پژوهش حقوق کیفری، سال چهارم، شماره دوازدهم، پاییز 1394، ص 97-69

حفظ صحت و استنادپذیری ادله‌ی الکترونیک با استفاده از بیومتریک و رمزنگاری

حسنعلی مؤذن زادگان* ـ الهام سلیمان دهکردی** ـ مهشید یوشی***

(تاریخ دریافت: 1393/12/5، تاریخ پذیرش: 1394/8/24)

چکیده

استنادپذیری ادله‌ی الکترونیک عبارت از واجد اعتبار بودن داده‌های الکترونیک در محضر دادگاه و ایفای نقش در صدور رأی مقتضی است. برای این که دلیل الکترونیک بتواند همانند ادله‌ی سنتی کارکرد اثباتی داشته باشد، باید دو شرط عمده‌ی استنادپذیری یعنی صحت انتساب، اصالت و انکارناپذیری را دارا باشد. برای محقق شدن این دو شرط اساسی ضروری است داده‌ها در مرحله‌ی توقیف به صورت مناسب حفاظت شوند. در بند «ط» ماده‌ی 2 قانون تجارت الکترونیک و ماده‌ی 40 قانون جرایم رایانه‌ای به استفاده از راهکارهای ایمن جهت حفاظت از داده‌ها اشاره شده که از مهم‌ترین آن‌ها می‌توان به بیومتریک و رمزنگاری اشاره کرد. فناوری بیومتریک داده‌های اشخاص را با توجه به الگوی عمومی دریافت و پردازش می‌کند و تنها به فردی که داده‌هایش پردازش شده اجازه‌ی دستیابی به اطلاعات می‌دهد و دیگران نمی‌توانند به اطلاعات دست یابند؛ در رمزنگاری نیز اطلاعات به وسیله‌ی در هم سازی به گونه‌ای که تنها با یک کلید محرمانه از حالت در هم خارج می‌شوند، مورد حفاظت قرار می‌گیرند و برای فردی که به این اطلاعات دسترسی ندارد، ناخوانا باقی می‌ماند. به این شیوه داده‌ها از خطر تغییر و تحریف محفوظ باقی می‌مانند و می‌توانند به گونه‌ای مطمئن مورد استناد قرار گیرند.

کلمات کلیدی: دلیل الکترونیک، استنادپذیری ادله‌ی الکترونیک، بیومتریک، رمزنگاری

---

* دانشیار گروه حقوق کیفری و جرم شناسی دانشگاه علامه طباطبایی

** دانشجوی دکتری حقوق کیفری و جرم شناسی دانشگاه علامه طباطبایی(نویسنده مسؤول)

Email: soleiman.elham@gmail.com

*** کارشناس ارشد حقوق کیفری و جرم شناسی دانشگاه قم

مقدمه

حقوق سنتی به دلیل گسترش فناوری اطلاعات با نوع جدیدی از ادله در کشف جرم روبه‌رو شده که این ادله به دلیل مشکلاتی از قبیل «دشوار بودن صحت انتساب، قابلیت تحریف، تخدیش و تخریب» دستگاه قضایی را در کشف و اثبات با چالش جدیدی مواجه نمود. این چالش ازاین‌رو است که تضمین امنیت، اعتبار و اصالت داده‌ها که پیش‌شرط تعیین‌کننده‌ی استنادپذیری ادله‌ی الکترونیک محسوب می‌شود، امری به‌غایت دشوار است و تنها از طریق راهبردهای فنی تااندازه‌ای محقق می‌شود. قانون‌گذار ایران نیز از توجه به این راهبردهای فنی غافل نبوده و در مقررات مختلف به این ضرورت اشاره‌کرده است. نخست قانون‌گذار در *بند ط* قانون تجارت الکترونیک به‌کارگیری رویه‌ی ایمن را برای تطبیق صحت ثبت داده‌پیام و جلوگیری از هرگونه خطا یا تغییر در مبادله، محتوا یا ذخیره‌سازی ضروری دانسته و در ماده‌ی 14 همین قانون تنها داده‌ای که از طریق مطمئن ایجاد و نگهداری شده، دارای ارزش اثباتی دانسته است؛ در ادامه قانون جرایم رایانه‌ای در ماده‌ی 40 در بحث توقیف داده‌ها به تدابیر امنیتی به‌طور تمثیلی پرداخته و در آیین‌نامه‌ی استنادپذیری ادله‌ی الکترونیک به‌ضرورت استفاده از این راهکارها در مواد 1، 15 و 38 صحه گذارده و سرانجام در ماده‌ی 656 قانون آیین دادرسی کیفری مصوب 1392 مقنن به این موضوع پرداخته و استفاده از تمهیدات امنیتی مطمئن برای احراز هویت و احراز اصالت را ضروری تلقی می‌کند. با نظر به اشارات مکرر قانون‌گذار به استفاده از این تدابیر امنیتی به نظر می‌رسد بن‌مایه‌ی قابلیت استناد بودن این ادله، اتخاذ این تدابیر است هرچند تاکنون اقدامات چندانی در خصوص فراهم ساختن بسترها جهت استفاده از این راهکارها انجام نشده است.

لازم به ذکر است داده‌هایی که در محاکم قضایی مورد استناد قرار می‌گیرند به دودسته‌ی داده‌های شخصی و داده‌های عمومی تقسیم می‌شوند. داده‌های شخصی بنا بر قانون انتشار و دسترسی آزاد به اطلاعات به اطلاعات فردی نظیر نام و نام خانوادگی، عادت‌های فردی، ناراحتی‌های جمعی، شماره‌حساب بانکی و رمز عبور اطلاق می‌شود. این داده‌ها به سه قسم بیومتریکال، نسبت‌دهی شده و زندگی‌نامه‌ای تقسیم‌شده است که در قانون دسترسی آزاد به اطلاعات تنها به اطلاعاتی که به فرد نسبت داده‌شده و اطلاعاتی که

در طول زندگی کسب نموده، توجه شده و به اطلاعات شخصی بیومتریکال اشاره نشده است. بر اساس این قانون اطلاعات عمومی اطلاعاتی غیرشخصی هستند که از مصادیق مستثنیات این قانون نباشند، نظیر آیین‌نامه‌ها و ... با تحقیق در این دو تعریف به نظر می‌رسد اطلاعات شخصی بیومتریکال که صفات فیزیکی منحصربه‌فردی هستند تا حد زیادی از خطاپذیری به دورند و افراد برای حفاظت از اصالت و تمامیت داده‌های خود از این بخش از داده‌هایشان به‌عنوان راهبردی امنیتی استفاده می‌کنند. مراجع قضایی نیز درصورتی‌که اشخاص اطلاعات خود را به آن‌ها دهند می‌توانند از اطلاعات بیومتریکال خود جهت حفاظت و حراست از آن‌ها استفاده کنند؛ اما گاهی فرد اطلاعات مهم خود را با استفاده از رمزنگاری حفاظت و حراست می‌کند، با استفاده از این شیوه نیز صحت و اصالت داده حفظ می‌شود و درصورتی‌که مراجع قضایی نیاز به این اطلاعات داشته باشند فرد بایست اطلاعات خود را در اختیار مأموران ذی‌صلاح قرار دهد و آن‌ها نیز درصورتی‌که بخواهند به این اطلاعات استناد کنند باید از دو شیوه‌ی ایمن‌سازی پیش‌گفته استفاده نماید. این رویه در مواد 656 و 658 قانون آیین دادرسی کیفری مورداشاره قرارگرفته و حتی در مواد 660 و 661 این قانون برای افرادی که موجبات افشای این داده ها و نقض تدابیر امنیتی سامانه را فراهم می‌سازند، مجازات تعیین‌شده است.[1]

در ادامه به تبیین بیومتریک و رمزنگاری که مصادیق بارز این تدابیر امنیتی است، پرداخته می‌شود و اثرات عملی استفاده از این راهبردها در جهت استنادپذیری ادله‌ی الکترونیک بیان می‌شود.

دلیل الکترونیک و استنادپذیری آن

الف. دلیل الکترونیک

دلیل در لغت به معنی راهنماست. در ماده 194 قانون آیین دادرسی مدنی این‌طور آمده: «دلیل امری است که اصحاب دعوا برای اثبات یا دفاع از ادعا به آن استناد می‌کنند» (کاتوزیان 1388: 42). در حقوق کیفری تعریفی از دلیل ارائه نشده است و تنها در ماده

1- پیش‌ازاین نیز قانون‌گذار در ماده‌ی 40 و 49 و 50 قانون جرائم رایانه‌ای و ماده‌ی 11 و 15 و 16 آیین‌نامه‌ی استناد پذیری ادله‌ی الکترونیک نیز به این امر اشاره‌کرده است.

160 قانون مجازات اسلامی مصوب 1392 قانون‌گذار به احصای ادله پرداخته است: «ادله‌ی اثبات جرم عبارت از اقرار، شهادت، قسامه و سوگند در موارد مقرر قانونی و علم قاضی است». با تدقیق در این مقرره به نظر می‌رسد قانون‌گذار به‌صراحت علم قاضی را به‌عنوان یکی از ادله برشمرده است و خلاف قانون مجازات اسلامی سابق تفکیکی میان استناد به علم قاضی در دعاوی حق‌الناسی و حق‌اللهی قائل نشده است و اقناع وجدانی قاضی اهمیت دوچندانی یافته است؛ بنابراین قاضی در دو مرحله‌ی گردآوری ادله و ارزیابی آن در چارچوب قانون از آزادی عمل برخوردار است و می‌تواند از ادله‌ی الکترونیک نیز برای اثبات و احراز جرم استمداد جوید؛ هرچند در قانون آیین دادرسی کیفری مصوب 1392 (اصلاحی 1394) در فصل دادرسی الکترونیک نیز تعریفی از این نوع از ادله ارائه نشده است.

دلیل الکترونیک در معنی رایج و مصطلح عبارت است از «هر داده‌پیامی که اصحاب دعوا برای اثبات یا دفاع از مدعای خود به آن استناد می‌کنند» (شهبازی نیا 1389: 208). در این تعریف، ادله‌ی الکترونیک با واژه‌ی «داده‌پیام» تعریف‌شده است که شرح آن در ماده 2 قانون تجارت الکترونیک آمده است.[1] قانون‌گذار با الهام از قانون نمونه تجارت الکترونیک آنسیترال، قانون تجارت الکترونیک و ماده 47 آیین‌نامه‌ی استناد پذیری ادله‌ی الکترونیک مصوب 1393، داده‌پیام را تنها منحصر به ابزارهای الکترونیک ننموده است و هر ابزاری اعم از تلگرام، تلکس، ابزارهای نوری و سایر ابزارهای ناشی از فناوری اطلاعات همانند پوشه‌های صوتی و تصویری نیز دلیل الکترونیک محسوب می‌شوند و قالب ادله‌ی الکترونیک موضوعیت نداشته و قانون‌گذار تنها به محتوای داده‌پیام توجه نموده است (محمدی 1388: 153). در صدر ماده 12 قانون تجارت الکترونیک[2] واژه‌ی «اسناد» با حرف «و» عطف به واژه‌ی ادله شده و این شبهه را ایجاد کرده که ادله‌ی الکترونیک تنها در قالب سند قابلیت ظهور و بروز را دارند؛ اما با توجه به عبارت ذیل ماده به نظر می‌رسد این شبهه

1- ماده 2 قانون تجارت الکترونیک: «هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری یا فناوری جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود».

2- ماده 12 قانون تجارت الکترونیک: «اسناد و ادله‌ی اثبات دعوا ممکن است به‌صورت داده‌پیام بوده و در هیچ محکمه یا اداره‌ی دولتی نمی‌توان بر اساس قواعد ادله‌ی موجود، ارزش اثباتی داده‌پیام را صرفاً به دلیل شکل و قالب آن رد کرد».

قابل حل است و دلیل الکترونیک در هر قالبی صرف‌نظر از محتوا قابلیت ظهور دارد. هرچند مقنن در این قانون تنها به ادله‌ای چون امضای الکترونیک، داده‌پیام‌های عادی و داده‌پیام‌های مطمئن اشاره نموده، لیکن این امر نافی سایر ادله‌ی الکترونیک نیست و ماده 13 و 14 قانون تجارت الکترونیک[1] نیز صحت این مدعا را تأیید می‌کند. ازاین‌رو تفسیر صرف ادله‌ی الکترونیک به اسناد الکترونیک صحیح نیست و سند الکترونیک تنها یک بخش از اسناد الکترونیک به‌حساب می‌آید و دامنه‌ی اسناد الکترونیک اعم از سند معنی مصطلح و غیر آن است.

نکته قابل‌ذکر دیگر بحث تعارض دلایل سنتی با دلایل الکترونیکی است. همان‌طور که پیش‌تر اشاره شد، قانون‌گذار در مواد 6 و 7 قانون تجارت الکترونیک ارزش اثباتی امضای الکترونیکی و داده‌پیام عادی را معادل نوشته می‌داند. تعیین ارزش دلایل در حد اسناد عادی را بر اساس ماده 13 آن قانون به قاضی واگذار کرده است. در ماده 14 و 15 ارزش اثباتی داده‌پیام مطمئن را بیان کرده و آن را در حکم سند رسمی می‌داند؛ بنابراین با مشخص شدن ارزش این ادله، در حل تعارض دلایل سنتی با ادله‌ی الکترونیکی قاضی با تمسک به همان اصول و قواعد حاکم بر تعارض دلایل سنتی حل تعارض می‌کند؛ بنابراین اگر دلیل الکترونیکی مطمئن با اسناد سنتی در تعارض باشد؛ دلیل الکترونیکی که در حکم سند رسمی است مقدم می‌شود و اگر همین دلیل با اسناد رسمی معمولی در تعارض قرار گیرد، با توجه به اختیاری که قاضی در کشف حقیقت دارد، با عنایت به ماده 13 قانون تجارت الکترونیکی دراین‌باره تصمیم می‌گیرد (لینان دبلفون 1388: 94).

هرچند در قانون جدید مجازات اسلامی مصوب 1392 در مواد 161 و 162 به‌صراحت به رفع این تعارض اشاره‌شده و علم قاضی به سایر ادله رجحان دارد.

دلیل الکترونیک از مزایا و معایبی برخوردار است. ازجمله این مزایا می‌توان به موارد زیر اشاره کرد:

1- ماده 13: «به‌طورکلی ارزش اثباتی داده‌پیام‌ها با توجه به عوامل مطمئنه ازجمله تناسب روش‌های ایمنی به کار گرفته‌شده با موضوع و منظور مبادله‌ی داده‌پیام تعیین می‌شود»؛ ماده 14: «کلیه‌ی داده‌پیام‌هایی که به طریق مطمئن ایجاد و نگهداری شده‌اند، از حیث محتویات و امضای مندرج در آن، تعهدات طرفین یا طرفی که تعهد کرده و کلیه‌ی اشخاصی که قائم‌مقام قانونی آن‌ها محسوب می‌شوند، اجرای مفاد آن و سایر آثار در حکم اسناد معتبر و قابل استناد در مراجع قضایی و حقوقی است».

1- قابلیت کپی‌برداری؛ 2- سهولت تغییر و اصلاح در نسخه‌ی کپی و نگهداری نسخه‌ی اصل؛ 3- صعوبت حذف؛ 4- قابلیت ذخیره‌سازی در مکان‌های مختلف سیستم رایانه‌ای بدون آگاهی واردکننده (رضایی 1387: 6). از جهات ضعف نیز می‌توان به این موارد اشاره نمود:

1- دشواری شناخت پدیدآورنده یا صادرکننده؛ 2- عدم اطلاع از تغییر در داده به دلیل فقدان ابزار خاص و پیشرفته؛ 3- قابلیت بالای حذف داده با نصب یک برنامه نه‌چندان پیشرفته؛ 4- تأثیر نقص سیستم بر خروجی داده؛ 5- تأثیر ابزارهای پردازشی بر روی اصل داده؛ 6- سهولت دسترسی افراد غیرمجاز به داده؛ 7-کثرت و فراوانی داده به دلیل ذخیره شدن در برخی بخش‌های کامپیوتر اعم از کامپیوتر شخصی (pc)، اداری یا منزل، سرور فایل‌های شبکه یا سیستم‌های بزرگ، پست الکترونیک، نسخه‌های پشتیبان، ماشین‌های فاکس یا سرورهای فاکس و... 8- کدگذاری داده جهت تخریب (جلالی فراهانی 1386: 88).

ب. استنادپذیری ادله‌ی الکترونیک

استنادپذیری ادله‌ی الکترونیک عبارت از واجد اعتبار بودن داده‌های الکترونیکی در محضر دادگاه و ایفای نقش در صدور رأی مقتضی است. برای این‌که دلیل الکترونیک قابل استناد باشد باید واجد چند شرط باشد: **نخست** قابلیت ارائه؛ در محیط‌های رایانه‌ای ضبط اسناد باید به‌گونه‌ای باشد که در موارد لزوم، امکان ارائه و بازتولید آن میسر و قانون اعتبار آن را به رسمیت شناخته باشد، در غیر این صورت در موقع اختلاف، قابلیت ارائه به دادگاه یا مراجع حل اختلاف را نخواهد داشت؛ **دوم** اصالت؛ اطلاعات رایانه‌ای به سهولت قابل‌تغییرند و کپی‌برداری از آن‌ها به سهولت صورت می‌گیرد؛ ازاین‌رو امکان تشخیص اصل از کپی به‌آسانی امکان‌پذیر نیست؛ **سوم** قابلیت ایجاد علم عادی؛ علم به معنی آگاهی انسان نسبت به ماهیت وقایع و پدیده‌های اطراف است، حالتی است که درنتیجه‌ی سنجش قراین، شواهد و اوضاع‌واحوال حاکم بر پدیده‌های خارجی به‌دست‌آمده و با حصول آن امکان هرگونه مخالفت از بین می‌رود.[1]

1- لازم به ذکر است که این سه شرط تنها از دیدگاه حقوق‌دانان مطرح‌شده و در قوانین مرتبط فقط به شروط 1 و 2 اشاره‌شده است.

در مباحث قضایی دو نوع علم به ذهن متبادر می‌شود: **نخست** علمی که قواعد و ضوابط را بیان کرده و به بحث از تکالیف و وظایف اشخاص می‌پردازد؛ **دوم** علم قاضی نسبت به موضوع مورد نزاع و واقعیت مورد مناقشه که این علم درنتیجه‌ی تجربیات و مطالعه‌ی علوم یا از طریق مطالعه‌ی پرونده و توضیحات طرفین و ارائه‌ی ادله برای قاضی حاصل می‌شود. در فرایند دادرسی این نوع از علم مدنظر است و به آن علم عادی اطلاق می‌شود. در علم اصول، مراد از علم، علم قطعی است یعنی قطع جزمی که در آن احتمال خلاف و خطا داده نمی شود، اما در فرایند دادرسی رسیدن به این علم که هیچ مجهولی در آن باقی نماند، مدنظر نیست، بلکه مراد از علم، علم متعارف است که وسیله‌ی حل‌وفصل دعاوی و مرافعات قرار می‌گیرد. پذیرش این ادله از سوی قانون‌گذار می‌تواند عاملی برای استنادپذیری آن‌ها در فرایند کیفری باشد. امکان احراز این سه معیار در خصوص اسناد و ادله‌ی فیزیکی چندان دشوار نیست، اما در مورد ادله‌ی الکترونیکی با توجه به گمنامی اشخاص در فضای سایبر این امر به‌راحتی میسر نمی‌شود. لذا اگر احراز هویت پدیدآورنده را یکی از ارکان استنادپذیری اسناد و ادله قلمداد کنیم؛ باید گفت چنین ضابطه‌ای در خصوص اسناد الکترونیکی و دارای منشأ شبکه‌ای قابل‌اثبات نیست یا دشوار است. به لحاظ شیوع و به‌کارگیری انواع ارتباطات الکترونیکی ضرورت اقتضا می‌کند که استناد به این ادله را بر اساس موازینی در نظام حقوقی خود بپذیریم (باستانی 1386: 72). وضعیت ادله رایانه‌ای در هر کشور به اصول اساسی ادله در آن کشور بستگی دارد. در کشورهای دارای حقوق رومی و ژرمنی اصل بر آزادی تحصیل و ارزیابی ادله است. ازاین‌رو پذیرش سوابق رایانه‌ای در این کشورها به‌آسانی صورت می‌گیرد؛ اما در نظام کامن لا رسیدگی‌ها شفاهی و تدافعی است و علم حاصل از منابع فرعی از قبیل اشخاص دیگر، کتاب‌ها یا سوابق پذیرفته نیست (زیبر 1383: 47). این کشورها در پذیرش سوابق رایانه‌ای به‌عنوان دلیل تردید دارند یا آن را با شرایط سخت موردپذیرش قرار می‌دهند (نوری 1383: 192). در نظام حقوقی ایران در ماده 1258 قانون مدنی و در فصل دهم قانون آیین دادرسی مدنی انواع ادله نام‌برده شده که عبارت‌اند از: اقرار، اسناد کتبی، شهادت، سوگند و اماره، معاینه محل، تحقیق محل و کارشناسی. تقریباً همه حقوقدانان بر این امر اتفاق‌نظر دارند که دلایل مذکور در این ماده جنبه‌ی حصری دارند و تنها امری به‌عنوان دلیل پذیرفته می‌شود که مشمول تعریف یکی از ادله ی اثبات دعوا مذکور در قانون باشد. با الهام از این دیدگاه

صاحب‌نظران دو رویکرد را مطرح ساخته‌اند: بر اساس *رویکرد اول* چون دلایل الکترونیکی در هیچ‌یک از قالب‌های مطروحه در قانون قرار نمی‌گیرند، لذا این نوع ادله را باید به‌عنوان نوع جدیدی از ادله تلقی نمود (عباسی کلیمانی 1385: 62)؛ اما در *رویکرد دوم* اعتقاد بر این است که چون نظام حقوقی ایران کارکردگرا است و نه شکل‌گرا می‌توان از روش معادل‌سازی استفاده کرد. این روش نخست اهداف و کارکردهای عناصر ادله‌ی سنتی را تعیین و سپس شیوه‌ی تأمین این کارکردها را در دلایل الکترونیک معرفی خواهد نمود. استفاده از این راهکار موجب می‌شود قانون ایران در بحث استنادپذیری ادله‌ی الکترونیکی از اصلاح قوانین بی‌نیاز شود (حسن بیگی 1384: 56). به نظر می‌رسد در نظام حقوقی ایران، در بحث استنادپذیری ادله‌ی کیفری بیشتر از شیوه‌ی اقناعی استفاده‌شده است. قانون نمونه‌ی آنسیترال نیز از همین روش پیروی کرده است.

«در نظام تقنینی، در ماده 50 قانون جرایم رایانه‌ای، قانون‌گذار برای مستند شناختن داده‌های رایانه‌ای دو شرط را در نظر داشته است:

نخست- داده‌های رایانه‌ای توسط طرف دعوا یا شخص ثالثی که از دعوا آگاهی نداشته، ایجاد یا پردازش یا ذخیره یا منتقل‌شده باشد.

دوم- به صحت، تمامیت، اعتبار و انکارناپذیری داده‌ها خدشه‌ای وارد نشده باشد».

با لحاظ دو شرط مذکور در ماده به نظر می‌رسد در شرط نخست نوعی تعارض وجود داشته و قانون‌گذار طرف دعوا را همسان با شخص ثالث به‌عنوان فردی بی‌طرف و نه ذی‌نفع، متصدی ایجاد، پردازش، ذخیره یا انتقال داده‌ها در نظر گرفته است. درحالی‌که شاید شخص طرف دعوا در تولید داده‌ها هیچ قصد مغرضانه‌ای نداشته است؛ اما این شبهه در ذهن ایجاد می‌شود که قیاس این شخص با شخص ثالثی که از دعوا آگاهی نداشته، چندان مطلوب نیست و به‌نوعی نقض شرط دوم محسوب می‌شود.

مراد از داده‌ی رایانه‌ای در ماده 50 قانون جرایم رایانه‌ای همان موارد مذکور در ماده 32 این قانون است که عبارت‌اند از: داده‌ی ترافیک، اطلاعات کاربر و داده محتوا[1]. در ماده 35 قانون جرایم رایانه‌ای آمده: «مقام قضایی می‌تواند دستور ارائه‌ی داده‌های حفاظت‌شده‌ی مذکور در مواد 22، 33 و 34 فوق را به اشخاص یادشده بدهد تا در اختیار

1- باوجوداینکه در تبصره 1 و 2 ماده 32 ذکری از داده محتوا به میان نیامده است، درصورتی‌که عبارت محتوای ذخیره‌شده مذکور در ماده 33، همان داده محتوا تلقی شود، این تقسیم‌بندی ناظر بر هر سه قسم است.

ضابطین قرار گیرد. مستنکف از اجرای این دستور به مجازات مقرر در ماده 34 محکوم خواهد شد». با عنایت به اینکه مواد یادشده در ذیل فصل نگهداری داده‌ها و ارائه‌ی داده‌ها آمده‌اند، به نظر می‌رسد هر سه داده‌ی «ترافیک، کاربر و محتوا» صرف‌نظر از محتوا قابلیت ارائه به مراجع قضایی را دارند و باید به شکلی صحیح و به‌گونه‌ای که به اصالت، تمامیت و انکارناپذیری آن‌ها خللی وارد نشود، نگهداری شوند. دلیل این مدعا پیروی نظام ادله‌ی ایران از سیستم ادله‌ی تلفیقی است که در این سیستم هر دلیلی صرف‌نظر از محتوای آن درصورتی‌که موجب قناعت وجدانی قاضی و علم وی گردد، دارای ارزش اثباتی است که این امر به‌صراحت در ماده 161 و 162 قانون مجازات اسلامی مصوب 1392 تأیید شده است. در تأیید این مدعا در آیین‌نامه‌ی استنادپذیری ادله‌ی الکترونیک مصوب 1393 در مواد 7، 16، 18 و 35 به این امر صحه گذاشته است.

پ. شرایط قابلیت استناد ادله‌ی الکترونیک

در ماده 51 قانون جرایم رایانه‌ای مقررشده: «کلیه‌ی مقررات مندرج در فصل‌های دوم و سوم این بخش علاوه بر جرایم رایانه‌ای شامل سایر جرایمی که ادله‌ی الکترونیک در آن‌ها مورد استناد قرار می‌گیرند نیز می‌شود». همچنین در تبصره‌ی ماده 52 آمده: «در مواردی که در بخش دوم این قانون برای رسیدگی به جرایم رایانه‌ای مقررات خاصی از جهت آیین دادرسی پیش‌بینی‌نشده است، طبق مقررات قانون آیین دادرسی کیفری اقدام خواهد شد». با توجه به این دو ماده به نظر می‌رسد کلیه‌ی داده‌های مذکور در فوق در دعاوی سنتی نیز به کار می‌رود و این ادله تنها منحصر به رسیدگی به دعاوی سایبری نیست. از سوی دیگر دعاوی سایبری برای اثباتشان بی‌نیاز به ادله‌ی سنتی نیستند و در بسیاری از موارد درجایی که قانون جرایم رایانه‌ای با خلأ مواجه است باید به قانون آیین دادرسی کیفری مراجعه و استناد نمود.

در بند «ح» ماده 2 قانون تجارت الکترونیک، قانون‌گذار خصایصی جهت مطمئن بودن یک سیستم اطلاعاتی[1] برشمرده که عبارت‌اند از: «1- به نحو معقولی در برابر سوءاستفاده و نفوذ محفوظ باشد؛ 2- سطح معقولی از قابلیت دسترسی و تصدی صحیح را دارا باشد؛ 3- به نحوی معقول متناسب بااهمیت کاری که انجام می‌دهد پیکربندی و سازمان‌دهی شده

1- Secure Information دستگاه

باشد؛ 4- موافق با رویه‌ی ایمن باشد». در ماده 10 این قانون نیز قانون‌گذار در بحث شرایط امضای الکترونیکی مطمئن شرایطی ذکر کرده که عبارت‌اند از: «الف- نسبت به امضاکننده منحصربه‌فرد باشد؛ ب- هویت امضاکننده‌ی «داده‌پیام» را معلوم نماید؛ ج- به‌وسیله‌ی امضاکننده یا تحت اراده‌ی انحصاری وی صادرشده باشد؛ د- به نحوی به یک «داده‌پیام» متصل شود که هر تغییری در آن «داده‌پیام» قابل‌تشخیص و کشف باشد». در ماده 13 این قانون مقررشده: «به‌طورکلی ارزش اثباتی داده‌پیام‌ها با توجه به عوامل مطمئنه ازجمله تناسب روش‌های ایمنی به کار گرفته‌شده با موضوع و منظور مبادله‌ی «داده‌پیام» تعیین می‌شود».

با تدقیق در این سه مقرره به نظر می‌رسد قانون‌گذار دو شرط اصلی استناد به اسناد را در مورد ادله‌ی الکترونیک که عبارت‌اند از قابلیت انتساب و حفظ صحت، تمامیت و انکارناپذیری داده‌ها را مدنظر داشته و در موارد مختلف این قانون به آن اشاره‌شده است. هرچند در قانون مذکور از ادله‌ای چون امضای الکترونیکی داده‌پیام‌های مطمئن و داده‌پیام‌های عادی به‌صراحت سخن به میان آمده است، این تصریح نافی ارزش اثباتی سایر داده‌ها نیست و قانون‌گذار در ماده 14[1] بر این مدعا مهر تأیید گزارده است.

قانون‌گذار در ماده 6 و 7 داده‌پیام و امضای الکترونیکی را معادل نوشته و امضای سنتی محسوب کرده و ماده 12 این قانون بر اصل لزوم پذیرش اسناد الکترونیکی تصریح کرده است: «اسناد و ادله اثبات دعوا ممکن است به‌صورت داده‌پیام بوده و در هیچ محکمه یا اداره دولتی نمی‌توان ارزش اثبات داده‌پیام را صرفاً به خاطر شکل و قالب رد کرد». در مواد 14 و 15 به ارزش اثباتی ادله‌ی مطمئن پرداخته است (شیرزاد 1388: 25). برای پذیرش این دلایل در دادگاه، نخست باید دلیل ارائه‌شده در یکی از قالب‌های ادله‌ی سنتی مذکور در قانون قرار گیرد تا از ارزش اثباتی آن نوع دلیل برخوردار شود. تنها قالبی که ادله‌ی الکترونیکی می‌توانند در آن جای‌گیرند *نوشته* است. این امر ناشی از ویژگی داده‌پیام است؛ زیرا تمام دلایل الکترونیکی به‌صورت داده‌پیام هستند. تمام اطلاعات ثبت‌شده توسط

1- ماده 14 قانون تجارت الکترونیک: «کلیه‌ی «داده‌پیام»هایی که به طریق مطمئن ایجاد و نگهداری شده‌اند از حیث محتویات و امضای مندرج در آن، تعهدات طرفین یا طرفی که تعهد کرده و کلیه‌ی اشخاصی که قائم‌مقام قانونی آنان محسوب می‌شوند، اجرای مفاد آن و سایر آثار در حکم اسناد معتبر و قابل استناد در مراجع قضایی و حقوقی است».

ابزارهای الکترونیکی شفاهی یا کتبی، داده‌پیام هستند. ازنظر قانونی همان‌طور که در بالا اشاره نمودیم داده‌پیام ازنظر قانونی جایگزین نوشته است و قانون هر نوشته‌ای که برای اثبات دعوا مورد استناد قرار گیرد را سند می‌داند؛ بنابراین در نظام سنتی اثبات دعوا دلیل الکترونیکی از اعتبار سند برخوردار است (استنلی 1391: 40). اسناد الکترونیکی که دارای شرایط مطمئن نیستند از ارزش اثباتی اسناد عادی برخوردارند؛ حتی اگر فناوری مورداستفاده در آن‌ها غیر ایمن باشد و تا زمانی که اصالت آن اسناد تکذیب نشده یا طرف دعوا به اصالت آن‌ها اعتراض نکرده حمل بر صحت سند است و دادرس نمی‌تواند به علت ایمن نبودن فناوری مورداستفاده و یا امضا آن را معتبر نداند. سند الکترونیکی مانند سند عادی قابل‌انکار و تردید است و کلیه‌ی کارکردهای سند عادی را نیز دارد؛ بنابراین از جمع مواد برمی‌آید که دلیل الکترونیکی از ارزش اثباتی همان قالب نظام ادله‌ی سنتی برخوردار است و چون معادل قالب نوشته در نظام سنتی است از کارکردهای سند بهره‌منداست (نوری 1382: 54)؛ یعنی از شیوه‌های خاص جمع‌آوری و نگهداری دلایل ارتکاب جرم جهت حفظ ارزش اثباتی آن‌ها و به‌بیان‌دیگر چگونگی جمع‌آوری قانونی دلایل و نگهداری آن‌ها جهت بهره‌برداری قضایی به همان صورت اولیه که کشف‌شده‌اند، استفاده نمود (زندی 1389: 49).

مستندسازی ادله بدین‌جهت صورت می‌گیرد که نشان داده شود دلایل به‌دست‌آمده در موقعیت ذاتی و اصلی خود قرار دارند و از اطمینان کافی برخوردارند و هیچ تغییر و تحریفی در آن‌ها صورت نگرفته است. به‌عنوان‌مثال تصویر به‌دست‌آمده از چتروم را می‌توان در جهت تصدیق مکالمه‌ی الکترونیکی صورت پذیرفته مورداستفاده قرار داده تا نشان داد که هیچ‌گونه تغییری در آن ایجاد نشده است.

برای محقق شدن این دو شرطِ استناد به ادله‌ی الکترونیک که هم در قانون جرایم رایانه‌ای و هم در قانون تجارت الکترونیک به آن اشاره‌شده نیازمند پیش‌شرط‌هایی است که قانون‌گذار ایران از این پیش‌شرط‌ها غافل نبوده و در مواد مختلفی چه به‌طور صریح و چه به‌طور ضمنی به آن پرداخته است. ازجمله‌ی این مواد می‌توان به ماده 40 قانون جرایم رایانه‌ای اشاره نمود: «در توقیف داده‌ها با رعایت تناسب، نوع، اهمیت و نقش آن‌ها در ارتکاب جرم به روش‌هایی از قبیل چاپ داده‌ها، کپی‌برداری یا تصویربرداری از تمام یا بخشی از داده‌ها، غیرقابل‌دسترس کردن داده‌ها با روش‌هایی از قبیل تغییر گذرواژه یا

رمزنگاری و ضبط حامل‌های داده عمل می‌شود». واژه‌ی «از قبیل» بیانگر این است که این راهکارها حصری نیستند و راهکارهایی چون ته‌نقش نگاری دیجیتال و بیومتریک و... را نیز می‌توان از زمره‌ی این موارد شمرد.

در ماده 49 قانون مذکور نیز آمده: «به‌منظور حفظ صحت و تمامیت، اعتبار و انکارناپذیری ادله‌ی الکترونیک جمع‌آوری‌شده، لازم است مطابق آیین‌نامه‌ی مربوط از آن‌ها نگهداری و مراقبت به عمل آید». مطابق بند «ه» ماده 1 آیین‌نامه‌ی استنادپذیری ادله‌ی الکترونیک مصوب 1393 باید از داده‌ها، زنجیره‌ی حفاظتی ایمن به‌نحوی‌که امکان ردیابی آن‌ها از مبدأ تا مقصد را فراهم سازد، در نظر گرفت. ماده 15 این آیین‌نامه در حفاظت از داده‌ها خطاب به مسئول حفاظت این‌گونه آمده: «دستور حفاظت باید فوری و با روش مطمئن به مجری حفاظت ابلاغ شود». در تبصره‌ی همین ماده نیز آمده: «روش مطمئن روشی است که با توجه به نوع داده و طول مدت‌زمان حفاظت، امکان بهره‌برداری از داده‌های حفاظت‌شده را در مراحل بعدی دادرسی ممکن می‌سازد». در ماده 38 این آیین‌نامه آمده: «توقیف با رعایت تناسب نوع اهمیت و نقش داده یا سامانه‌های رایانه‌ای یا مخابراتی به روش‌های زیر انجام می‌شود: الف- توقیف داده‌ها از طریق چاپ داده‌ها، غیرقابل‌دسترس کردن داده‌ها به روش‌هایی از قبیل تغییر گذرواژه یا رمزنگاری و ضبط حامل‌های داده؛ ب- توقیف سامانه‌های رایانه‌ای یا مخابراتی از طریق تغییر گذرواژه، پلمپ سامانه در محل استقرار یا ضبط سامانه».

با ملاحظه در این موارد به‌صراحت هم در قانون جرایم رایانه‌ای و هم در آیین‌نامه‌ی مربوط به آن به راهبردهای امنیتی جهت حفظ تمامیت و اصالت ادله‌ی الکترونیکی اشاره‌شده و این امر نشانگر اهمیت این موضوع از نگاه مقنن است؛ بااین‌وجود در رویه‌ی عملی جهت ایمن‌سازی اطلاعات تاکنون اقدامی صورت نگرفته است.

در بند «ت» ماده 2 قانون تجارت الکترونیک آمده: «رویه‌ی ایمن[1] رویه‌ای است برای تطبیق صحت ثبت داده‌پیام منشأ و مقصد آن با تعیین تاریخ و برای یافتن هرگونه خطا یا تغییر در مبادله، محتوا یا ذخیره‌سازی داده‌پیام از یک‌زمان خاص. یک‌رویه‌ی ایمن ممکن است با استفاده از الگوریتم‌ها یا کدها، کلمات یا ارقام شناسایی، رمزنگاری، روش‌های

1- Secure Methode

تصدیق هویت یا پاسخ برگشت یا طرق ایمنی مشابه انجام شود». در این بند از ماده نیز قانون‌گذار به شیوه‌هایی جهت ایمنی سازی ادله‌ی الکترونیک پرداخته است و سرانجام در مواد 652 و 656 قانون آیین دادرسی کیفری مصوب 1392 (اصلاحی 1394) نیز استفاده از تمهیدات امنیتی مطمئن به‌عنوان راهبردی جهت فراهم‌سازی دو شرط استناد به ادله‌ی الکترونیک که عبارت‌اند از صحت انتساب و حفظ انکارناپذیری و اصالت پرداخته است. در ماده 656 این قانون آمده: «به‌منظور حفظ صحت و تمامیت، اعتبار و انکارناپذیری اطلاعات مبادله شده میان شهروندان و محاکم قضایی، قوه قضائیه موظف است تمهیدات امنیتی مطمئن برای امضای الکترونیک و احراز هویت و احراز اصالت را فراهم کند».

با توجه به همه‌ی موارد گفته‌شده و اشاره‌ی مکرر قانون‌گذار به نظر می‌رسد بحث حفاظت از صحت و اصالت داده‌ها جهت ارائه به محاکم قضایی از بحث‌های ضروری است که به همین منظور در ادامه به دو راهکار مهم بیومتریک و رمزنگاری پرداخته می‌شود.

1- بیومتریک

الف. تعریف و ویژگی‌های بیومتریک

فناوری بیومتریک ازجمله فناوری‌های نوظهور در عرصه‌ی فناوری اطلاعات است و شاه‌کلید ورود به دنیای اطلاعات و کنترل ارتباطات تلقی می‌شود. توسعه‌ی کاربرد این فناوری در عرصه‌های گوناگون باعث شده مواجهه‌ی صحیح با آن مستلزم اتخاذ رویکردی جامع و همه‌جانبه‌نگر باشد. این واژه از زبان یونانی نشأت‌گرفته و از دو بخش «به یو» به معنی زندگی و «متریک» به معنی اندازه‌گیری تشکیل‌شده است. بیومتریک در اصطلاح «به هر خصوصیت فیزیولوژیکی یا رفتاری منحصربه‌فرد، متمایزکننده، مقاوم و قابل‌سنجش که بتواند برای تعیین یا تأیید خودکار هویت افراد و تأمین هرچه بیشتر امنیت اطلاعات به کار رود، اطلاق می‌شود» (Close Angeline 2003: 12). این فناوری داده‌هایی از اشخاص را به‌طور خودکار با توجه به الگوی عمومی دریافت کرده و در صورت نیاز آن را پردازش و تحلیل می‌کند تا بتواند در جامعه‌ی آماری بزرگ‌تر، افراد را از یکدیگر متمایز کند و از سرقت اطلاعات یا جعل اطلاعات یا دسترسی غیرمجاز به داده‌ها و اطلاعات اشخاص ممانعت و ازاین‌رو از امنیت افراد حمایت کند.

ویژگی‌های بیومتریک به‌طور عمده به دودسته تقسیم می‌شوند: 1) خصوصیات فیزیولوژیکی که به ساختار و شکل بدن مربوط می‌شود: شناسایی از طریق اثرانگشت، نقشه‌ی کف دست، نقشه‌ی رگ‌های دست، صوت، عنبیه نگاری، شبکیه نگاری، چهره‌نگاری، شکل گوش، بوی بدن، ساختار ناخن، صوت و هندسه‌ی دست نمونه‌ای از این شیوه‌اند. 2) خصوصیات رفتاری: همان‌طور که از اسمش هویداست برخی رفتارهای انسان را مورد واکاوی قرار می‌دهد؛ امضا، چگونگی راه رفتن، تشخیص لبخند و نحوه‌ی تایپ نمونه‌ای از این شیوه‌اند (هاتف 1387: 17).

سیستم بیومتریک عبارت است از «نرم‌افزار یا سخت‌افزار کامپیوتری که برای شناسایی یا بررسی یک فرد به‌کاربرده می‌شود». علم بیومتریک هم‌زمان با تحولات جهانی در عرصه‌ی امنیت اطلاعات و فضای جدیدی که اینترنت فرا روی مراکز ارائه‌دهنده‌ی خدمات گذارده، ضرورت حمایت از امنیت را دوچندان نموده است (احسانی مؤید 1389: 8). امروزه کارت‌های شناسایی، تراکنش‌های مالی و اعتباری، تأیید هویت مشتریان و دسترسی به حساب‌ها، دسترسی به رایانه‌های شخصی یا شبکه، تراکنش‌های از راه دور مثل تجارت الکترونیک، شناسایی ملی، مدیریت بحران‌های بزرگ شهری، رأی‌گیری، گواهی‌نامه‌های رانندگی، شناسایی مجرمان، دسترسی فیزیکی زمانی و کنترل حضوروغیاب، شناسایی شهروندان، توزیع امکانات عمومی و مهم‌تر از همه حفاظت از داده و سیستم‌های رایانه‌ای تنها بخشی از کارکردهایی است که بیومتریک ارائه نموده است (Chawki 2005: 28-29). آنچه در ادامه تبیین می‌شود، مهم‌ترین کاربرد بیومتریک، ایمن‌سازی سند الکترونیک است.

ب. کیفیت ایمن‌سازی سند الکترونیک از طریق بیومتریک

مشخصه‌های ایدئال بیومتریک - همانند ثبات، تمایز، در دسترس بودن، قابلیت دستیابی و قابلیت پذیرش - تا حد زیادی قادر است تمامیت و انتساب اسناد را در قیاس با فناوری دانشی و سایر فناوری‌های سنتی به گونه‌ی بهتری تضمین کند. این سامانه قادر است ویژگی‌های یک فرد را بدون تماس مستمر کارمند با سیستم ارزیابی و اندازه‌گیری کند و نتایج قابل قبولی در جهت تأمین امنیت اطلاعات ارائه دهد؛ همچنین با پاسبانی از اطلاعات هویت افراد یکپارچگی امنیت را تضمین می‌کند و به‌عنوان مهم‌ترین فاکتور برای حمایت

از این حوزه به شمار می‌آید. برای مثال اگر فردی کارت هوشمند خود را گم کند و یک بیگانه آن را پیدا کند سابقه‌ی اعتباری این فرد به خطر می‌افتد؛ اما اگر کارت هوشمند را بتوان صرفاً زمانی استفاده کرد که کاربر توسط ویژگی بیومتریک خود شناسایی شود کاربر در برابر این تهدید محافظت می‌شود.

این سامانه دسترسی افراد غیرمجاز به اطلاعات اشخاص را محدود می‌کند؛ برای مثال سامانه‌ی بیومتریکِ اطلاعات کاربران می‌تواند به‌طور قابل‌اطمینانی تضمین کند که اطلاعات کاربران صرفاً در اختیار افراد مجاز قرار می‌گیرد. برای این کار بیومتریک در سه مرحله دست به اقدام می‌زند: «جمع‌آوری، استخراج، مقایسه». در *گام اول* یک سیستم باید بیومتریکی که قرار است مورداستفاده قرار دهد جمع‌آوری کند. یکی از تفاوت‌های اساسی موجود در این گام، خصوصیتی است که مورد تحلیل قرار می‌گیرد. بدیهی است این خصوصیت بر کسب بیومتریک اثر می‌گذارد. تمامی سیستم‌های بیومتریک دارای نوعی مکانیسم جمع‌آوری هستند. این مکانیسم می‌تواند دارای یک حس‌گر یا خواننده باشد که فرد دست یا انگشت خود را روی آن می‌گذارد؛ یک دوربین باشد که تصویری از صورت یا چشم می‌گیرد یا نرم‌افزاری که ریتم و سرعت تایپ کردن را ثبت می‌کند. بسته به اهداف سیستم، ثبت‌نام می‌تواند دارای مجموعه‌ای از سایر اطلاعات قابل‌شناسایی افراد نیز باشد.

در *گام دوم* دستگاه‌های بیومتریکی که به‌صورت تجاری در دسترس هستند تصویر کامل بیومتریک‌ها را به روشی که نهادهای مجری قانون اقدام به جمع‌آوری اثرانگشت با جوهر می‌کنند، ثبت نمی‌کنند؛ در عوض شاخصه‌های معینی از بیومتریک استخراج می‌شود و به‌این‌ترتیب فقط صفات معینی، جمع‌آوری می‌شوند. مثل اندازه‌های معینی از اثرانگشت یا نقاط فشار روی یک امضا (Levy 2005: 49-51). این‌که کدام قسمت‌ها مورداستفاده قرار می‌گیرند بستگی به نوع بیومتریک و نیز طراحی هر سیستم منحصربه‌فرد دارد. این اطلاعات استخراج‌شده که گاهی داده‌های خام نیز نامیده می‌شوند، تبدیل به کد ریاضیاتی می‌شوند. این‌که این کار دقیقاً چطور صورت می‌گیرد، در سیستم‌های انحصاری متفاوت فرق می‌کند و کد مذکور به‌صورت یک نمونه ذخیره می‌شود (پیکربندی خاص یک سیستم تعیین خواهد کرد که این اطلاعات کجا و چگونه ذخیره شوند). بدون توجه به

جزئیات می‌توان گفت تمام سیستم‌های بیومتریک باید نمونه‌ای از بیومتریک را ایجاد و نگهداری کنند تا هر فرد را بتوانند ارزیابی یا شناسایی کنند.

در گام سوم و برای مقایسه یک سیستم بیومتریک شاخصه‌های معینی از ویژگی‌های بیومتریک یک فرد را سنجیده و هر بار که آن فرد بیومتریک زنده‌ی خود را عرضه می‌کند، ثبت می‌شوند. این اطلاعات استخراج‌شده با استفاده از همان روشی که نمونه را ایجاد کرد تبدیل به کد می‌شوند. کد جدید ایجادشده از روی اسکن زنده در صورت ضرورت انجام تطبیق یکی با همه، با یک بانک اطلاعات مرکزی از این نمونه‌ها و در صورت تطبیق یکی با یکی، با یک نمونه‌ی واحد ذخیره‌شده مقایسه می‌شود. اگر این مقایسه و تطبیق در محدوده‌ی طیف معینی از ارقام آماری درست عمل نماید، در سیستم معتبر تلقی می‌شود (Kerr 2005: 52-53). برای نمونه هر بار که یک دستگاه بیومتریک اثرانگشت، چهره، امضا یا صدای یک شخص را می‌خواند، داده‌هایی که تولید می‌کند کمی متفاوت است. اگر نرم‌افزار تشخیص نتواند پاسخگوی این نوسان باشد، هیچ‌وقت به فرد اجازه‌ی ورود نخواهد داد. در این مسیر بیومتریک یک لایه‌ی حفاظتی ایجاد می‌کند که با کلمات رمز استاندارد ترکیب می‌شود و تنها به فردی که صاحب اطلاعات بیومتریکال است، اجازه‌ی ورود می‌دهد.

به‌این‌ترتیب بیومتریک تأمین‌کننده‌ی سه ضرورت اساسی برای ورود به دنیای سایبر است: 1- شناسایی هویت 2- تأیید هویت 3- امنیت هویت (ساجدی 1386: 5). نسبت دادن شناسه به یک فرد خاص شناسایی هویت اطلاق می‌شود در این فرایند سؤالی که مطرح می‌شود این است که «او چه کسی است». سیستم بیومتریک به آسانی هویت فرد را افشا می‌کند و به این سؤال پاسخ مثبت می‌دهد. به صحه گذاردن و تأیید هویت ادعا شده از سوی فرد توسط دیگران، «تصدیق هویت» تعبیر می‌شود. به حفاظت از سیستم‌های اطلاعاتی در مقابل تلاش‌های افراد غیرمجاز برای دستیابی به اطلاعات یا دست‌کاری اطلاعات، «امنیت اطلاعات» اطلاق می‌شود (Mason 2006: 24).

یک زنجیره‌ی بیومتریک می‌تواند به سهولت قابلیت مستندسازی دوباره‌ی اسناد را نیز تحقق بخشد و فرد را قادر سازد در مرحله‌ی محتوا، انتقال و منبع، صحت اسناد را به آسانی اثبات کند (حسن‌آبادی 1386: 17). اعتبارسنجی محتوا بدین معنا است که آیا مدرک قبل از انتقال به موجودیت دیگر در موجودیت قبلی‌اش به‌صورت نامناسب تغییر کرده یا نه؟

اعتبارسنجی انتقال به این مسئله می‌پردازد که آیا در حین انتقال از یک موجودیت، موجودیت بعدی به‌طور نامناسب تغییر کرده یا نه؟ اعتبارسنجی منبع تضمین می‌کند که آیا داده‌ها از منشأ مورد ادعا نشأت‌گرفته‌اند یا نه؟ برای تحقق این سه سطح بیومتریک از مکانیسم‌های امنیت‌مدار درون چارچوب استفاده می‌کند. ازجمله این مکانیسم‌ها می‌توان به «رمزنگاری، نقش‌نگاری، انگشت‌نگاری دیجیتالی و دینامیک‌های کلید فشاری» اشاره نمود. رمزنگاری به‌منظور از بین بردن خطر ره‌گیری داده‌ها، استراق سمع، تغییر داده‌ها، جعل داده‌ها و تکذیب منشأ و خاستگاه داده‌ها مورداستفاده قرار می‌گیرد (احمدی 1388: 9). نقش نگاری به‌منظور افزودن لایه‌ی دیگری از حفاظت در برابر ره‌گیری و استراق سمع داده‌ها، تغییر داده‌ها، جعل داده‌ها، تکذیب منشأ و خاستگاه داده‌ها و مهم‌تر از همه سرقت اطلاعات استفاده می‌شود. انگشت‌نگاری دیجیتالی جهت جلوگیری از تغییر و جعل داده‌ها مورداستفاده قرار می‌گیرد و درنهایت دینامیک‌های کلید فشاری به‌منظور جلوگیری از دسترسی غیرمجاز به داده‌ها و سرقت اطلاعات به کار می‌رود.

پ. مزایا و معایب کاربرد بیومتریک

با این توضیح، بیومتریک دارای مزایا و معایبی است. ازجمله این مزایا (حسن‌آبادی 1386: 43) می‌توان به موارد زیر اشاره کرد:

1- افزایش ایمنی: کدها و رمزهای عبور به‌سادگی حدس زده می‌شوند یا قابل شکستن هستند. ابزارهای همراه مانند کلیدها، نشان‌ها و کارت‌ها قابل سرقت هستند. بسیاری از کاربران، اعداد یا کلمات واضح را به‌عنوان رمز عبور انتخاب می‌کنند. به‌خصوص زمانی که تعداد رمزهای مورداستفاده زیاد باشد. به دلیل دشواری به خاطر سپاری کلمات یا اعداد، ساده انتخاب می‌شوند یا درجایی نوشته می‌شوند. در مقابل بیومتریک‌ها قابل سرقت یا فراموشی نیستند و به نگهداری خاصی نیاز ندارند؛

2- افزایش راحتی: دلایلی که بالا ذکر شد؛ خود گواهی بر سهولت استفاده از بیومتریک به‌جای ابزار رایج فعلی است. با استفاده از تکنولوژی‌های بیومتریکی سرعت دستیابی به منابع موردنظر افزایش می‌یابد. هزینه‌ی نگهداری از دستگاه‌ها و مسائل امنیتی مربوط کاهش چشم‌گیری می‌یابد و باعث صرفه‌جویی در اقتصاد می‌شود؛

3- کاهش شدید امکان تقلب و دسترسی غیرمجاز: در موارد استفاده از منافع عمومی، ورود به مراکز امنیتی، کاربردهای روزانه، انجام امور مالی و ... بیومتریک‌ها مانع تقلب افراد سودجو می‌شوند.

4- تشخیص افراد مظنون: با استفاده از بیومتریک‌ها هویت واقعی افراد آشکار می‌شود. با استفاده از این فنّاوری از بسیاری از مهاجرت‌های غیرقانونی، فرار از قانون و اعمال تروریستی جلوگیری می‌شود.

ازجمله معایب آن این است که گروه‌های فعال حامی آزادی‌های اجتماعی وجود این سیستم را نافی آزادی انسان می‌دانند و معتقدند این فنّاوری در کشورهای مورداستفاده نتوانسته مانع رخنه‌گری به اطلاعات و حریم خصوصی افراد شود. گذشته از این امر هر یک از سیستم‌های بیومتریک از ثبت اطلاعات برخی افراد به علل مختلف (ازجمله جراحت یا معلولیت یا به علت حساسیت به شرایط محیطی) عاجزند (هاتف 1386: 75) و برخی خطرات استراتژیک مربوط به بیومتریک را موارد زیر تلقی می‌کنند (Gaur 2015: 18):

- آسیب جسمی به فردی که این فنّاوری می‌تواند وارد سازد، باید در نظر گرفته شود. نگرانی‌هایی مربوط به آسیب‌های واقعی می‌تواند آسیب جسمی به فرد از سنسور را نیز شامل شود؛ برای مثال لیزری که در معاینه‌ی شبکیه‌ای استفاده می‌شود به همان اندازه‌ی ترسی است که شخصی فریبکار بخواهد عضوی از بدن مثل انگشت را قطع کند، به‌منظور کنار گذاشتن سیستم بیومتریک.
- نگرانی دیگر که با لحاظ کار در صنعت شناسایی عنبیه مطرح می‌شود، آن است که آیا عفونت‌های چشم مثل ورم ملتحمه از طریق دوربین قابل‌انتقال هستند یا خیر. استفاده‌کنندگان از اسکنرهای بیومتریک لمسی اغلب از انتقال بیماری و باکتری در خلال استفاده از اسکنرها در هراسند.
- کشورهای مختلف فرهنگ‌ها و عقاید مذهبی متفاوتی دارند که تجارت و رسوم اجتماعی را کنترل می‌کند و مردم در پذیرش رسومی که با فرهنگ و دستورهای مذهبی‌شان در تعارض باشد، مخالفت می‌کنند.

2- رمزنگاری

الف. تعریف و ویژگی‌های رمزنگاری

یکی از ابزارهای دفاعی در مقابل بسیاری از حملات و جرایم کامپیوتری، استفاده از مکانیک‌های رمزنگاری است. با رمزنگاری اطلاعات و فایل‌های باارزش می‌توان جرایمی از قبیل دسترسی غیرمجاز را بی‌اثر ساخت. اگرچه رمزنگاری به‌عنوان بهترین راه‌حل حفاظت از اطلاعات در برابر سرقت هویت شناخته‌شده است، اما به این برنامه در تجارت، به دلیل سابقه زیاد جاسوسی و روابط دیپلماتیک و نظامی، اهمیت بیشتری داده می‌شود. رمزنگاری قدمتی بسیار طولانی دارد و کشورها در طول تاریخ و خصوصاً در زمان جنگ‌ها برای محرمانه ماندن اطلاعات مهم از آن استفاده می‌کنند (Swire 2012: 425). ورود به دنیای ارتباطات رادیویی و ارسال امواج، مخابراتی و ماهواره‌ای و گسترده شدن و تحول آن‌ها - خصوصاً در قرن بیستم - و پس‌ازآن اختراع رایانه‌ها و ایجاد شبکه‌های رایانه‌ای و استفاده‌های مختلف از آن‌ها نظیر تجارت الکترونیک، سرمنشأ پیدایش علم نوینی به نام «فن‌آوری رمزنگاری» شده است. روش‌های رمزنگاری در طول زمان بسیار تغییر و تحول داشته‌اند. درواقع «این روش‌ها در حدود 4000 سال مورداستفاده قرارگرفته و شروع استفاده از آن‌ها با هیروگلیف‌های مکتوب مصر باستان بوده است» (ابوالحسن پور 1386: 40). از زمان این اقدام یونانی‌ها و رومی‌ها به بعد، دولت‌ها برای حفاظت از ارتباطات مهم نظامی و دیپلماتیک خود از رمزنگاری استفاده کرده‌اند و امروزه الگوریتم‌های ریاضی که به‌واسطه‌ی کامپیوتر به وجود آمده‌اند، رمزنگاری را به‌طور مجانی یا با هزینه بسیار کم برای اشخاص ممکن می‌سازد.

مفهوم ساده رمزنگاری عبارت است از «مبهم نمودن اطلاعات به طریقی که از دید فرد غیرمجاز پنهان شود و درعین‌حال فرد مجاز قادر به مشاهده و استفاده از اطلاعات باشد» (فضلی 1388: 30). فردی مجاز است که کلید مناسب برای رمزگشایی دارد. فن‌آوری رمزنگاری روشی است که جهت ممانعت از دسترسی دیگران به اطلاعات خصوصی افراد مورداستفاده قرار می‌گیرد و در برابر حملات دسترسی به اطلاعات و خصوصاً شنود اطلاعات بسیار کارایی دارد. یک سیستم رمز از سه رکن مهم تشکیل می‌شود: 1- مکانیسم رمزنگاری، معمولاً الگوریتم ریاضی برای برگرداندن پیام عادی (پیام اصلی) و تبدیل به

متن رمزنگاری‌شده (پیام در شکل رمزنگاری‌شده)؛ 2- مکانیسم کشف رمز، معمولاً الگوریتمی برای برگرداندن متن رمزنگاری‌شده به متن قبلی و عادی؛ و 3- مکانیسمی برای تولید و پخش کلیدها. کلید پنهانی شبیه کلید مشابه کلید فیزیکی (ملموس) یا قفل ترکیبی عمل می‌کند. کلید فیزیکی اندکی متفاوت تغییر می‌کند (cut) تا قفل خاصی ایجاد کند، مثل یک ماشین. به همین نحو، قفل ترکیبی، مشابه آن‌هایی که برای دانش‌آموزان و دانشجویانی که از قفسه‌های قفل‌دار استفاده می‌کنند، برای قسمتی از ارقام یا سمبل‌ها به‌کاربرده می‌شود تا قفل را باز کند (Swire 2012: 426).

ب. روش‌های رمزنگاری و انواع آن

رمزنگاری برای اطلاعات، حکم قفل برای اطلاعات چاپی را دارد. اطلاعات به‌وسیله درهم سازی به‌نحوی‌که فقط با یک کلید محرمانه از حالت در هم خارج شود، موردحفاظت قرار می‌گیرد. پیام درهم‌ریخته شده که «متن سری[1]» نامیده می‌شود، به‌طورکلی برای کسی که کلید را نداشته باشد ناخواناست. فرایند ایجاد متن سری را «سری‌سازی[2]» یا «رمزی سازی[3]» می‌نامند. درواقع رمزنگاری جلو افراد را برای قطع (متوقف ساختن) پیام‌ها نمی‌گیرد، اما مانع آن می‌شود که اشخاص بتوانند پیام‌های قطع‌شده را بخوانند. پیام‌هایی که باید رمزنگاری شوند «متن ساده[4]» نام دارند، اما متن خروجی فرایند رمزنگاری را «متن رمزی[5]» می‌نامند. رمزنگاری روش‌های متفاوتی دارد؛ از این روش‌ها می‌توان به روش‌های جایگزینی، جابه‌جایی (پس‌وپیش کردن)، پنهان‌سازی، سیستم ابزاری و الگوریتم‌های ریاضی یا کدهای منبع اشاره کرد. اغلب رمزها با دو نوع اصلی دگرگونی شکل، یعنی با «جایگشت» و «جانشینی» تشکیل می‌شوند. در جایگشت، ترتیب قرار گرفتن کاراکترها یا «بیت‌ها» تغییر می‌کند؛ درحالی‌که در جانشینی، بیت‌ها، کاراکترها یا بلوک‌ها تغییر می‌کنند و بیت‌ها، کاراکترها یا بلوک‌های دیگری جانشین آن‌ها می‌شوند. این دگرگونی شکلی، طوری مرتب می‌شود که برای رسیدن به نتایج متفاوت می‌توان روش

1- ciphertext
2- Encipherment
3- Encryption
4- Plain text
5- Chipper text

واحدی با کلیدهای مختلف به کار گرفت. برای «رمزگشایی» شخص باید هم به روش و هم به کلیدی که رمزی سازی با آن انجام‌شده، آگاهی داشته باشد. درحالی‌که کلیدها محرمانه نگاه داشته می‌شوند، خود روش اغلب علنی است؛ زیرا بسیاری از افراد می‌توانند در آن سهیم باشند و از آن محصولات نرم‌افزاری و سخت‌افزاری استفاده کنند (انیسی حماسه 1389: 34). برخلاف آنکه روش‌های رمزنگاری، مدلی است ثابت که همه از الگوریتم آن مطلع هستند و آن الگوریتم با یک کلید محرمانه و قابل‌تغییر کار می‌کند.

سیستم‌های رمزنگاری به دو نوع رمزنگاری متقارن و رمزنگاری نامتقارن تقسیم می‌شوند:

در ***رمزنگاری متقارن***[1] یا کلید خصوصی برای رمزنگاری و رمزگشایی از یک کلید استفاده می‌شود، این روش رمزنگاری به روش تک کلید معروف است. در رمزنگاری «کلید متقارن» هر یک از کامپیوترها دارای یک کلید (Secret) (کد) بوده که با استفاده از آن قادر به رمزنگاری یک بسته‌ی اطلاعاتی قبل از ارسال در شبکه برای کامپیوتر دیگر می‌باشند. درروش فوق می‌بایست ابتدا نسبت به کامپیوترهایی که قصد برقراری و ارسال اطلاعات برای یکدیگر دارند، آگاهی کامل وجود داشته باشد. هریک از کامپیوترهای شرکت‌کننده در مبادله‌ی اطلاعاتی باید دارای کلید رمز مشابه به‌منظور رمزگشایی اطلاعات باشند. برای رمزنگاری اطلاعات ارسالی نیز از کلید فوق استفاده خواهد شد (ابوالحسن پور 1386: 15). باوجود مزایایی از قبیل «روش رمزنگاری سریع» و «کاربرد آن برای حجم زیاد اطلاعات»، کاستی‌هایی وجود دارد که لزوم استفاده از رمزنگاری نامتقارن را ایجاب می‌کند:

«1- ازآنجایی‌که دو طرف کلید یکسانی دارند احتمال خطر دسترسی غیرمجاز کلید بالاست؛ 2- اگر لازم باشد پیام به ازای هر دو نفر فقط محرمانه باشد، تعداد کلیدها ممکن است خیلی زیاد شوند؛ 3- فرستنده یا گیرنده چون دارای کلیدهای یکسانی هستند می‌توانند ادعا کنند که امضاکننده طرف مقابل بوده است (که این شکل با حضور یک شخص ثالث و با یک مرجع صدور کلید قابل‌رفع است)» (انیسی حماسی 1389: 50).

1- Symmetric Encryption (or private Key)

رمزنگاری نامتقارن[1] یا کلید عمومی در ابتدا باهدف مشکل انتقال کلید در رمزنگاری متقارن پیشنهاد شد. در رمزنگاری نامتقارن یا عمومی از ترکیب یک کلید عمومی و یک کلید خصوصی استفاده می‌شود. در این سیستم هر شخص یک جفت کلید دریافت می‌کند که یکی کلید عمومی نام دارد و دیگری کلید اختصاصی. کلید عمومی برای اطلاع عموم منتشر می‌شود ولی کلید اختصاصی محرمانه نگه‌داشته می‌شود. به‌این‌ترتیب دیگر نیازی نیست که فرستنده و گیرنده از یک کلید محرمانه مشترک استفاده کنند، بلکه تمام ارتباطات از طریق کلید عمومی انجام می‌شود و نیازی به ارسال کلید اختصاصی نیست (Swire 2012: 427). در این سیستم احتیاجی به برقراری یک کانال ارتباطی مطمئن نیست، بلکه تنها لازم است کلیدها به روش مطمئنی به کاربرها اختصاص یابند. هر دو کلید با استفاده از عملیات ریاضی بر روی اعداد اول تهیه‌شده‌اند و با یکدیگر مرتبط هستند به‌گونه‌ای که رابطه‌ی رمزنگاری‌شده با هر یک، قابل رمزگشایی با دیگری هست. ازجمله مزایای این روش «متفاوت بودن کلیدها، قابلیت مقیاس‌پذیری نسبت به سیستم متقارن، حفظ صحت، یکپارچگی، اعتبار و انکارناپذیری داده‌ها» (Govinda 2011: 2) و از معایب آن می‌توان به‌سرعت پایین در حجم اطلاعات بالا و پیچیدگی تولید کلید (Kumar 2013: 3) اشاره کرد.

ازآنجاکه سری ماندن پیام‌ها وابسته به کلید است طول کلید یکی از نکات بسیار مهم در طراحی الگوریتم‌های رمزنگاری است. به‌طورکلی سری ماندن و امنیت پیام‌ها با داشتن یک الگوریتم قوی (ولی عمومی) و به همراه یک کلید طولانی تضمین می‌شود (Govinda 2011: 3). تفاوت این دو روش در این است که الگوریتم‌های متقارن از کلید یکسانی برای رمزگذاری و رمزگشایی استفاده می‌کنند یا این‌که کلید رمزگذاری به‌سادگی از کلید رمزگذاری استخراج می‌شود. درحالی‌که الگوریتم‌های نامتقارن از کلیدهای متفاوتی برای رمزگذاری و رمزگشایی استفاده می‌کنند و امکان استخراج کلید رمزگشایی از کلید رمزگذاری وجود ندارد (اسدی 1384: 20).

1- Asymmetric Encryption (or Public Key)

پ. کیفیت ایمن سازی سند الکترونیک با استفاده از رمزنگاری

با استفاده از فناوری رمزنگاری می‌توان سه سرویس امنیتی ارائه کرد: 1- محرمانه سازی هویت؛ 2- حفظ تمامیت (عدم اعمال تغییر بر اطلاعات)؛ 3- اعتبارسنجی مبدأ اطلاعات و جلوگیری از تکذیب اطلاعاتی که از مبدأ آمده‌اند. رمزنگاری روش‌های متفاوتی دارد از میان این روش‌ها می‌توان از روش‌های جایگزینی، جا به جاسازی، پنهان‌سازی، سیستم ابزاری، الگوریتم ریاضی، امضای دیجیتالی و ... نام برد (Mason 2006: 21-22). اغلب رمزها با دو نوع اصلی دگرگونی شکل یعنی با جایگشت و جانشینی تشکیل می‌شوند. در جایگشت ترتیب قرار گرفتن کارکترها تغییر می‌کند، درحالی‌که در جانشینی کاراکترها کلاً تغییر می‌کند و بیت‌ها، کاراکترها یا بلوک‌های دیگری جانشین می‌شوند (عبداللهی 1391: 45). در اینجا به مهم‌ترین نوع رمزنگاری که امضای دیجیتالی است، اشاره می‌شود.

امضای دیجیتالی[1] بلوکی از داده است که به پیام یا سند پیوست می‌شود و آن داده را به شخص یا مؤسسه‌ی به‌خصوصی منسوب می‌کند (وصالی ناصح 1384: 58). همچنین امضای دیجیتال، «خلاصه پیام»[2] نامیده می‌شود که از طریق کاربست کلید خصوصی رمزنگاری‌شده است (Greenleaf 1997: 3). این پیوند به نحوی است که امضا می‌تواند توسط دریافت‌کننده یا شخص ثالث مستقل تأیید شود و نمی‌توان آن را جعل کرد. اگر حتی یک بیت از داده حذف‌شده باشد، امضا در فرایند تأمین اعتبار رد می‌شود. امضاهای دیجیتالی اعتبار منبع یک پیام را نشان می‌دهند. این فناوری که با استفاده از الگوریتم‌های رمزنگاری ایجاد می‌شود، مبتنی بر تکنولوژی‌های مطمئنی نظیر زیر ساختار کلید عمومی[3] است، تصدیق رمزگذاری شده‌ای است که معمولاً به یک پیام پست الکترونیکی یا یک گواهی‌نامه ضمیمه می‌شود تا هویت واقعی تولیدکننده‌ی پیام را تأیید کند. به‌علاوه امکان انکار را از بین می‌برد؛ زیرا کسی نمی‌تواند منکر امضای پیام شود و خود را وارهاند

1- Digital Signature

2- Message Digest - با فرایند محتوای پیام از طریق الگوریتم خاصی ایجادشده است.

3- (PKI)؛ اختراع رمزنگاری کلید عمومی دو نوآوری تازه به همراه آورد. اولین نواری ، توانایی ارسال پیام به‌طرف دیگر بدون نیاز به شخص ثالث مورد اعتماد یا کانال خارج خط (خارج رایانه) برای توزیع کلید سری ، است. دومین نوآوری ، توانایی محاسبه امضاهای دیجیتالی است.

(Wang 2006: 30-32). غیر از مواردی که کلید خصوصی شخص مورد بهره‌برداری قرارگرفته است کسی نمی‌تواند آن امضا را به وجود آورد. *اولین مرحله* برای کاربران امضای دیجیتالی این است که یک جفت کلید عمومی و خصوصی ایجاد شود. کلید خصوصی توسط فرستنده پیام به‌صورت محرمانه نگهداری می‌شود و کلید عمومی به‌صورت آنلاین در دسترس قرار می‌گیرد. *دومین مرحله* این است که فرستنده با ایجاد یک خلاصه منحصربه‌فرد از پیام اصلی چکیده‌ی پیغام و رمزگذاری آن پیام را به‌صورت دیجیتالی تأیید و امضا می‌کند. فرستنده متن اصلی پیام را با استفاده از یک فرمول ریاضی خاص به یک پیام فشرده تبدیل می‌کند که به آن «نتیجه‌ی خود» گفته می‌شود. *سومین مرحله* این است که فرستنده پیام را امضای دیجیتال نماید و سپس پیام را به همراه «نتیجه‌ی خود» برای گیرنده بفرستد. در این مرحله «نتیجه‌ی خود» به‌وسیله‌ی کلید خصوصی اصل-ساز رمزگذاری می‌شود و به پیام اصلی ضمیمه می‌شود. در *چهارمین مرحله* مخاطب پس از دریافت پیام ابتدا آن را به‌وسیله‌ی کلید خصوصی خودش رمزگشایی می‌کند، آنگاه امضای دیجیتالی را به‌وسیله‌ی کلید عمومی ارسال‌کننده رمزگشایی می‌کند و به نتیجه‌ی خود دست می‌یابد و نهایتاً مخاطب یک پیام فشرده‌ی دیگری از پیام اصلی ایجاد و آن را با پیام رمزگذاری شده مقایسه می‌کند؛ اگر نتیجه‌ی دو پیام باهم مطابقت داشتند گیرنده پی می‌برد که پیام تغییرنیافته است (Close 2003: 14)؛ بنابراین با این امضا چهاراصل امنیت اطلاعات تضمین می‌شود: «*تأیید هویت*: گیرنده می‌تواند مطمئن باشد که فرستنده کیست؛ *تمامیت*: گیرنده می‌تواند مطمئن باشد که اطلاعات حین انتقال تغییر نکرده است؛ *انکارناپذیری*: فرستنده نمی‌تواند امضای داده را انکار کند و سرانجام با این اقدام اصل *محرمانگی* که پاسبان امنیت فضای سایبر محسوب می‌شود، نیز حفظ‌شده است».

نتیجه‌گیری

با تدقیق در تعاریف داده‌های شخصی و داده‌های عمومی، به نظر می‌رسد اطلاعات شخصی بیومتریکال که صفات فیزیکی منحصربه‌فردی هستند، تا حد زیادی از خطاپذیری به دورند و افراد برای حفاظت از اصالت و تمامیت داده‌های خود از این بخش از داده‌هایشان به‌عنوان راهبرد امنیتی استفاده می‌کنند. مراجع قضایی نیز درصورتی‌که اشخاص اطلاعات خود را به آن‌ها دهند می‌توانند از اطلاعات بیومتریکال خود جهت

حفاظت و حراست از آن‌ها استفاده کنند؛ اما گاهی فرد اطلاعات مهم خود را با استفاده از رمزنگاری حفاظت و حراست می‌کند و درصورتی‌که مراجع قضایی به این اطلاعات نیاز داشته باشند فرد باید اطلاعات خود را در اختیار مأموران ذی‌صلاح قرار دهد و آن‌ها نیز درصورتی‌که بخواهند به این اطلاعات استناد کنند باید از دو شیوه‌ی ایمن‌سازی پیش‌گفته استفاده نماید. این رویه در مواد 656 و 658 قانون آیین دادرسی کیفری مورداشاره قرارگرفته و حتی در مواد 660 و 661 این قانون برای افرادی که موجبات افشای این داده‌ها و نقض تدابیر امنیتی سامانه را فراهم می‌سازند، مجازات تعیین‌شده است. پیش‌ازاین نیز قانون‌گذار در ماده‌ی 40 و 49 و 50 قانون جرایم رایانه‌ای و ماده‌ی 11 و 15 و 16 آیین‌نامه‌ی استنادپذیری ادله‌ی الکترونیک نیز به این امر اشاره‌کرده است. با این اوصاف به نظر می‌رسد آنچه برای مراجع قضایی اهمیت دارد این است که اصالت، تمامیت و انکارناپذیری داده‌ها حفظ شود که این مهم می‌تواند از همان بدو ورود داده‌ها به مراجع قضایی توسط فرد صاحب داده‌ها یا در مرحله‌ی توقیف توسط فردی که متصدی جمع‌آوری است، تأمین شود تا داده‌ها ایمن شوند و در مراجع قضایی قابل استناد باشند.

با توجه به مطالب مذکور بیومتریک و رمزنگاری به‌عنوان دو راهکار امنیتی در تأمین شروط استنادپذیری کمک شایانی می‌کنند. یک زنجیره‌ی بیومتریک می‌تواند به سهولت قابلیت صحت اسناد را تحقق بخشد و فرد را قادر سازد در مرحله‌ی محتوا، انتقال و منبع صحت اسناد را به آسانی اثبات کند. این زنجیره به دلیل پردازش اطلاعات هر فرد با ویژگی‌های منحصربه‌فرد خودش به‌محض ورود رخنه گران تطابق اطلاعات وارده را با اطلاعات پردازش‌شده‌ی قبلی موردسنجش و ارزیابی قرار می‌دهد و در صورت عدم تطابق اجازه‌ی دسترسی به اطلاعات فرد را به او نمی‌دهد. در رمزنگاری نیز با استفاده از روش‌هایی چون جایگزینی، جابه‌جا سازی، سیستم ابزاری، الگوریتم ریاضی، امضای دیجیتالی و ... از صحت انتساب و انکارناپذیری اطلاعات حمایت به عمل می‌آید. در پایان پیشنهاد می‌شود با لزوم توجه به ماده‌ی 14 قانون تجارت الکترونیک که تنها داده‌های الکترونیکی را معتبر شناخته که با شرایط ایمن حفاظت‌شده‌اند و آن‌ها را دارای ارزش اثباتی دانسته است، قانون‌گذار می‌بایست به‌گونه‌ای جدی زیرساخت‌هایی چون زیست‌سنجی و سامانه‌ی شناسایی خودکار اثرانگشت، زیرساخت کلید عمومی، شخصی‌سازی صدور و ... را آماده سازد تا در پرتو فراهم شدن این بسترها امکان

به‌کارگیری کارآمدتر این تدابیر امنیتی فراهم شود و بالطبع ایمنی اطلاعات الکترونیکی از مرحله‌ی کشف تا مرحله‌ی ارائه و استناد در دادگاه‌ها تأمین و تسهیل شود.

منابع

الف) فارسی

- ابوالحسن پور، وحیده. (1386). «شبکه‌های مجازی اختصاصی»، *مجله الکترونیکی پژوهشگاه اطلاعات و مدارک ایران*، دوره 5، شماره 2، 1386، صص 20 -1.
- احسانی مؤید، فرزانه. (1389). «ورود جاسوس‌ها ممنوع»، *ماهنامه‌ی اطلاعات*، شماره 12، سال یازدهم، صص 18 - 1.
- احمدی، جواد. (1388). «دنیای بیومتریک». *ماهنامه‌ی فناوری*، سال چهارم، شماره 13، ص 28-13.
- استنلی، پائول. (1391). *حقوق حفظ اسرار*، مترجم: محمدحسین وکیلی مقدم، چاپ اول، تهران، کتاب همگان.
- اسدی، مریم. (1384). «فناوری‌های امنیت اطلاعات: با یک دیدگاه طبقه‌بندی». *علوم اطلاع‌رسانی*، دوره 20، شماره 3 و 4، بهار و تابستان 1384، صص 16-1.
- انیسی حماسه، زهره. (1389). «امضای دیجیتال راهکاری مؤثر در پیشگیری از جرایم رایانه‌ای». *ماهنامه عصر فناوری اطلاعات*، شماره 56، مرداد 1389، سال ششم، صص 53 - 48.
- باستانی، برومند. (1386). *جرایم کامپیوتری و اینترنتی*، چاپ دوم، تهران، انتشارات بهنامی.
- جلالی فراهانی، امیرحسین. (1386). «استنادپذیری ادله‌ی الکترونیکی در امور کیفری». *مجله‌ی فقه و حقوق*، شماره 15، سال چهارم، صص 114- 83.
- حسن آبادی، مهدی. (1386). «تکنولوژی‌های تصدیق هویت». *نشریه‌ی رایانه*، شماره 167، سال دهم، صص 25- 9.
- حسن بیگی، ابراهیم. (1384). *حقوق و امنیت در فضای سایبر*، چاپ اول، تهران، مؤسسه‌ی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران.
- رضایی، علی. (1382). *حقوق تجارت الکترونیک*، چاپ اول، تهران، گنج دانش.
- زندی، محمدرضا. (1389). *تحقیقات مقدماتی در جرایم سایبری*، چاپ اول، تهران، جنگل.

- زیبر، اولریش. (1383). *جرایم رایانه ای*، مترجم: محمد علی نوری، رضا نخجوانی، مصطفی بختیاروند، احمد رحیمی مقدم، چاپ اول، تهران، گنج دانش.
- ساجدی، حامد. (1386). «بیومتریک، فناوری در خدمت امنیت». *ماهنامه تکفا*، شماره 7، سال پنجم، صص 142- 134.
- شهبازی نیا، مرتضی، عبداللهی، محبوبه. (1389). «دلیل الکترونیک در نظام ادله‌ی اثبات دعوا». *فصلنامه‌ی حقوق دانشکده حقوق و علوم سیاسی*، دوره 40، شماره 4، زمستان 89، صص 205 - 193.
- شیرزاد، کامران. (1388). *جرایم رایانه ای از دیدگاه حقوق جزای ایران و حقوق بین‌الملل*. چاپ اول، تهران، شرکت نشر بهینه فراگیر.
- عباسی کلیمانی، عاطفه. (1385). *مطالعه‌ی تطبیقی جرایم اینترنتی در حقوق ایران و اسناد بین‌المللی*. پایان‌نامه کارشناسی ارشد حقوق جزا و جرم‌شناسی، پردیس قم دانشگاه تهران.
- عبداللهی، محبوبه. (1391). *دلیل الکترونیکی در نظام ادله‌ی اثبات دعوا*، چاپ اول، تهران، انتشارات خرسندی.
- فضلی، مهدی. (1388). *مسؤولیت کیفری در فضای سایبر*، چاپ اول، تهران، انتشارات خرسندی.
- کاتوزیان، ناصر. (1388). *اثبات و دلیل اثبات*، چاپ ششم، تهران، انتشارات میزان.
- لینان دبلفون، زویه. (1388). *حقوق تجارت الکترونیک*، مترجم: ستار زرکلام، چاپ اول، تهران، انتشارات شهردانش.
- محمدی، سام، میری، حمید. (1388). «بررسی تطبیقی ارائه‌ی ادله‌ی الکترونیک در دادگاه؛ اشکال و اعتبار آن». *نامه مفید*، شماره 76، صص 178 - 151.
- نوری، محمد علی. (1382). *حقوق تجارت الکترونیک*، چاپ اول، تهران، انتشارات گنج دانش.
- وصالی ناصح، مرتضی. (1384). «امضای الکترونیک و جایگاه آن در ادله‌ی دعوا». *مجله کانون وکلا*، دوره دوم، شماره 59، سال 48، صص 69 - 54.
- هاتف، رضا. (1387). «تأمین امنیت». *گاهنامه‌ی امنیت*، شماره 28، سال ششم، صص 28 - 12.

- هـاتف، مهـدی. (1386). «بیومتریـک رویکـردی نـوین در تـأمین امنیـت». *دوماهنامـه‌ی توسعه‌ی انسانی پلیس*، شماره 12، سال چهارم، صص 84 - 70.

ب. انگلیسی

- Chawki, Mohamad; AbdelWahab, Mohamad. (2005). Identity Theft in Cyber Space: Issues and Solution, *George Town University Law Center*, Vol. 3, pp. 8-30.
- Close Angeline Grace,Zinkhan Georg; Finney,Zachary. (2003). Cyber Identity Theft: A Conceptual Model and Implication for Public Policy, *Northwestern University School of Law*, No. 07-09, pp. 1-27.
- Gaur, Priyanka; Srivastava, Prabhat. (2015). Biometric Risks - How to Deal with the Challenges, *Scholedge International Journal of Management & Development*, Vol. 2, No. 7, pp. 16-23.
- Greenleaf, Graham; Clarke, Roger. (1997). Privacy Implications of Digital Signatures, *IBC Conference on Digital Signatures (Proc.)*, Sydney, pp. 1 - 12.
- K.Govinda; E.Sathiyamoorth. (2011). Multilevel Cryptography Technique Using Graceful Codes, *Journal of Global Research in Computer Science*, Vol. 2, No. 7, pp. 1-5.
- Kerr, Orins. (2005). Digital Evidence and the New Criminal Procedure, *The George Washington University Law School Public Law and Legal Theory Working Papper*, No. 108, pp. 1-62.
- Kumar, Animesh. (2013). Asymmetric key Cryptography, pp. 1- 11, Available at SSRN: http://ssrn.com/abstract=2372882.
- Levy. S, Grand. (2005). Theft Identity, *The American Journal of International Law*, Vol. 80, No. 1, pp. 40-60.
- Mason, Stephan. (2006). Electronic Signature in Practice, *Journal of High Technology Law*, Vol. VI, No. 2, pp. 33-48.
- Swire, Peter; Ahmad, Kenesa. (2012). Encryption and Globalization, *Columbia Science and Technology Law Review*, Vol. 23, No. 157, pp. 416 - 481.
- Wang, Minyan. (2006). The Impact of Information Technology Development, *Journal of Law and Technology*, Vol. 15, No. 3, pp. 1-37.