ای

واژه «داده» در فرهنگ کامپیوتر مایکروسافت به معنای فقره یا فقراتی از اطلاعات تعریف شده است (هیات مولفان و ویراستاران انتشارات مایکروسافت، ۱۳۸۱: ۱۷۵). کنوانسیون راجع به جرایم رایانه‌ای نیز داده را عبارت از هر نوع اطلاعات یا مفاهیم قابل پردازش در سیستم رایانه‌ای دانسته است (نوری، ۱۳۸۳: ۵۹). داده دارای اشکال مختلفی از قبیل آنالوگ، دیجیتال و موج نوری یا الکترومغناطیسی است. داده‌های رایانه‌ها دارای ساختار دیجیتالی هستند و به اقسام مختلفی از قبیل برنامهٔ رایانه‌ای، متن، صوت و تصویر قابل تقسیم هستند (فضلی، ۱۳۹۱: ۷۶). طبق ماده ۲ قانون تجارت الکترونیک داده پیام «هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری یا فناوری‌های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود». تعریف ارائه شده از داده پیام در این ماده کلیه مصادیق داده را تحت‌پوشش قرار می‌دهد و از این

رو برخی بر این باورند که مقنن «داده‌پیام» را مترادف واژه «داده» به کار برده است (جاویدنیا، ۱۳۸۷: ۶۰-۶۳)[۱].

به‌علاوه این ماده با ذکر عبارت «فناوری‌های جدید اطلاعات» کلیه داده‌های قابل مبادله از طریق ابزارهای ارتباطی مثل تلگراف، تلکس، فکس، تلفن همراه و سایر ابزارهای نوین اعم از دیجیتالی، مغناطیسی، نوری، الکترومغناطیسی و حتی فناوری‌هایی که ممکن است در آینده کشف شوند، را نیز در برمی‌گیرد (شهبازی‌نیا، ۱۳۸۹: ۱۹۴). این مقرره از بند (ف) ماده ۲ قانون تجارت الکترونیک نیز قابل استنباط است. مطابق این بند: «وسایل ارتباط از راه دور (Means Of Distance Communication): عبارت از هر نوع وسیله‌ای است که بدون حضور فیزیکی هم‌زمان تأمین‌کننده و مصرف‌کننده جهت فروش کالا و خدمات استفاده می‌شود».

امروزه به‌دلیل در هم آمیختن تجهیزات مخابراتی و سیستم‌های رایانه‌ای، تفکیک بین داده‌های رایانه‌ای و مخابراتی عملاً ممکن نیست (جاویدنیا، ۱۳۸۷: ۵۹) با این وجود مقنن با وضع عبارت «سامانه‌های رایانه‌ای یا مخابراتی» در بند ب ماده ۶ ق.ج.ر. هر دو نوع داده را موضوع جرم جعل قرار داده و تردیدی باقی نگذاشته که گستره داده در جرم جعل رایانه‌ای صرفاً به داده‌های رایانه‌ای و قابل انتقال از طریق اینترنت محدود نمی‌شود و تمامی داده‌های قابل انتقال از طریق ابزارهای مخابراتی را نیز تحت پوشش قرار می‌دهد.

در مورد این ابهام که آیا صرفاً داده‌های به شکل نوشته موضوع جرم جعل قرار می‌گیرند یا این‌که سایر انواع داده‌ها نیز ممکن است موضوع این جرم قرار گیرند، نظرهای مختلفی مطرح شده است. در همین ارتباط برخی از نویسندگان در تعریف سند الکترونیک – یا همان داده‌های قابل استناد و موضوع جرم جعل- اظهار داشته‌اند سند الکترونیک:

«داده‌پیامی است که به‌صورت الکترونیک تولید، ثبت، ذخیره، پردازش، بازیابی، دریافت یا منتقل گردیده و مبین اطلاعات یا بازنمایی از اطلاعات، داده‌ها، ارقام، علایم و سایر اشکال نمایش نوشتاری است که در اثبات اعمال و وقایع حقوقی به کار می‌رود و به واسطه آن حقی یا تعهدی مستقر یا ساقط یا حقیقتی اثبات یا تأیید گردیده است» (ساورایی، ۱۳۹۳: ۸۶).

مطابق این تعریف صرفاً داده‌هایی که به شکل نوشتاری قابل نمایش هستند دارای ارزش اثباتی و قابل استناد هستند این در حالی است که در مواد ۶، ۷، ۱۰، ۱۲، ۱۳، ۱۴، ۱۵، ۱۸ قانون تجارت الکترونیک بدون این‌که تفاوتی بین داده‌های حاوی نوشته، صوت، تصویر یا رمز در نظر گرفته شود، شرایط داشتن ارزش اثباتی و قابل استناد بودن داده‌ها تشریح شده است. ماده ۶ ق.ج.ر. نیز جعل را در مورد تمامی داده‌های قابل استناد قابل تحقق دانسته و تفکیکی بین داده‌هایی که به شکل

۱. برای مطالعه بیشتر در خصوص مفاهیم داده و داده‌پیام بنگرید به: (جاویدنیا، ۱۳۸۷؛ صص ۵۸- ۶۶).

نوشته‌اند و داده‌هایی که حاوی اطلاعات صوتی یا تصویری یا رمزی هستند، قائل نشده است. در این راستا به ماده ۲ قانون تجارت الکترونیک نیز می‌توان استناد نمود. بر اساس ماده مزبور داده پیام بر خلاف نوشته صرفاً نمودی از گفتار نیست بلکه شامل تمام اطلاعات نوشتاری، صوتی، تصویری، رمزی و برنامه‌های رایانه‌ای یا نرم‌افزار است. بنابراین کلیه داده‌های صوتی، تصویری و یا رمزی ممکن است دارای ارزش اثباتی و قابل استناد باشند و موضوع جرم جعل واقع شوند. در نتیجه هر دادهٔ قابل استناد، حتی اگر به‌صورت نوشته نباشد می‌تواند موضوع جرم جعل قرار گیرد. در خصوص داده محسوب شدن نرم‌افزارهای رایانه‌ای، برخی مقررات بین‌المللی از جمله قوانین مربوط به جعل رایانه‌ای سازمان همکاری اقتصادی و توسعه[1] و پیشنهادات مربوط به جرایم رایانه‌ای مصوب ۱۹۸۵ میلادی شورای اروپا،[2] نرم افزار را داده رایانه‌ای به حساب نیاورده‌اند و جعل داده‌های رایانه‌ای و نرم افزارهای رایانه‌ای را به تفکیک جرم‌انگاری نموده‌اند (اسشولبرگ، ۲۰۰۴: ۳)، ولی از آنجا که مفهوم موسع داده شامل نرم‌افزارهای رایانه‌ای نیز می‌شود (عالی پور، ۱۳۹۳: ۳۷) می‌توان اظهار داشت رابطه این دو عموم و خصوص مطلق است و با ذکر داده نیازی به قید برنامه‌های رایانه‌ای نیست.

نکته دیگر این‌که نباید تصور شود تمام داده‌ها دارای ارزش اثباتی‌اند و می‌توانند موضوع بزه جعل قرار گیرند. برخی از نویسندگان با طرح انتقاد از این‌که ماده ۶ ق.ت.ا. داده پیام را در حکم نوشته قرار داده، این استنباط را داشته‌اند که این ماده تمامی داده‌ها را معتبر و قابل استناد دانسته است (ساورایی، ۱۳۹۱: ۳۷۶). از طرف دیگر ایشان پنداشته‌اند مضمون ماده ۱۲ ق.ت.ا.[3] این است که هر داده‌ای باید مورد پذیرش دادگاه قرار گیرد (ساورایی، ۱۳۹۲: ۴۸۹ و ساورایی، ۱۳۹۱: ۳۷۶). این در حالی است اولاً مطابق ماده ۱۲۸۴ قانون مدنی هر نوشته‌ای معتبر نیست و صرفاً نوشته‌هایی سند محسوب می‌شوند که در مقام دعوی و دفاع قابل استناد باشند. ثانیاً مواد مختلف قانون مجازات اسلامی -به جز در برخی موارد محدود مانند جعل دستخط مقامات عالی-، جعل را نه در مورد هر نوشته‌ای بلکه صرفاً در خصوص اسناد اعم از عادی و رسمی قابل تحقق دانسته است. بنابراین رابطه سند و نوشته عموم و خصوص مطلق است و قرار دادن داده در حکم نوشته اقدامی کاملاً هوشمندانه بوده است. در مورد ابهام مندرج در ماده ۱۲ نیز می‌توان گفت، اینکه مقنن مقرر

---

1. Organization for Economic Cooperation and Development (OECD).

۲. کنوانسیون جرایم رایانه‌ای شورای اروپا (The Council of Europe appointed in 1985) در ماده ۷ به جرم جعل رایانه‌ای پرداخته و هدف اصلی از وضع این کنوانسیون تطبیق قوانین کیفری با مقتضیات فضای رایانه‌ای بود (کلوگ، ۲۰۱۲: ۳۶۸).

۳. ماده ۱۲- «اسناد و ادله اثبات دعوی ممکن است به صورت داده پیام بوده و در هیچ محکمه یا اداره دولتی نمی‌توان بر اساس قواعد ادله موجود، ارزش اثباتی (داده پیام) را صرفاً به دلیل شکل و قالب آن رد کرد».

نموده محاکم نباید به دلیل شکل و قالبِ داده آن را رد کنند بدین مفهوم نیست که لازم است هر داده‌ای مورد پذیرش محاکم قرار گیرد؛ بلکه منظور مقنن این بوده که شکل و قالب داده نمی‌تواند دلیل نپذیرفتن آن باشد ولی داده ممکن است بنا به دلایل دیگری از جمله غیر قابل استناد بودن، رد شود. به عبارت دیگر مقنن نپذیرفتن همه داده‌ها به دلیل شکل و قالب آنها را خلاف قانون دانسته و این گزاره به معنای این نیست که همه داده‌ها دارای اعتبار هستند. بنابراین همانطور که جعل مادی موضوعات فیزیکی در مورد هر نوشته‌ای قابل تحقق نیست، هر داده‌ای نیز نمی‌تواند موضوع جعل رایانه‌ای قرار گیرد و لازمه تحقق جعل مادی رایانه‌ای این است که داده موضوع جرم ویژگی‌های معینی داشته باشد.

۲. اوصاف داده موضوع بزه جعل مادی (غیر مفادی) رایانه‌ای

داده موضوع جعل مادی رایانه‌ای در صورتی مجعول است که دارای دو ویژگی کلی «قلب رابطه انتساب» و «قابلیت استناد» باشد. به عبارت دیگر داده‌هایی که رابطه انتساب آن‌ها قلب شده و در ابتدا معتبر و مستند بوده‌اند ولی به واسطه اقدامات جاعل غیر مستند به نظر برسند یا این‌که در حقیقت فاقد ارزش اثباتی باشند ولی به واسطه اقدامات جاعل مستند به نظر برسند مجعول هستند. البته برخی نویسندگان با استناد به ماده ۶۸ ق.ت.ا. بر این باور هستند که داده موضوع جعل رایانه‌ای باید دارای ارزش مالی نیز باشد (قناد، ۱۳۹۰: ۸۲)؛ اما باتوجه به این‌که ماده مزبور با تصویب ماده ۶ ق.ج.ر. نسخ شده و مقرره اخیر، ارزش مالی داشتن داده را شرط تحقق جرم ندانسته، وجود چنین شرطی برای تحقق جرم لازم به‌نظر نمی‌رسد.

۱.۲. قلب رابطه انتساب

رابطه انتساب به معنای رابطه بین ایجاد کننده یا ارسال کننده داده (اصل ساز) [۱] با داده است. مفهوم قلب رابطه انتساب نیز این است که سند یا داده واقعاً و تماماً منتسب به همان شخصی که، در ظاهر نماینگر آن است، نباشد. به عبارت دیگر در اسناد یا داده‌هایی که در ظاهر به شخص معینی منتسب هستند ولی در واقع آن سند یا داده را شخص دیگری ایجاد یا ارسال [۲] نموده، قلب رابطه انتساب محقق شده است. شرط تحقق انواع جرم جعل اعم از عادی و رایانه‌ای قلب رابطه

۱. مطابق بند ب ماده ۲ ق.ت.ا.: «اصل ساز (Originator): منشا اصلی داده پیام است که داده پیام به وسیله او یا از طرف او تولید یا ارسال می‌شود اما شامل شخصی که در خصوص داده پیام به عنوان واسطه عمل می‌کند نخواهد شد».

۲. در خصوص داده‌ها، قلب رابطه انتساب ممکن است در ارسال داده نیز اتفاق بیفتد. برای مثال اگر جاعل وانمود کند داده‌ای که خودش آن را ارسال کرده توسط دیگری ارسال شده قلب رابطه انتساب از نوع ارسال داده محقق می‌شود.

انتساب است. زیرا منظور از قلب حقیقت در جعل، قلب رابطه انتساب است و اینکه گفته شده در جعل، سند باید در مورد خود دروغ بگوید (میرمحمدصادقی، ۱۳۸۴: ۲۹۲) بدین معنا است که سند باید در مورد تنظیم کننده خود دروغ بگوید.

دلیل این‌که رابطه انتساب مقلوب ویژگی اصلی داده‌های مجعول است، این است که قابل استناد بودن –هر چند در ظاهر- بدون وجود رابطه انتساب فاقد معناست و اگر داده به نحوی ایجاد یا ارسال شده باشد که هویت کاربر معلوم نباشد، قابلیت استناد نخواهد داشت (جلالی فراهانی، ۱۳۸۶: ۸۹). از طرف دیگر بدون قلب رابطه انتساب جعل محقق نمی‌شود. زیرا وجه تشابه جعل اسناد عادی و رایانه‌ای این است که شخصی که سند یا داده در قبال وی مورد استفاده یا استناد قرار می‌گیرد به اشتباه بیفتد و تصور نماید داده و یا سند واقعاً توسط منتسب الیه ایجاد شده است.

در همین راستا گرک[1] اظهار داشته جعل رایانه‌ای عبارت از تغییر اسناد الکترونیک است و در توضیح بیشتر برخی شیوه‌های متداول جعل را برشمرده است. شیوه‌هایی مانند ساخت سند الکترونیک که در ظاهر منتسب به نهاد معتبر باشد، تغییر تصاویر الکترونیک قابل استناد در محاکم دادگستری و تغییر متن‌های مستند الکترونیک (گرک، ۲۰۱۲: ۳۰-۳۱). آنچه از تمامی این شیوه‌ها و موارد مندرج در ماده ۶ ق.ج.ر. می‌توان استنباط نمود، این است که در همه این موارد رابطه انتساب بین منتسب‌الیه و داده قلب شده است.

رابطه انتساب داده با اصل ساز در داده‌های رایانه‌ای به شیوه‌های مختلفی قابل تشخیص است. یکی از بهترین شیوه‌های شناخت اصل ساز استفاده از کد شناسایی یا قرارداد اینترنت (IP)[2] رایانه است. توضیح بیشتر این‌که هر رایانه دارای یک نشانی منحصر به فرد به صورت اعداد و ارقام است و به واسطه این کد، پس از ارتباط کاربر با اینترنت، هم شناسایی مالک سیستم رایانه‌ای و هم مکانی که کاربر داده را در آن محل به وجود آورده است، امکان‌پذیر می‌شود (آستریا، ۲۰۰۴: ۴۴).

در تشخیص این‌که چه داده‌هایی در ظاهر دارای رابطه انتساب به نظر می‌رسند می‌توان به ماده ۱۸ قانون تجارت الکترونیک رجوع نمود. این ماده مقرر داشته: «در موارد زیر داده پیام منسوب به اصل ساز است:

الف – اگر توسط اصل ساز یا به وسیله شخصی ارسال شده باشد که از جانب اصل ساز مجاز به این کار بوده است.

ب – اگر به وسیله سیستم اطلاعاتی برنامه ریزی شده یا تصدی خودکار از جانب اصل ساز ارسال شود».

1. Gercke.
2. Internet Protocol.

بنابراین مطابق بند (الف) در مواردی که داده ارسال شده، منتسب به شخصی غیر از ارسال کننده واقعی باشد یا در صورتی که ارسال کننده خود را نماینده مجاز از طرف منتسب الیه معرفی کند ولی چنین سمتی نداشته باشد، داده با قلب رابطه انتساب ارسال شده است. بر اساس بند (ب) نیز اگر شخصی با مداخله در سیستم اطلاعاتی برنامه‌ریزی شده یا تصدی خودکار داده‌ای را ارسال نماید و آن را به شخص دیگری غیر از خودش نسبت دهد باز هم رابطه انتساب داده قلب شده است.

گاهی اوقات نیز جاعل اقدام به تغییر قسمتی از داده‌ی ارسال یا ایجاد شده توسط دیگری می‌نماید. در این روش داده‌ای که در نهایت ایجاد یا ارسال می‌شود تماماً به اصل ساز منتسب نبوده و قسمت‌های از داده مجعول است ولی جاعل تمامیت داده را به عنوان داده معتبر مورد استفاده قرار می‌دهد. بعلاوه این امکان هم وجود دارد که جاعل داده را پس از ارسال توسط فرستنده و قبل از دریافت توسط گیرنده تغییر دهد و تمامیت آن را مخدوش نماید یا تصرفاتی در سیستم رایانه‌ای گیرنده یا فرستنده ایجاد نماید که داده تغییر یابد یا ارسال قسمتی از آن متوقف شود. در چنین مواردی نیز داده‌ای که توسط گیرنده دریافت می‌شود فاقد رابطه انتساب صحیح بوده و عیناً همان داده‌ای نیست که مورد نظر فرستنده بوده و توسط وی ایجاد شده است.

۲.۲. قابلیت استناد

منظور از قابل استناد بودن داده این است که داده سندیت[۱] داشته و دارای ارزش اثباتی باشد. لزوم دارا بودن ارزش اثباتی از تصریح ماده ۶ ق.ج.ر. برداشت می‌شود. بند (الف) ماده ۶ ق.ج.ر. به صراحت جعل را در خصوص داده‌های قابل استناد یا دارای ارزش اثباتی قابل تحقق دانسته اما با-توجه به این‌که بند (ب) این ماده «داده‌ها یا علائم موجود در کارت‌های حافظه یا قابل پردازش در سامانه‌های رایانه‌ای یا مخابراتی یا تراشه‌ها»[۲] را نیز موضوع جرم به حساب آورده است این پرسش ایجاد می‌شود که چرا مقنن در موارد مصرح در بند (ب) اشاره‌ای به قابل استناد بودن داده‌ها یا علائم مذکور نکرده است؟ برای روشن شدن این مسئله باید به این امر توجه نمود که واژه «علائم» مندرج در ماده مذکور ماهیتاً نوعی از داده به شمار می‌رود (هیأت مؤلفان و ویراستاران انتشارات مایکروسافت، ۱۳۸۱: ۶۶۷) بنابراین موضوع بزه جعل رایانه‌ای در این بند نیز چیزی جز داده نیست. از سوی دیگر به نظر می‌رسد منظور قانون‌گذار از «کارت‌های حافظه یا قابل پردازش» کارت‌ها یا تراشه‌هایی است که توسط مراجع و نهادهای دولتی یا عمومی تولید و صادر می‌شود. از

---

۱. سند نوشته‌ای است که در مقام دعوی و دفاع قابل استناد باشد (ماده ۱۲۸۴ قانون مدنی).

۲. در خصوص تعاریف «علائم»، «کارت حافظه» و «تراشه» بنگرید به: (عالی پور، ۱۳۹۳: ۲۰۵).

همین رو گفته شده موارد مندرج در بندهای (الف) و (ب) با هم همسان هستند و از آنجا که کارت‌ها و تراشه‌های مذکور در بند (ب) به خودی خود قابل استناد هستند، قانون‌گذار اشاره‌ای به لزوم قابل استناد بودن داده‌های موجود در این کارتها و تراشه‌ها ننموده است (عالی پور، ۱۳۹۳: ۲۰۸). این احتمال نیز وجود دارد که مقنن به قرینه بند (الف)، خود را از ذکر قابل استناد بودن داده‌های موضوع بند (ب) بی‌نیاز دانسته است. لذا باتوجه به این ابهام و نظر به این‌که «قابل استناد بودن داده» یک شرط اضافه برای تحقق جرم جعل است، با اعمال اصل برائت و تفسیر مقررات کیفری به نفع متهم می‌توان اظهار داشت در مواردی که داده قابل استناد نباشد جرم محقق نمی-شود. بنابراین صرف قلب رابطه انتساب برای تحقق جعل کافی نیست و برای اینکه داده‌ای مجعول به حساب آید، باید از ارزش اثباتی نیز برخوردار باشد. زیرا ممکن است داده‌ای با قلب رابطه انتساب به وجود آمده باشد ولی فاقد ارزش اثباتی اولیه یا ثانویه باشد. بر همین اساس برخی آراء صادره از محاکم دادگستری نیز به لزوم قابل استناد بودن داده برای تحقق جعل رایانه‌ای و استفاده از سند مجعول رایانه‌ای اشاره کرده‌اند[1].

ماده ۶ ق.ج.ر. جز دو شرط برخورداری از ارزش اثباتی و قلب رابطه انتساب ویژگی دیگری را برای موضوع جعل رایانه‌ای لازم ندانسته است. از این رو ویژگی‌هایی از جمله شبیه بودن داده مجعول به داده اصیل یا ایجاد ضرر به‌عنوان نتیجه جرم جعل نقشی در وقوع جرم ندارند. شبیه بودن سند مجعول به سند اصیل در جعل اسناد غیر رایانه‌ای نیز لازم نیست بلکه همین که سند مجعول بتواند باعث اشتباه اشخاص متعارف شود برای تحقق جعل کافی است (میرمحمد صادقی، ۱۳۸۴: ۲۹۱). در مورد ایجاد ضرر نیز هر چند وقوع بالفعل و عینی ضرر شرط وقوع جرم نیست ولی گفته شده حقوق‌دانان بر این امر اتفاق نظر دارند که سند مجعول باید قابلیت اضرار داشته باشد (منصورآبادی، ۱۳۹۲: ۷۰-۷۲). البته برخی حقوق‌دانان در خصوص لزوم قابلیت به اشتباه انداختن و قابلیت اضرار سند مجعول تشکیک کرده و اظهار داشته‌اند این دو مبنای قانونی ندارند و صرفاً رویه قضایی آن‌ها را لازم دانسته است (عالی پور، ۱۳۹۳: ۲۰۰-۲۰۹ و بای، ۱۳۸۸: ۴۷۵). این در حالی است که قابلیت ایجاد ضرر و به اشتباه انداختن در واژه‌های «سند» و «داده قابل استناد» مستتر است. با این توضیح که اولاً جعل در خصوص نوشته‌ها یا داده‌هایی صدق می‌کند که مشتمل بر اجزاء و شرایط و ویژگی‌های داده یا سند اصیل باشند (منصورآبادی،۱۳۹۲: ۳۸) ثانیاً هر نوشته یا داده‌ای که در مقام دعوی و دفاع قابل استناد باشد، قابلیت ایجاد ضرر را هم خواهد

---

۱. دادنامه شماره ۱۲۹۹ مورخ ۱۳۹۰/۱۲/۱۶ صادره از شعبه ۱۰۳۳ دادگاه عمومی تهران قابل دسترسی در سایت بانک آراء پژوهشکده قوه قضاییه به نشانی:

http://j.ijri.ir/SubSystems/Showjudgement.aspx?id=QUQ0VE5wUUpmL0U9.

داشت. البته توجه به این امر ضروری است که سند یا داده در ظاهر باید دارای ارزش اثباتی به نظر برسند نه اینکه واقعاً معتبر باشند. بر این اساس داده یا نوشته‌ای که در ظاهر ویژگی‌های داده قابل استناد یا سند را داشته باشد، می‌تواند موجب به اشتباه انداختن اشخاص متعارف شود به گونه‌ای که آن‌ها داده یا سند مجعول را به عنوان داده یا سند درست قلمداد می‌کنند و به این ترتیب داده یا سند مجعول دارای وصف قابلیت اضرار می‌شود. خلاصه این‌که ضرورت قابلیت به اشتباه انداختن اشخاص متعارف و قابلیت اضرار شروطی مستقل نیستند و نتایج ماهیت «سند» یا «داده قابل استناد» به‌عنوان موضوعِ جرمِ جعل اسناد عادی یا رایانه‌ای می‌باشند.

۳.۲. قابلیت استناد داده اولیه یا ثانویه

در مورد ماده ۶ ق.ج.ر. این ابهام وجود دارد که برای تحقق بزه جعل مادی رایانه‌ای آیا لازم است داده اولیه که موضوع دخل و تصرف جاعل قرار می‌گیرد، قابل استناد باشد یا داده‌ای که در نهایت توسط جاعل به‌وجود می‌آید. قبل از ورود به این بحث لازم است شیوه‌های مختلف اقدام مرتکب از حیث قابلیت استناد داده بررسی شود. در این خصوص حالات زیر برای جعل داده قابل تصور است:

۱- داده اولیه مستند است و مرتکب با اقدامات خود آن را غیرمستند جلوه می‌دهد؛

۲- داده اولیه مستند است و مرتکب با تغییر در مندرجات داده آن را به نحو دیگری مستند جلوه می‌دهد؛

۳- داده اولیه غیرمستند است و مرتکب با اقدامات خود آن را مستند جلوه می‌دهد؛

۴- داده اولیه غیرمستند است و مرتکب تغییراتی در آن انجام می‌دهد ولی باز هم داده غیرمستند به نظر می‌رسد؛

۵- مرتکب اقدام به ایجاد داده به ظاهر مستند می‌نماید؛

۶- مرتکب اقدام به ایجاد داده‌ای منتسب به غیر می‌کند که غیرمستند است.

مطابق مطالبی که در مباحث پیشین بدان پرداختیم در تمام این حالات قلب رابطه انتساب اتفاق می‌افتد؛ زیرا مرتکب «دادهٔ» ایجاد یا تغییر داده شده توسط خودش را به دیگری منتسب می‌نماید. بنابراین آنچه در حالات بالا متفاوت است قابلیت استناد داده اولیه یا داده ثانویه (داده‌ای که در نهایت توسط مرتکب ایجاد می‌شود) است.

تحقق جعل در مورد فروض ۲ و ۵ محرز است زیرا مرتکب با قلب رابطه انتساب داده‌ای را به‌وجود آورده و یا تغییر داده که در ظاهر از اوصاف داده قابل استناد برخوردار است. در حالت ۳ نیز جرم جعل واقع می‌شود و دلیل آن، این است که مطابق ماده ۶ ق.ج.ر. ایجاد داده می‌تواند یکی از اقسام رکن مادی بزه جعل رایانه‌ای باشد. معنای این گزاره این است که حتی اگر در ابتدا هیچ

داده‌ای وجود نداشته باشد و مرتکب اقدام به ایجاد یا ورود داده به ظاهر مستند نماید، جرم محقق می‌شود. بنابراین به طریق اولی تغییر داده‌های نامعتبر به نحوی که معتبر به نظر برسند نیز می‌تواند رکن مادی بزه جعل باشد. کما این‌که در جعل اسناد عادی نیز اگر مرتکب سندی منتسب به غیر را از ابتدا بسازد یا سند نامعتبر و باطلی را صحیح جلوه دهد، جرم جعل واقع می‌شود.

ابهام اصلی در مورد حالتی است که داده اولیه مستند است و مرتکب با اقدامات خود آن را غیرمستند جلوه می‌دهد (فرض نخست). قبل از نسخ ماده ۶۸ قانون تجارت الکترونیک، با توجه به عبارت «به عنوان داده‌پیام‌های معتبر استفاده نماید» مندرج در آن ماده، تحقق جرم مشروط بر این امر بود که داده مجعول در نهایت معتبر به نظر برسد. از این رو حالت اخیر جزء مصادیق جعل به حساب نمی‌آمد. در مقررات ملی اکثر کشورها نیز رویه به همین صورت است. زیرا در اکثر کشورها جعل رایانه‌ای از نظر مادی دارای دو عنصر اساسی است: یکی تغییر یا دستکاری داده و دیگری قصد مرتکب مبنی بر استفاده از داده مجعول به‌عنوان داده معتبر و معتبر به نظر رسیدن داده مجعول[1]. اما در ایران با وضع ماده ۶ ق.ج.ر. و نسخ ماده ۶۸ ق.ت.ا. موضع قانون‌گذار در این خصوص به‌صورت دقیق مشخص نشده است. به نظر می‌رسد مراد مقنن از وضع عبارت کلی «داده‌های قابل استناد» در ماده ۶ ق.ج.ر. این است که این جرم شامل مصداقی که مرتکب با تغییر داده مستند، آن را غیرمستند جلوه می‌دهد، نیز می‌شود. مضافاً این‌که هدف مقنن حمایت از اعتبار کلیه اسناد رایانه‌ای است؛ کما این‌که در خصوص اسناد عادی نیز بی‌اعتبار جلوه دادن اسناد معتبر جرم جعل قلمداد می‌شود. از این رو به نظر می‌رسد مورد اخیر نیز در دامنه مصادیق جعل رایانه‌ای قرار می‌گیرد.

بنابراین ویژگی قابل استناد بودن هم معطوف به داده‌ای است که در نهایت جعل شده و هم داده‌ای که در ابتدا مورد استفاده و دخل و تصرف جاعل قرار گرفته است؛ به عبارت دیگر جعل زمانی محقق می‌شود که یا داده اولیه واقعاً مستند باشد یا داده ثانویه مستند به نظر برسد. از این رو در حالات ۴ و ۶ بر خلاف چهار فرض دیگر جرم جعل محقق نمی‌شود؛ زیرا هیچ‌کدام از داده‌های اولیه یا ثانویه مستند نیستند.

۳. انواع داده‌های دارای ارزش اثباتی

داده به روش‌های مختلفی از ارزش اثباتی برخوردار می‌شود. یکی از مرسوم‌ترین و مطمئن‌ترین روش‌ها، استفاده از امضای الکترونیک است. اما گاهی اوقات قرائن و اوضاع و احوال به گونه‌ای است

1. United Nation Office on Drugs and Crime, Vienna, Comprehensive Study on Cybercrime, Draft—February 2013., p98.

که حتی اگر منتسب‌الیه داده را امضاء نکرده باشد، با توسل به سنجش عقلانی (عرفی) می‌توان داده را دارای ارزش اثباتی تلقی نمود.

لذا باتوجه به بندهای (الف)، (ک) و (ن) ماده ۲ و مواد ۶ الی ۱۶ ق.ت.ا. و سایر مقرراتی که در مطالب پیش رو مورد تبیین قرار می‌گیرد داده‌ها از حیث ارزش اثباتی به سه دسته داده‌های فاقد ارزش اثباتی، داده‌های دارای ارزش اثباتی مطمئن و داده‌های دارای ارزش اثباتی عادی (غیر مطمئن) قابل تقسیم هستند.

۱.۳. جعل داده‌های دارای ارزش اثباتی مطمئن

داده در صورتی که به امضای الکترونیک مطمئن منضم باشد دارای ارزش اثباتی مطمئن است. مطابق بند «ی» ماده ۲ قانون تجارت الکترونیک؛ « امضای الکترونیکی (Signature Electronic): عبارت از هر نوع علامت منضم شده یا به نحو منطقی متصل شده به داده پیام است که برای شناسایی امضاء کننده داده پیام، مورد استفاده قرار می‌گیرد».

قانون تجارت الکترونیک امضای الکترونیک را معادل امضای سنتی دانسته و در ماده ۷ مقرر داشته: «هر گاه قانون وجود امضاء را لازم بداند امضای الکترونیکی مکفی است». بر اساس بند «ی» ماده ۲ ق.ت.ا. هر نوع امضای الکترونیک حتی امضای عادی دارای ارزش اثباتی است. البته قید «برای شناسایی امضاء کننده» گویای این است که صرفاً علامت‌هایی امضاء محسوب می‌شوند که نشان‌دهنده هویت امضاء کننده باشند.

در اینجا ذکر این امر نیز ضروری است که امضای الکترونیک با امضاء ذیل اسناد مادی تفاوت های زیادی دارد. امضاء ذیل اسناد و نوشته‌های مادی که به اشکال مختلفی از جمله نوشتن نام، نام‌خانوادگی یا نشانه خاصی ایجاد می‌شود، با داشتن سه ویژگی «انحصاری بودن»، «انتساب به شخص معین» و «پیوستگی به متن» دو نقش ایجاد رابطه انتساب و قصد منتسب الیه بر تایید مندرجات را به خوبی ایفا می‌کند (آهنی، ۱۳۹۱: ۴۴). در مقابل امضای الکترونیک شامل روش‌های مختلفی از جمله نوشتن نام تنظیم‌کننده ذیل پیغام الکترونیکی یا کلیک عبارت «می‌پذیرم» در قراردادهای «کلیک-قرارداد» یا وارد کردن گذر واژه در خصوص کارت‌های اعتباری و غیره می‌شود. این امضاءها تقریباً هم نشان‌دهنده هویت امضاءکننده است و هم بر تأیید مندرجات داده توسط منتسب‌الیه دلالت دارد ولی به‌دلیل سهولت جعل و تغییر و نداشتن پیوستگی ذاتی به امضاء کننده، به اندازه امضاءهای سنتی، دو مقوله رابطه انتساب و تأیید مندرجات را با ضریب اطمینان بالا تضمین نمی‌کنند. اما امضاءهای الکترونیک مطمئن به لحاظ ویژگی‌هایی که دارند دارای اعتباری بیش از امضای الکترونیک عادی هستند.

امضای الکترونیک در صورتی‌که از ویژگی‌های مندرج در ماده ۱۰ ق.ت.ا. برخوردار باشد مطمئن محسوب می‌شود. این ماده مقرر می‌دارد: «امضای الکترونیکی مطمئن باید دارای شرایط زیر باشد:

الف- نسبت به امضاء کننده منحصر به فرد باشد.

ب- هویت امضاء کننده داده پیام را معلوم نماید.

ج- به وسیله امضاء کننده و یا تحت اراده انحصاری وی صادر شده باشد.

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

اوصاف مندرج در این ماده در حال حاضر با امضای الکترونیک مبتنی بر رمزنگاری انطباق دارد. امضای الکترونیک مبتنی بر رمزنگاری، توسط اشخاص ثالثِ معتبر از جمله نهادهایی موسوم به «دفاتر خدمات صدور گواهی الکترونیکی»، ارائه و تأیید می‌شوند. لذا یکی از روش‌های نوین امضای الکترونیکی مطمئن، امضای الکترونیکی مبتنی بر رمزنگاری نامتقارن کلید عمومی و خصوصی است که در ایران دفاتر خدمات صدور گواهی الکترونیکی متصدی ایجاد و تأیید چنین امضاءهایی هستند.

ماده ۱۴ قانون تجارت الکترونیکی اشعار داشته داده مطمئن در حکم اسناد معتبر و قابل استناد است. بر اساس ماده ۱۵ نیز «نسبت به داده پیام مطمئن، سوابق الکترونیکی مطمئن و امضای الکترونیکی مطمئن، انکار و تردید مسموع نیست و تنها می‌توان ادعای جعلیت به داده پیام مزبور نمود یا ثابت نمود که داده پیام مزبور به جهتی از جهات قانونی از اعتبار افتاده است». ماده اخیر در مقایسه با ماده ۱۲۹۲ قانون مدنی برای داده پیام مطمئن اثری مشابه اسناد رسمی قائل شده است. بنابراین داده‌های منضم به امضای الکترونیکی مطمئن از ارزش اثباتی بیش از اسناد عادی برخوردارند.

از این رو داده‌هایی که منضم به امضاء الکترونیک مطمئن هستند دارای بالاترین ارزش اثباتی هستند. زیرا به‌کارگیری فناوری‌های پیشرفته در امضاء الکترونیک مطمئن، انتساب داده به صادر کننده آن، هویت صادرکننده و تمامیت داده را تضمین می‌کند. بعلاوه با استفاده از این امضاءها کوچک‌ترین تغییر پس از انضمام امضاء به داده قابل تشخیص است.

شیوه‌های گوناگونی برای جعل داده‌های دارای ارزش اثباتی مطمئن وجود دارد. برای مثال اگر شخص امضای الکترونیکی مطمئن متعلق به دیگری را به داده ایجاد شده توسط خودش منضم کند و یا امضایِ با ویژگی‌های ظاهری امضای الکترونیکی مطمئن را ایجاد نماید و آن را منتسب به مراکز مجاز صدور امضاء مطمئن نماید، مرتکب جعل داده‌ی دارای ارزش اثباتی مطمئن شده است.

۲.۳. جعل داده‌های دارای ارزش اثباتی عادی

داده در دو صورت زیر دارای ارزش اثباتی عادی است:

الف) داده‌های منضم به امضای الکترونیک عادی؛

ب) داده‌هایی که بر اساس اوضاع و احوال دارای ارزش اثباتی هستند.

الف) داده‌های منضم به امضاء الکترونیک عادی (ساده)

بر اساس بند ک ماده ۲ هر امضایی که مطابق ماده ۱۰ قانون تجارت الکترونیک نباشد امضای الکترونیک عادی یا ساده محسوب می‌شود. روش‌های متفاوتی برای امضاء الکترونیک ساده وجود دارد. برای نمونه پیوست کردن تصویر ساده امضای دستی به داده، تایپ نام شخص ذیل داده، ورود رمز برای کارت هوشمند و انتخاب واژه موافقم روش‌های امضای ساده محسوب می‌شوند. در همین راستا رویه قضایی کشور یونان نامه الکترونیک (ایمیل) را با این استدلال که استفاده از رمز ورود، امضای الکترونیک عادی تلقی می‌شود، داده منضم به امضای الکترونیک عادی محسوب می‌کند (وزووس، ۲۰۱۳: ۱۹۸-۲۰۰). بر این اساس در کشور یونان هک رمز ایمیل صرف نظر از این‌که مرتکب وارد ایمیل شود یا نه، جعل امضای الکترونیک عادی تلقی می‌شود. در حقوق ایران باتوجه به تعریف قانونی امضای الکترونیک مندرج در بند «ی» ماده ۲ قانون تجارت الکترونیک گذرواژه یکی از مصادیق امضای الکترونیک است زیرا این داده (گذرواژه) علامتی است که به داده‌پیام مربوط به دستور ورود به ایمیل یا سایر ابزارها و خدمات الکترونیک متصل می‌شود و «برای شناسایی امضاء کننده داده پیام، مورد استفاده قرار می‌گیرد». حقوق‌دانان نیز بر امضای الکترونیک بودن گذرواژه صحه گذاشته‌اند (بای، ۱۳۸۸: ۴۶۴). با این وجود مقنن در ماده یک ق.ج.ر. برای جرم دسترسی غیر مجاز از طریق جعل گذرواژه[1] مجازاتی به مراتب کمتر از جعل رایانه‌ای در نظر گرفته است[2]. این نحوه قانون‌گذاری مانند این است که مقنن برای خیانت در امانت از طریق تخریب عمدی مجازاتی کمتر از تخریب عمدی مقرر کند. به پیروی از این ماده یکی از شعب

---

۱. دلیل اینکه هک گذرواژه جعل امضای الکترونیک به حساب می‌آید این است که مرتکب داده‌ی قابل استناد ایجاد شده توسط خودش را به دیگری (دارنده واقعی داده) منتسب میکند.

۲. ماده یک قانون جرایم رایانه‌ای مقرر داشته دسترسی غیر مجاز در صورتی قابل مجازات است که داده‌ها یا سامانه از طریق تدابیر امنیتی (ازجمله قراردادن گذرواژه، نصب باروی آتشین، رمزنگاری و پنهانگذاری) حفاظت شده باشد، بر این اساس وقوع این جرم مستلزم نقض این تدابیر است و نظر به اینکه یکی از مهمترین این تدابیر قرار دادن رمز عبور است مقنن برای ارتکاب رفتارهای جعل رمز عبور و دسترسی غیر مجاز به داده یا سامانه یک مجازات قرار داده است (عالی پور، ۱۳۹۳: ۱۶۶- ۱۷۲). همچنین در ارتباط با ارکان جرم دسترسی غیرمجاز و چگونگی اعمال مقررات مربوط به تعدد مادی و معنوی جرم دسترسی غیر مجاز با سایر جرایم رایانه‌ای بنگرید به: (همان: ۱۶۵-۱۷۱).

عمومی کیفری تهران هک گذرواژه را جعل به‌حساب نیاورده و مرتکب را به این جرم محکوم نکرده است. در این پرونده باوجود این‌که در دادنامه اقدام به هک گذرواژه مورد توجه دادگاه قرار گرفته است، مرتکب محکوم به جرم جعل رایانه‌ای نشده و دادگاه متهم را صرفاً مستند به ماده یک قانون جرایم رایانه‌ای به جرم دسترسی غیر مجاز محکوم کرده است[۱].

یکی دیگر از روش‌های امضای الکترونیک پیوست کردن داده به داده‌های مبتنی بر ویژگی‌های زیستی است. داده‌های مبتنی بر ویژگی زیستی به داده‌هایی اطلاق می‌شود که بیانگر ویژگی‌های فیزیکی انسان است. برای مثال داده‌های مربوط به اثر انگشت، عنبیه چشم و تُن صدای اشخاص مصادیق داده‌های مبتنی بر ویژگی زیستی هستند. اگر شخصی داده‌ای را ایجاد نماید و سپس با منضم کردن داده مبتنی بر ویژگی‌های زیستی شخص دیگری به آن، داده ایجاد شده توسط خودش را به دیگری منتسب نماید، از این طریق مرتکب جعل داده دارای ارزش اثباتی عادی شده است.

قانون‌گذار در مواد ۶ و ۷ و بند «ی» ماده ۲ قانون تجارت الکترونیک هر نوع امضای الکترونیکی -در صورتی‌که بیانگر هویت امضاءکننده باشد- را دارای اعتبار دانسته و داده‌پیام و امضای الکترونیکی را به ترتیب برابر با نوشته و امضای سنتی به حساب آورده است. این در حالی است که در برخی از کشورها از جمله برزیل گونه‌هایی از انواع امضاء الکترونیک مانند الصاق داده مربوط به اسکن امضای عادی به داده‌های دیگر را به‌دلیل آسان بودن جعل چنین امضایی، فاقد اعتبار به‌حساب آورده‌اند (روهرمن، ۲۰۰۸: ۲۶). البته می‌توان گفت رویکرد مقنن در کشور ایران سنجیده‌تر است؛ زیرا هر چند امضای الکترونیک عادی به طور کامل تضمین کننده تمامیت سند و هویت صادر کننده آن نیست ولی با وجود این دارای ارزش اثباتی و قابلیت استناد است و باتوجه به این‌که مطابق مفهوم مخالف ماده ۱۵ قانون تجارت الکترونیک ادعای انکار و تردید در مورد آن قابل پذیرش است، این امکان برای مدعی عدم اعتبار امضای عادی وجود دارد که با طرح ادعای انکار یا تردید، بار اثبات صحت امضاء را بر عهده مدعی اصالت امضاء قرار دهد.

بند ۲ ماده ۵ دستورالعمل شماره CE/93/1999 مورخ ۱۳ دسامبر ۱۹۹۹ اتحادیه اروپا نیز امضای الکترونیک عادی را دارای ارزش اثباتی به حساب آورده و اعضاء اتحادیه را از نپذیرفتن آن صرفاً به این دلیل که دارای ساختار الکترونیکی است منع کرده است (زرکلام، ۱۳۸۲: ۳۷).

---

۱. دادنامه شماره 9109970230600270مورخ ۹۱/۸/۳ صادره از شعبه ۱۰۸۳ دادگاه عمومی تهران، تایید شده به موجب دادنامه صادره از شعبه ۳۸ دادگاه تجدید نظر استان تهران به شماره 9109970223801452 مورخ ۱۳۹۱/۱۰/۳۰ قابل دسترسی در سایت بانک آراء پژوهشکده قوه قضاییه به نشانی:
http://j.ijri.ir/SubSystems/Jpri2/Showjudgement.aspx?id=TzAyZnJydmVvTUU9.

بنابراین داده‌های منضم به امضای الکترونیک عادی دارای ارزش اثباتی و معادل سند عادی محسوب می‌شوند. از این رو در مواردی که شخصی مندرجات داده‌ای را با امضای الکترونیک متعلق به دیگری تأیید کند، داده ایجاد شده در ظاهر از ارزش اثباتی عادی برخوردار می‌شود. نتیجه اینکه اگر شخصی اقدام به ایجاد داده‌های منضم به امضای الکترونیک عادی کند و آن را به دیگری منتسب نماید یا این‌که داده ایجاد شده توسط خودش را به امضاء الکترونیک عادی دیگری منضم کند، مرتکب جعل داده با ارزش اثباتی عادی شده است.

ب) داده‌هایی که باتوجه به اوضاع و احوال دارای ارزش اثباتی هستند

ارزش اثباتی داده لزوماً منوط به منضم بودن آن به امضاء الکترونیک نیست. در برخی موارد قرائن و اوضاع و احوال به‌گونه‌ای است که حتی اگر منتسب‌الیه، داده را امضاء نکرده باشد، می‌توان با توسل به سنجش عقلانی (عرفی) داده را دارای ارزش اثباتی عادی دانست.

بند ن ماده ۲ ق.ت.ا. در خصوص سنجش معقول یا عقلانی اشعار می‌دارد: «معقول (سنجش عقلانی)، (Reasonableness Test): با توجه به اوضاع و احوال مبادله داده پیام از جمله: طبیعت مبادله، مهارت و موقعیت طرفین، حجم مبادلات طرفین در مورد مشابه، در دسترس بودن گزینه‌های پیشنهادی و رد آن گزینه‌ها از جانب هر یک از طرفین، هزینه گزینه‌های پیشنهادی، عرف و روش‌های معمول و مورد استفاده در این نوع مبادلات، ارزیابی می‌شود».

ماده ۶۵۵ قانون آیین دادرسی کیفری اصلاحی ۱۳۹۴ نیز داده‌های رایانه‌ای را در صورت رعایت سازوکارهای امنیتی مذکور در مواد قانون مزبور و تبصره‌های آن، دارای اعتبار و قابل استناد دانسته است. لذا این قانون نیز اعتبار داده‌ها را مشروط به منضم بودن آن به امضاء الکترونیک نکرده است.

از طرف دیگر ماده ۱۳ ق.ت.ا. نیز تلویحاً ارزش اثباتی داده را منوط به انضمام داده به امضای الکترونیک منتسب الیه ندانسته و اشعار داشته «به‌طور کلی، ارزش اثباتی داده پیام‌ها باتوجه به عوامل مطمئنه از جمله تناسب روش‌های ایمنی به‌کار گرفته شده با موضوع و منظور مبادله داده پیام تعیین می شود». واژه «تناسب» در این ماده انعکاس دهنده یک معیار نوعی است. بنابراین مطابق این ماده، تشخیص میزان ارزش اثباتی داده به دادگاه واگذار شده است (ساعی، ۱۳۹۰: ۱۶۸) و دادگاه می‌تواند با توجه به ارتباط بین روش‌های به کار گرفته شده و موضوع مبادله داده، رابطه انتساب و تأیید داده را احراز نماید و مشخص نماید که آیا داده دارای ارزش اثباتی به‌نظر می‌رسد یا خیر. به عبارت دیگر آنچه از این ماده می‌توان استنباط نمود این است که برای این‌که داده‌ای دارای ارزش اثباتی باشد ضرورتاً لازم نیست از طرف منتسب الیه امضاء شده باشد بلکه

همین‌که روش‌های به کار رفته در تولید و ارسال داده، با موضوع و منظور مبادله داده تناسب داشته باشد، داده دارای ارزش اثباتی است[۱].

در همین ارتباط ماده ۹ قانون نمونه آنسیترال مصوب ۱۹۹۶ معیارهای مختلفی را برای تشخیص قدرت اثباتی داده‌های الکترونیکی برشمرده است[۲]. مطابق این ماده نباید داده‌های الکترونیکی را به این دلیل که به صورت داده پیام است و یا داده پیام فاقد اصل است مردود اعلام کرد. ماده فوق الذکر مقرر نموده قدرت اثباتی داده الکترونیکی بستگی به میزان اعتبار روش ایجاد داده، نگهداری و مبادله و محافظت از تمامیت داده‌ها و نحوه شناسایی فرستنده پیام و سایر ملاحظات مرتبط دیگر، دارد. لذا این قانون نیز سنجش معیارهای قانونی در خصوص کلیه داده‌ها را بر عهده دادرس گذاشته و تفکیکی بین داده‌های منضم به امضای الکترونیک (اعم از عادی یا مطمئن) و غیر آن قائل نشده است[۳]. در کشور ژاپن نیز همین رویه رعایت شده است. برای مثال در یک پرونده کیفری متهم که افسر تحقیق اداره پلیس بوده تاریخ تدوین یک فایل الکترونیکی را تغییر می‌دهد تا از این طریق ادله جرم را امحاء نماید. هر چند داده تغییر یافته توسط متهم منضم به امضای الکترونیک نبوده ولی از آنجا که آن داده در محاکم ژاپن دارای ارزش اثباتی بوده، وی محکوم به یک سال و شش ماه حبس بابت ارتکاب بزه جعل رایانه‌ای می‌شود[۴].

بنابراین در صورتی‌که جاعل داده را به نحوی ایجاد نماید یا تغییر دهد که باتوجه به معیارهای قانونی دارای ارزش اثباتی به نظر برسد ولی در واقع چنین نباشد، داده ایجاد شده در صورت قلب رابطه انتساب مجعول به حساب می‌آید.

---

۱. برخی قوانین خارجی شروط خاصی را برای قابل استناد بودن داده مقرر کرده‌اند. برای مثال قانون امضای الکترونیک ایالت یوتای امریکا مقرر داشته: «اگر فرستنده سند الکترونیکی، از ذخیره یا اخذ پرینت اسناد بوسیله دریافت کننده جلوگیری نماید، آن سند علیه دریافت کننده سندیت نخواهد داشت» (ریچاردز، ۱۹۹۹: ۱۵).

2. UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with Additional Article 5 as Adopted in 1998, United Nation Publication, ISBN 92-1-133607-4.

۳- البته قانونگذار بعضاً موارد خاصی را به موجب قانون یا آیین نامه احصاء می‌نماید که برای تایید، لزوماً نیازمند امضاء الکترونیک، آن هم با ویژگی‌های معینی است. برای مثال در ایالات متحده امریکا، قرارداد الکترونیک بیع با ارزش بیش از پانصد دلار در صورتی الزام آور محسوب می‌شود که مندرجات آن به واسطه امضا الکترونیک با ویژگی‌های خاص مورد تایید طرفین قرار گرفته باشد (اسمندینگاف، ۱۳۸۷: ۲۷۱).

4. Case Translation: Japan Digital Evidence and Electronic Signature Law Review, 9, pario Communications Limited, (2012). Electronic version at: http://www.courts.go.jp/hanrei/pdf/20110816120455.

نتیجه‌گیری

روابط انسان‌ها قرن‌ها به صورت شفاهی و کتبی بوده تا این‌که اختراعات علمی شگرف حوزه اطلاعات و ارتباطات در عصر اخیر سبب دگرگونی گسترده در شیوه برقراری روابط گردید. امروزه ایجاد ارتباط از طریق مبادله داده‌های رایانه‌ای و مخابراتی از طریق ابزارهایی همچون رایانه‌ها، تلفن‌های همراه، فکس، تلفن و سایر ابزارهای نوین ارتباطی به قسمتی مهم از زندگی روزمره اکثر اسخاص مبدل گشته است. استفاده گسترده از این ابزارها در مبادلات مالی و غیرمالی و اتکا مردم به داده‌هایی که از این طرق جابجا می‌شوند اقتضا دارد مقنن در راستای حمایت از روابط اجتماعی مبتنی بر این ابزارها، با رفتارهایی که تمامیت و صحت داده‌ها را مخدوش و نقض می‌کند مبارزه نموده و مرتکبین چنین اعمالی را تحت تعقیب کیفری قرار دهد.

جعل رایانه‌ای یکی از مهم‌ترین جرایمی است که علیه صحت و تمامیت داده‌ها ارتکاب می‌یابد و موجب سلب اعتماد عمومی نسبت به آن می‌شود. نظر به این‌که طیف وسیعی از داده‌ها با ویژگی-ها و اوصاف متکثر و متفاوت توسط ابزارهای رایانه‌ای و مخابراتی جابجا می‌شوند، مسئله مهم مرتبط با جعل رایانه‌ای این است که آیا مقنن همه داده‌ها را موضوع این جرم قرار داده یا از داده-هایی با ویژگی‌های معین حمایت کرده است.

با تجزیه و تحلیل قوانین و مقررات مربوطه این نتیجه حاصل آمد که موضوع جعل رایانه‌ای گونه خاصی از داده‌های رایانه‌ای یا مخابراتی نیست بلکه هر نوع داده‌ای اعم از داده‌های دیجیتالی، نوری، الکترومغناطیسی و ... که قابل انتقال از طریق ابزارهای ارتباطی مختلف از قبیل فکس، تلگراف، رایانه و گوشی همراه باشد، می‌تواند موضوع جرم جعل رایانه‌ای قرار گیرد. به‌علاوه این‌که صرفاً داده‌های به شکل نوشته موضوع جرم جعل قرار نمی‌گیرند بلکه سایر داده‌ها از جمله داده-هایی که به شکل رمز، صوت یا تصویر باشند نیز ممکن است در صورت داشتن شرایط قانونی جعل شوند. البته همان‌طور که در جعل مادیِ موضوعاتِ فیزیکی، مقنن هر نوشته‌ای را موضوع جرم جعل ندانسته و جز در مواردی اندک، موضوع جعل را سند (نوشته قابل استناد در مقام دفاع و دعوی) قرار داده است، در جعل رایانه‌ای نیز صرفاً داده‌ای موضوع جرم قرار می‌گیرد که دارای ویژگی‌های معینی باشد. ویژگی‌های اساسی داده‌های مجعول یکی این است که رابطه انتساب بین آن‌ها و منتسب الیه مقلوب و مخدوش شده باشد و دیگر این‌که دارای قابلیت استناد به نظر برسند. قلب رابطه انتساب که همان قلب حقیقت است در صورتی محقق می‌شود که داده واقعاً به کسی که ظاهراً نماینگر آن است، منتسب نباشد و داده در صورتی دارای قابلیت استناد به‌نظر می‌رسد که حداقل در ظاهر دارای ویژگی‌های داده‌ی دارای ارزش اثباتی باشد، هر چند چنین داده‌هایی اساساً فاقد ارزش اثباتی هستند.

داده‌هایِ دارای ارزش اثباتی، از ویژگی‌ها و ممیزه‌های متفاوتی برخوردارند و نظر به اینکه مطابق ماده ۶ ق.ج.ر. لازم است داده موضوع جعل، قابل استناد باشد یا اینکه دستکم در ظاهر ویژگی‌های داده قابل استناد را داشته باشد، شناخت داده مجعول مستلزم شناخت اوصاف داده قابل استناد یا دارای ارزش اثباتی است به عبارت دیگر شناخت ویژگی‌های داده‌های دارای ارزش اثباتی به ما کمک می‌کند تا دریابیم، داده ایجاد یا ارسال شده و یا تغییر یافته، مجعول هست یا خیر.

مستنبط از قوانین و مقررات ایران داده‌ها از حیث ارزش اثباتی به سه دستهٔ داده‌های فاقد ارزش اثباتی، داده‌های دارای ارزش اثباتی مطمئن و داده‌های دارای ارزش اثباتی عادی قابل تفکیک هستند. نوع آخر داده‌ها نیز به دو دستهٔ داده‌های منضم به امضای الکترونیک عادی و داده-هایی که باتوجه به اوضاع و احوال دارای ارزش اثباتی هستند، دسته‌بندی می‌شوند. هر کدام از این داده‌ها اوصاف و ویژگی‌های معینی دارند. به‌طور کلی، از حیث قابلیت استناد؛ داده معادل نوشته است، داده‌های دارای ارزش اثباتیِ مطمئن ارزشی همسان با اسناد رسمی و داده‌های دارای ارزش اثباتی عادی دارای ارزش اثباتی مشابه اسناد عادی هستند. با این وجود مقنن در تعیین مجازات تقاوتی بین جعل داده دارای ارزش اثباتی مطمئن با داده دارای ارزش اثباتی عادی قائل نشده است.

مطابق ماده ۶ ق.ج.ر. رفتار مجرمانه جعل رایانه‌ای عبارت است از «تغییر یا ایجاد داده‌های قابل استناد یا ایجاد یا وارد کردن متقلبانهٔ داده به آن‌ها». بر این اساس این پرسش مطرح می‌شود که برای تحقق جرم کدام داده باید قابل استناد باشد؟ داده اولیه که موضوع دخل و تصرف جاعل قرار می‌گیرد یا داده‌ای که در نهایت توسط جاعل به‌وجود می‌آید؟ برای پاسخ به این پرسش فروض شش‌گانه جعل از حیث قابل استناد بودن داده اولیه و ثانویه تشریح شد و مشخص شد در چهار حالت جعل محقق می‌شود؛ نخست زمانی که داده در ابتدا مستند باشد و با اقدامات جاعل غیر مستند به نظر برسد. دوم وقتی که داده اولیه مستند باشد و مرتکب با تغییر در مندرجات اصلی داده آن را به نحو دیگری مستند جلوه دهد. سوم حالتی که مرتکب با تغییر در مندرجات داده غیر مستند، آن را مستند جلوه دهد و چهارم موردی است که مرتکب اقدام به ایجاد داده به ظاهر مستند نماید. آنچه از ماده ۶ ق.ج.ر. قابل برداشت است این است که داده در حالت نخست باید واقعا دارای ارزش اثباتی باشد ولی در حالات دوم تا چهارم نیازی نیست داده واقعاً دارای ارزش اثباتی باشد بلکه همین که در ظاهر از ویژگی‌های داده مستند برخوردار باشد، برای تحقق جرم جعل رایانه‌ای کافی است.

منابع

آزمایش، علی (۱۳۷۳)، **تقریرات درس حقوق جزای اختصاصی**، دانشکده حقوق دانشگاه تهران.

آهنی، بتول (۱۳۹۱)، «اعتبار و نفوذ قراردادهای الکترونیک»، **فصلنامه حقوق**، مجله دانشکده حقوق و علوم سیاسی، دوره ۴۲، شماره۱، ص ۵۲-۳۷.

اسمندینگاف، توماس جی. (۱۳۸۷)، «قواعد ضروری جهت اعتبار تعاملات (تراکنشهای) الکترونیکی در عرصه جهانی»، ترجمه مصطفی بختیاروند، **مجله حقوقی بین المللی**، شماره ۳۸، ص ۲۸۳-۲۶۱.

اصلانی، حمیدرضا (۱۳۸۴)، **حقوق فن‌آوری اطلاعات**، چاپ اول، تهران: نشر میزان.

ایزدی فرد، علی‌اکبر و پیردهی حاجیکلا، علی (۱۳۸۹)، «سرقت اینترنتی: حدی یا تعزیری؟»، **مطالعات اسلامی: فقه و اصول**، سال چهل و دوم، شماره ۸۴/۱، ص ۶۸-۴۵.

بای، حسینعلی و پورقهرمانی، بابک (۱۳۸۸)، **بررسی فقهی حقوقی جرایم رایانه‌ای**، چاپ اول، مشهد: پژوهشگاه علوم و فرهنگ اسلامی.

جلالی فراهانی، امیرحسین (۱۳۸۶)، «استنادپذیری ادله الکترونیکی در امور کیفری»، **فقه و حقوق**، سال چهارم، شماره ۱۵، ص ۱۱۳-۸۳.

جاویدنیا، جواد (۱۳۸۶)، «نقد و بررسی جرم‌های مندرج در قانون تجارت الکترونیک»، **مجله حقوقی دادگستری**، شماره ۵۹، ص ۱۷۸-۱۲۵.

_____ (۱۳۸۷)، **جرایم تجارت الکترونیکی**، چاپ اول، تهران: خرسندی.

حیدری، علی‌مراد (۱۳۹۱)، «جعل رایانه‌ای در بستر تجارت الکترونیک»، **فقه و حقوق ارتباطات**، شماره سوم، ص ۳۱-۵.

زرکلام، ستار (۱۳۸۲)، «امضای الکترونیک و جایگاه آن در نظام ادله اثبات دعوا»، **مدرس علوم انسانی**، شماره ۲۸، ص ۵۶-۳۳.

_____ (۱۳۸۸)، «قانون تجارت الکترونیکی در بوته نقد»، مصاحبه با مجله تعالی حقوق، **ماهنامه آموزشی دادگستری کل استان خوزستان**، شماره ۳۶، سال چهارم، شهریور، ص ۲۵-۱۲.

زیبر، اولریش (۱۳۹۰)، **جرایم رایانه‌ای**، ترجمه محمدعلی نوری و همکاران، چاپ دوم، تهران: گنج دانش.

ساعی، سیدمحمدهادی و رضا باباخانی (۱۳۹۰)، «بررسی ارزش اثباتی اسناد الکترونیک در حقوق ایران»، **پژوهش‌نامه حقوق اسلامی**، سال سیزدهم، شماره اول، ص ۱۸۸-۱۵۷.

ساورایی، پرویز (۱۳۹۲)، «فراداده و قابلیت استناد به آن در مراجع اداری و قضایی»، **مجله تحقیقات حقوقی**، شماره ۶۲، ص ۵۱۵-۴۶۱.

_____ (۱۳۹۱)، «نقدی بر قانون تجارت الکترونیک ایران»، **مجله تحقیقات حقوقی**، شماره ۶۰، ص ۴۰۳-۳۶۹.

_____ (۱۳۹۳)، «تحلیل حقوقی سند»، **مجله تحقیقات حقوقی**، شماره ۶۵، ص ۱۰۷-۸۳.

شهبازی‌نیا، مرتضی و عبدالهی، محبوبه (۱۳۸۹)، «دلیل الکترونیک در نظام ادله اثبات دعوا»، **فصلنامه حقوق دانشگاه تهران**، دوره ۴۰، شماره ۴، ص ۲۰۵-۱۹۳.

عالی پور، حسن (۱۳۸۴)، «جرم‌های مرتبط با محتوا، محتوای سیاه فن آوری اطلاعات»، مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فن‌آوری اطلاعات، چاپ اول، انتشارات سلسبیل تهران، ص ۱۶۷-۱۴۲.

_____ (۱۳۹۳)، حقوق کیفری فناوری اطلاعات، چاپ سوم، تهران: انتشارات خرسندی.

عبدالهی، محبوبه (۱۳۸۷)، «دلیل الکترونیکی در دعوای حقوقی»، پایان نامه کارشناسی ارشد حقوق خصوصی، دانشگاه تربیت مدرس.

فضلی، مهدی (۱۳۹۱)، **مسئولیت کیفری در فضای سایبر**، چاپ دوم، تهران: انتشارات خرسندی.

قناد، فاطمه (۱۳۹۰)، «جعل در بستر فناوریهای اطلاعات و ارتباطات»، **آموزه‌های حقوق کیفری**، دانشگاه علوم اسلامی رضوی، شماره ۲، ص ۸۸-۶۳.

میرمحمدصادقی، حسین (۱۳۸۴)، **جرایم علیه امنیت و آسایش عمومی**، چاپ پنجم، تهران: نشر میزان.

منصورآبادی، عباس و فتحی، محمد جواد (۱۳۹۰)، «موضوع جعل و تزویر»، **مجله تحقیقات حقوقی**، شماره ۵۳، ص ۱۸۲-۱۴۷.

منصورآبادی، عباس و فتحی، محمدجواد (۱۳۸۷)، «رفتار مجرمانه جعل و تزویر»، **پژوهش حقوق و سیاست**، شماره ۲۸، ص ۳۰۰-۲۷۹.

منصورآبادی، عباس و فتحی، محمد جواد (۱۳۹۲)، **جعل و تزویر و جرایم وابسته**، چاپ دوم، تهران: سمت.

میرکمالی، سیدعلیرضا و عباس‌زاده امیرآبادی، احسان (۱۳۹۳)، «تحلیل جرم جعل مفادی»، **آموزه‌های حقوق کیفری**، دانشگاه علوم اسلامی رضوی، شماره ۸، ص ۲۴۱-۲۰۷.

نوری، محمد علی و نخجوانی، رضا (۱۳۸۳)، **حقوق حمایت داده‌ها**، چاپ اول، تهران: گنج دانش.

هیات مولفان و ویراستاران انتشارات مایکروسافت (۱۳۸۱)، **فرهنگ تشریحی اصطلاحات کامپیوتری مایکروسافت**، ترجمه فرهاد قلی‌زاده نوری، چاپ اول، تهران: کانون نشر علوم.

گزارش توجیهی پیش نویس قانون تجارت الکترونیکی (بی‌تا)، مرکز ملی شماره گذاری کالا و خدمات ایران وابسطه به موسسه مطالعات و پژوهش‌های بازرگانی.

Austria, Stephanie, **Forgery in Cyberspace: The Spoof could be on you!**, (2004). University of Pittsburgh School of Law, Journal of Technology Law and Policy,.

Clough, Jonatan, **The Council of Europe Convention on Cyber Crime: Defining 'Crime' In a Digital World**, (2012). Criminal Law Forum, At: www.springer.com. (last visited: 6.17.2016)

Gercke, Marco, **Understanding Cyber Crime: Phenomena, challenges and legal response**, (2012). ITU publication,. At: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html. (last visited: 6.21.2016)

Rohrmann, Carlos Alberto and Jason Soares Albergaria Neto, **Digital Evidence and Electronic Signature Law in Brazil**, (2008). Vol 5, Pario Communications Limited, at: www.deaeslr.org. (last visited: 7.17.2016)

Richards R., Jason, **The Utah Digital Signature Act As "Model" Legislation: A Critical Analysis**, (1999). Volume (17, Issue 3 Journal of Computer & Information Law).

Schjolberg, Stein and Chief judge, **Computer-Related Offences**, (2004). at: www.cybercrimelaw.net. (last visited: 8.5.2016)

Vossos, F., **Definition and legal nature of electronic documents, case translation: Greece, Pario Communications Limited,** (2013), at: www.sas-space.sas.ac.uk. (last visited: 8.21.2016).

- اسناد

Case Translation: Japan Digital Evidence and Electronic Signature Law Review, 9, pario Communications Limited, (2012). Electronic version at: http://www.courts.go.jp/hanrei/pdf/20110816120455. (last visited: 8.20.2016).

UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with Additional Article 5 as Adopted in 1998, United Nation Publication, ISBN 92-1-133607-4.

United Nation Office on Drugs and Crime, Vienna, Comprehensive Study on Cybercrime, Draft—February 2013.