استنادپذیری ادلهٔ الکترونیکی در امور کیفری*

تاریخ دریافت: ۱۳۸٦/۹/۲۳ تاریخ تأیید: ۱۳۸٦/۱۱/۳

امیرحسین جلالی فراهانی**

چکیده

در هزارهٔ نوین، تقریباً هیچ امری باقی نمانده است که به‌طور مستقیم یا باواسطه، به فناوری‌های نوین اطلاعاتی و ارتباطاتی (ICTs) وابسته نباشد. این وضعیت نوپدید، حوزه‌های گوناگون، از جمله نظام حقوقی را تحت تأثیر خود قرار داده است. در این میان، شاید هیچ شاخه‌ای به اندازهٔ نظام ادلهٔ اثبات دعاوی، تأثیر نپذیرفته باشد؛ زیرا داده‌های رایانه‌ای هیچ سنخیتی با اسناد و اطلاعات دنیای فیزیکی ندارند. این دغدغه در نظام ادلهٔ اثبات کیفری جدی‌تر است. به‌ویژه آنکه ضابطه‌مند شدن عملکرد مجریان قانون در مواجهه با پرونده‌های کیفری سایبری یا مرتبط با فضای سایبر، ضرور است. در غیر این صورت، نه تنها عدالت اجرا نشده است، بلکه به موازین حقوق بشری نیز تعرض شده است.

واژگان کلیدی: *داده‌های الکترونیکی، استنادپذیری، هویت پدیدآورنده، اعتبار، مجریان قانون.*

---

* این مقاله خلاصه‌ای از کار پژوهشی با عنوان «درآمدی بر استنادپذیری ادلهٔ الکترونیکی در امور کیفری» است که توسط نگارنده در سال ۱۳۸٦ برای معاونت حقوقی و توسعهٔ قضایی قوهٔ قضائیه انجام شده است.

** کارشناس ارشد حقوق کیفری و جرم‌شناس و پژوهشگر در حقوق کیفری سایبری.
(jalalyfarahany1979@gmail.com)

مقدمه

پس از احراز صلاحیت کیفری، مرجع قضایی موظف است دلایـل و مـدارک ارائـه شده از سوی طرفین دعوا را بررسی و نسبت به آنها تعیین تکلیف کنـد. «دلیـل» کـه در اصطلاح حقوق جزا به هر چیزی گفته می‌شود که وجود یا عدم وجود چیزی یا صحت و سقم ادعایی را ثابت می‌کنـد (آشـوری، ۱۳۸۰: ۲۰۱)، از چنـان جایگـاهی برخـوردار است که عده‌ای از صاحب‌نظران معتقدند تاریخ آئین دادرسی کیفری، در حقیقت تاریخ تحول ادلهٔ اثبات است و سیر تحول این حوزه را بر پایـهٔ نگـرش سیاسـت‌گـذاران هـر دوره، نسبت به ادلهٔ قابل استناد در محاکم طبقه‌بندی کرده‌اند.

حاکمیت علوم تجربی در دوران معاصر، نظام عدالت کیفری را هم تحت تأثیر خـود قرار داده است. مهم‌ترین ویژگـی دورهٔ تجربـی یـا علمـی، کـم‌رنـگ شـدن مـستندات غیرتجربی یا به عبارتی معنوی، در نظام عدالت کیفری اسـت. در دوره‌هـای گذشـته، از یک سو به دلیل عدم توسعهٔ علوم و از سوی دیگر اعتقاد همگان به جایگاه راسخ مهـم معنویات و امور باطنی، عمدهٔ دلایل ابرازی جهت اثبـات جـرایم، در اقـرار، شـهادت و نهایتاً علم قاضی خلاصه می‌شد که به دلیل نبود ابزارهـا و امکانـات لازم، حتـی گزینـهٔ آخر نیز معمولاً به دریافتهای باطنی قاضی محدود می‌شد؛ اما با گذشت زمان، بـا تأکیـد بر اثبات‌پذیری همهٔ وقایع از راه‌های تجربی، اهمیت این نوع ادله به نحو قابـل تـوجهی کاهش یافت.

پیدایش و پیشرفت حیرت‌انگیز فناوری‌های نو، سبب برگشت‌ناپذیری این رویکـرد شده است و صاحب‌نظران نظام عدالت کیفری کوشیده‌اند با نهادینه‌سـازی شـاخه‌هـای پژوهشی ـ کاربردی جدید، مانند کشف علمی جرایم، در عـین حـال کـه بـر غنـای آن می‌افزایند، نواقص و نارسایی‌های حقوقی ـ علمی آن را هم رفع کنند.

از جمله نمونه‌های برجستهٔ فراگیری که می‌توان نام برد، فناوری اطلاعات و ارتباطـات (ICT) است. امروزه کمتر حوزه‌ای را می‌توان یافت که از این فناوری تأثیر نپذیرفته باشـد. همهٔ حوزه‌هـایی کـه در سیـستم‌هـای رایانـه‌ای مـستقل (individual computer system) اداره می‌شوند و چه آنهایی که به جامعهٔ اطلاعاتی (information society) در گستره‌ای لایتناهی به نام فضای سایبر (cyber space) می‌پیوندند، ماهیت مشترکی به نام داده‌های

الکترونیکی (electronic data) دارند. این داده‌ها مفاهیم گوناگونی را در خود جای داده‌اند؛ لذا می‌توانند کارکردهای گوناگونی داشته باشند.

در پرتو نظام ادلهٔ اثبات در امور کیفری، از آنجا که داده‌ها، حقایق مربوط به امور خود را دربردارند، باید بتوانند به کشف جرایم کمک کنند. قدری تأمل آشکار می‌سازد که این حوزه، گستره‌ای بسیار وسیع‌تر از آنچه را که جرایم رایانه‌ای ــ سایبری (computer – cyber crime) نامیده می‌شوند، دربرمی‌گیرد.

به‌طور کلی، جرایم از سه جهت با فناوری اطلاعات و ارتباطات برخورد دارند:

۱. گاهی مجرمان برای ادارهٔ امور مجرمانه‌شان، این فناوری را به‌کار می‌گیرند. مثلاً، قاچاقچیان برای امور حسابداری‌شان از سیستم‌های رایانه‌ای یا برای هماهنگی با یکدیگر، از سیستم‌های ارتباطات الکترونیکی استفاده می‌کنند.

۲. گاهی نیز، مزایای این فناوری، مجرمان را به سمت خود جلب می‌کند تا با به‌کارگیری آن، علاوه بر پایین آوردن هزینهٔ جرم، نتایج مورد انتظارشان را افزایش دهند. برای مثال، یک کلاهبردار در شرایط عادی می‌تواند فقط تعداد محدودی را تحت تأثیر ترفندهای متقلبانه‌اش قرار دهد؛ حال آنکه در فضای سایبر، تعداد نامحدودی مخاطب وجود دارند که در صورت اثربخش بودن ترفندها، همان نتیجهٔ مورد انتظار ـ یعنی تحصیل اموال آنها ـ محقق می‌شود، با این تفاوت که تعقیب و دستگیری وی به مراتب دشوارتر خواهد بود.

۳. اما گروه سوم، جرایمی هستند که از این فناوری برخاسته‌اند. به عبارت دیگر، بدون این فناوری ارتکاب آنها امکان‌پذیر نخواهد بود؛ مانند دسترس غیرمجاز (unauthorized access, hacking) و کلاهبرداری رایانه‌ای (computer fraud).

در تمام موارد پیش‌گفته، عنصر مادی جرم، در بستر این فناوری تحقق می‌یابد؛ به همین دلیل قانونگذاران کیفری با احراز نارسایی قوانین فعلی، جرم‌انگاری‌های جدید را در دستور کار قرار داده‌اند.*

* کنوانسیون اروپایی جرایم سایبر (نوامبر ۲۰۰۱)، در بند ۲ مادهٔ ۱٤ که اولین مادّه از بخش شکلی کنوانسیون به شمار می‌آید، بر این سه نوع از جرایم تصریح کرده است (مرکز پژوهش‌های مجلس شورای اسلامی، ۱۳۸٤: ۲۲).

به این ترتیب، فناوری اطلاعات و ارتباطات، نسبت به حقوق جزای ماهوی (substantive criminal law)، حقوق جزای شکلی (procedural criminal law) را با تحولات بسیار عمیق‌تری مواجه کرده است. به‌عنوان مثال اگر با برداشتن مرزهای فیزیکی، صلاحیت کیفری را به چالش کشیده است، در اینجا ماهیتی به نام دادهٔ الکترونیکی، برگ جدیدی را در نظام ادلهٔ اثبات رقم زده است. با اینکه این داده‌ها تنها انعکاس متفاوتی از نظایر خود در دنیای فیزیکی به شمار می‌آیند، ولی ویژگی‌های منحصر به‌فردی دارند که مستلزم قواعد و تدابیر جدیدی هستند.

از جمله ویژگی‌هایی که شاید بتوان آنها را نقاط قوت داده‌های الکترونیکی نسبت به اطلاعات فیزیکی برشمرد، عبارت‌اند از (کیسی، ۱۳۸٦: ۱۹):

۱. از داده‌های الکترونیکی می‌توان دقیقاً کپی‌برداری کرد، به نحوی که تنها راه تفکیک اصل از کپی، مراجعه به یک سری داده‌های ثبت شدهٔ خاص در سیستم رایانه‌ای مورد نظر است؛ در حالی که دقیق‌ترین دستگاه‌های کپی، چنین توانایی‌ای ندارند.

۲. به لحاظ قرار داشتن داده‌ها در قالب انعطاف‌پذیر الکترونیکی و همچنین امکان کپی‌برداری دقیق از آنها، به راحتی می‌توان هرگونه تغییر و اصلاح را در نسخه‌های کپی، همانند نسخهٔ اصل انجام داد و اصل سند را محفوظ داشت.

۳. هرگونه تغییر و اصلاح انجام شده در داده‌ها، در فایل‌های جداگانه‌ای به ثبت می‌رسد؛ به همین دلیل، می‌توان با به‌کارگیری ابزار و برنامه‌های بسیار متنوعی که برای این کار طراحی و تولید شده‌اند، به موارد تغییریافته پی برد. برای مثال، الگوریتم تنظیم پیام (message digest 5) همانند جعبهٔ سیاه هواپیما عمل می‌کند و برای هر ورودی، شمارگان ۳۲ تایی متفاوتی تولید می‌کند. بنابراین، تنها در صورت یک کپی‌برداری دقیق، تنظیم پیامِ کپی با تنظیم پیامِ اصل یکسان خواهد بود، وگرنه حتی در صورت بروز تغییرات بسیار جزئی، تنظیم پیام کاملاً متفاوتی ایجاد خواهد شد.

٤. از بین بردن داده‌های الکترونیکی مشکل است. آنچه که ما در واقع امر به هنگام پاک کردن (deletion) داده‌ها انجام می‌دهیم، از بین بردن آنها نیست، بلکه غیرقابل دسترس کردن آنهاست. آنها در فضاهای راکد (slack space) و تخصیص‌نیافتهٔ (unspecified space) دیسک‌های ذخیره باقی می‌مانند، که با به‌کارگیری نرم‌افزارهای ویژه می‌توان بسیاری از آنها را بازیابی کرد.

۵. ویژگی آخر مربوط به ماهیت فضای سایبر است. چنانچه داده‌های رایانه‌ای از یک سیستم رایانه‌ای خارج و در فضای سایبر رها شوند، کپی‌های آنها در بسیاری از نقاط ذخیره خواهند شد. این وضعیت باعث می‌شود، از یک‌سو امکان از بین رفتن ادله به حداقل برسد و از سوی دیگر با استناد به سوابق الکترونیکی بیشتر و متنوع‌تر، امکان محکمه‌پسند بودن آنها افزایش می‌یابد.

در مقابل، این داده‌ها نقاط ضعف انکارناپذیری دارند، از جمله:

۱. مهم‌ترین ایراد این نوع اطلاعات، دشواری نسبت دادن آنها به پدیدآورنده‌شان است. چنانچه هویت پدیدآورنده احراز نشود، هر اندازه داده‌ها صحیح و دقیق هم باشند، استنادپذیر نخواهند بود.

۲. با اینکه امکان شناسایی هرگونه تغییر در داده‌ها وجود دارد، اما تغییر در آنها نیز بسیار آسان است. در حالی که برای شناسایی آنها، به ابزارهای خاص و پیشرفته، نیروی باتجربه و ماهر و همچنین زمان نسبتاً زیادی نیاز است.

۳. از بین بردن داده‌ها بسیار آسان است. می‌توان با نصب یک برنامهٔ نه چندان پیشرفته بر روی رایانه، تنظیم آن و زدن چند دکمه از صفحه کلید، تمامی داده‌های مورد نظر را از بین برد. گاهی مجرمین حرفه‌ای سایبری، به نحوی ادلهٔ مجرمانه را پاک می‌کنند که با ابزارهای پیشرفته هم نمی‌توان آنها را بازیابی کرد.

٤. نقص سیستم یا رسانهٔ ذخیره می‌تواند بر تمامیت (integrity) داده‌ها تأثیر گذارد. یکی از تفاوت‌های اصلی داده‌های الکترونیکی با اسناد و مدارک فیزیکی در این است که به تنهایی در دنیای خارج وجود ندارند و همواره به یک سیستم یا رسانه وابسته‌اند. بنابراین هرگونه تغییر در وضعیت سیستم، بر وضعیت داده‌ها تأثیر می‌گذارد.

۵. نقص برنامه‌های رایانه‌ای هم ایراد فوق را دامن می‌زند. هر داده‌ای که به یک سیستم رایانه‌ای وارد می‌شود، نوعی پردازش (process) بر روی آن انجام می‌شود. حتی صرفِ نگهداری و ذخیرهٔ داده‌ها در سیستم یا انتقال آنها بر روی یک رسانه نیز پردازش تلقی می‌شود. برای هر پردازش، به برنامه‌ای خاص نیاز است تا داده‌های مورد نظر را براساس دستورالعملِ تعریف شده، پردازش کند. بنابراین، حتی در ساده‌ترین حالت نیز داده‌ها به یک یا چند برنامه، وابستگی کامل دارند. در نتیجه اگر آن برنامه‌ها دچار نقص باشند، بر خروجی داده‌ها تأثیر مستقیم خواهند گذاشت.

٦. نسبت به اطلاعات فیزیکی، بیشتر در دسترس افراد غیرمجاز قرار دارند در حالی‌که دستیابی به یک سند یا مدرک فیزیکی برای افراد محدودی امکان‌پذیر است. در نتیجه می‌توان با اتخاذ تدابیری، احتمال دست‌یابی افراد غیرمجاز را به حداقل رساند. این مسئله تا حدودی در خصوص داده‌های موجود در سیستم‌های رایانه‌ای مستقل نیز درست است؛ زیرا، افراد معدودی با آن کار می‌کنند. اما هنگامی که همین داده‌ها به صورت آن‌لاین، در فضای سایبر قرار می‌گیرند، با امکاناتی که هم‌اکنون فضای سایبر در اختیار همه قرار می‌دهد، می‌توان به آنها دسترس پیدا کرد. به همین دلیل، بعضی از محاکم، میان داده‌های الکترونیکی آن‌لاین و آف‌لاین، تفاوت قائل شده‌اند و معتقدند: داده‌های دارای منشأ اینترنت، غیرقابل اعتمادند (Gahtan, 1999: 158).

با توجه به این مسائل، لازم است برای به‌کارگیری داده‌های الکترونیکی در فرایند دادرسی کیفری، چاره‌جویی اساسی شود. زیرا، از یک‌سو نمی‌توان آنها را نادیده انگاشت، زیرا تعیین تکلیف راجع به طیف گستردهٔ جرایم مرتبط با این فناوری به آنها وابسته است. از سوی دیگر می‌توان با اتکای به قواعد موجود، آنها را وارد این فرایند کرد، زیرا ماهیت و ویژگی‌های یکسانی ندارند.

از میان نظام‌های حقوقی موجود، نظام حقوق عرفی (common law) با چالش‌های بیشتری مواجه شده است. این نظام نسبت به دیگر نظام‌ها، به‌ویژه نظام حقوقی رومی ـ ژرمنی (civil law) تأکیدی بر اقناع وجدانی قضات ندارد و آنها مکلفند بر روی دلایل و مدارک ابرازی، تمرکز کنند. بنابراین در چارچوب این نظام، سیاست‌گذاری‌های جدیدی صورت گرفته است که می‌تواند برای کشورهای دیگر الگو باشد (دبیرخانهٔ شورای عالی انفورماتیک کشور، ١٣٧٦: ٦٦).

بر این اساس، موضوعات ناظر بر این حوزه، در دو فصل مطرح می‌شود:

١. ابتدا قواعد عمومی ناظر بر استنادپذیری ادلهٔ الکترونیکی بررسی می‌شود که عبارت‌اند از: هویت پدیدآورنده و اعتبار داده‌های الکترونیکی. در اینجا تفاوتی میان امور حقوقی و کیفری نیست و احراز آنها از سوی هر دو نوع دادگاه، لازم است.

٢. با توجه به اصل تحصیل آزادانهٔ دلایل در امور کیفری و الزام قضات به کشف حقیقت برخلاف امور حقوقی، اقدامات مجریان قانون به عنوان ضابطان قضایی در پرتو ضوابط حقوقی و علوم قانونی بررسی می‌شود.

گستردگی مطالب، اکتفا به کلیات را ایجاب می‌کند و آنچه بـه عنـوان نتیجـه‌گیـری مدّ نظر است، در نوشتارهای بعدی میسر خواهد بود.

فصل اول: قواعد عمومی ناظر بر استنادپذیری ادلهٔ الکترونیکی

به‌طورکلی، برای اینکه هرگونه اطلاعات در هـر قالـب، اعـم از الکترونیکـی و غیـر الکترونیکی، قابلیت ارائه به دادگاه، اعم از حقوقی و کیفری را داشته باشد و از سوی آن مورد استناد قرار گیرد، باید دارای دو شـرط باشـد: اول اینکـه، هویـت پدیدآورنـدهٔ آن معلوم باشد، زیرا دلیلی که پدیدآورندهٔ آن نـامعلوم اسـت، قابلیـت اسـتناد نـدارد. ثانیـاً اطلاعات معتبر باشد. نبود یا نقص هر یک از این شرایط، باعث رد دلایل خواهـد شـد. بنابراین باید دید، در رابطه با داده‌های الکترونیکی چه شرایطی را باید مدّ نظر قـرار داد تا این قواعد رعایت شود.

گفتار اول: هویت پدیدآورندهٔ ادلهٔ الکترونیکی

با توجه به توضـیحاتی کـه در خـصوص ویژگـی‌هـای منحـصر بـه فـرد داده‌هـای الکترونیکی ارائه شد، پیچیدگی‌های مربوط به رعایت این قاعده آشکار می‌شود. یکی از ویژگی‌های منحصر به فرد فنـاوری اطلاعـات و ارتباطـات، ناشـناختگی (anonymity) است، یعنی در محیطی فعالیت‌های گوناگون انجام می‌شود که امکـان انتـساب فعـل بـه پدیدآورنده، به آسانی میسّر نیست. برای مثال، هنگامی که متنی در محیط واژه‌پرداز یک سیستم رایانه‌ای تایپ می‌شود، تنها چیزی کـه انعکـاس مـی‌یابـد، یـک شـیوهٔ نگـارش تعریف شده مانند Zar یا Lotus است که مطابق تنظیمات کـاربر، در سـند الکترونیکـی درج می‌شود. اما تنها با مطالعهٔ آن سند نمی‌توان به پدیدآورنـدهٔ آن پـی بـرد، زیـرا هـر کاربر با استفادهٔ منطقی و نظام‌یافتهٔ صفحه‌کلید، می‌تواند پدیدآورنـده باشـد. البتـه همـهٔ اسناد ایجاد شده در محیط واژه‌پرداز، به نام کسی که به هنگام نصب برنامه نـامش درج شده، ثبت می‌شوند. بنابراین با اینکه قرینهٔ خوبی است، اما اطمینان‌بخش نیست؛ به‌ویـژه آنکه سیستم رایانه‌ای برای افراد زیادی قابل دسترس باشد.

حال اگر به جای یک سیستم رایانه‌ای محدود به زمان و مکان، که بـه هـر حـال بـا

مراجعه به امارات دیگر، می‌توان به پدیدآورندهٔ اصلی ظنین شد، گستره‌ای به اندازهٔ فضای سایبر پیش رو قرار گیرد، چه رخ می‌دهد؟ برای مثال، در محیط‌های گفت‌وگو (chat rooms)، هرکس می‌تواند با انواع هویت‌های مجعولی که برای خود برمی‌گزیند، با دیگر افراد کرهٔ زمین ارتباط برقرار کند. ایجاد یک اعتبار پست الکترونیکی نیز همانند ورود به محیط‌های گفت‌وگو، به تخصص، مهارت و ابزار خاصی نیاز ندارد و از ساده‌ترین فعالیت‌های شبکه‌ای به شمار می‌آید.

برای حل این مسئله، تدابیر و ابزارهای گوناگونی به‌کار گرفته شده است که به دلیل نقش اساسی آنها در استنادپذیری ادلهٔ الکترونیکی، قانون‌گذاران کشورها بنا به ضرورت به آنها جنبهٔ قانونی داده‌اند. آشنایی با فرایند اصلی و عمدهٔ ابزارهای احراز هویت الکترونیکی، به شناخت این حوزه کمک می‌کند؛ هرچند نباید ملاحظات جدی آن را نادیده انگاشت.

۱. فرایند احراز هویت پدیدآورندهٔ داده‌های الکترونیکی

این عنوان برخلاف ظاهر ساده، فرایند پیچیده‌ای را شامل می‌شود و حتی موضوعات آن به مباحث فلسفی هم کشیده شده است و از سوی صاحب‌نظران به تفصیل مورد بحث قرار گرفته است. مجموع این فرایند را می‌توان در سه مرحله خلاصه کرد:

الف. اعطای هویت (identity)

افراد به فراخور نقش‌هایی که در اجتماع می‌پذیرند، حائز هویت‌های گوناگونی مانند: آموزشی، درمانی، اقتصادی، سیاسی و... می‌شوند. البته همهٔ اینها در شخصیت واحد یک فرد جمع و به آن ختم می‌شوند، ولی برای حضور در هر یک از آنها باید هویت متناسب با آن را داشت. برای مثال نمی‌توان با هویت آموزشی از خدمات درمانی بهره‌مند شد یا با هویت اقتصادی، در امور سیاسی وارد شد (T. Kent, 2003: 20).

اعطای هویت باعث می‌شود، کلیهٔ امور و به تبع آن داده‌هایی که در جریان تراکنش‌ها به وجود می‌آیند، دارای شخصیت شوند و از ناشناختگی درآیند. هرچه این امر وسیع‌تر و نهادینه‌تر شود، میزان داده‌های دارای هویت و قابل استناد، بیشتر خواهد شد.

با این حال، هنوز در بعضی از حوزه‌های الکترونیکی، اصل بر ناشناختگی است. نمونهٔ بارز آن، پست الکترونیکی است. البته برخی سازمان‌های دولتی و غیردولتی در سطح بسیار محدودی به‌کارکنانشان اعتبارهای (account) رسمی اعطا کرده‌اند. اما آنچه از سوی مراکز اصلی ارائه‌دهندهٔ خدمات پست الکترونیکی مانند Yahoo وGmail و در گسترهٔ جهانی انجام می‌شود، الزامی به احراز هویت واقعیِ دارندهٔ پست الکترونیکی نیست.

لازم به ذکر است، اعطای هویت به اشخاص حقیقی خلاصه نمی‌شود و اشخاص حقوقی را هم دربرمی‌گیرد. این مسئله به‌ویژه با تغییر رویکرد قانون‌گذاران کشورها در تحمیل مسئولیت کیفری به آنها، اهمیت اساسی است. زیرا برای احراز مجرمیت آنها، به دلایلی نیاز است که دارای هویت آنها باشند.*

ب. اعطای شناسه (identifier) ویژگی (attitude)

برای اینکه یکتایی هویت افراد حفظ شود و استیفا از حقوق تخصیص‌یافتهٔ به آنها و همچنین مسئولیت‌های احتمالی، جنبهٔ انحصاری‌شان را حفظ کنند، اینگونه علامت‌ها و نشانه‌ها اعطا می‌شوند.

با کمی تسامح، می‌توان دو نکتهٔ پیش‌گفته را یک‌جا بیان کرد. زیرا، در اینکه هر دو به شخص مورد نظر ارجاع می‌دهند، وجه مشترک دارند. ولی تفاوت اصلی آنها این است که مانند چند شمارهٔ چند رقمی شناسه پدید می‌آید، اما ویژگی در شخص وجود دارد و به‌کار گرفته می‌شود، مانند اثر انگشت و عنبیهٔ چشم.

آنچه از منظر نظام حقوقی اهمیت دارد، این است که یکتایی و انحصار این گزینه‌ها، به‌ویژه شناسه‌ها، به هویتشان تضمین شود. اگر یک شناسه / ویژگی، به گونه‌ای تعریف شود که دو هویت، امکان بهره‌برداری از آن را داشته باشند، یا یک هویت، به دو شناسه / ویژگی تعلق داشته باشد، اصل این فرایند زیر سؤال خواهد رفت. بنابراین، برای افزایش میزان اطمینان‌پذیری (reliability) این فرایند، به‌ویژه برای حوزه‌های حساس، دو یا چند شناسه / ویژگی به یک هویت اختصاص می‌یابند و تأیید همهٔ آنها، ملاک ورود فرد به مجموعه خواهد بود.

* کنوانسیون جرایم سایبر، در مادهٔ ۱۲، مسئولیت کیفری اشخاص حقوقی مربوط به جرایم مندرج در این کنوانسیون را به رسمیت شناخته است (مرکز پژوهش‌های مجلس شورای اسلامی، ۱۳۸٤: ۱٦).

ج. تأیید (authentication) / تجویز (authorization)

چنانچه هویت، با شناسه / ویژگیِ اعطا شده منطبق باشد و شناسایی (identification) به شکل صحیح انجام شود، مرحلهٔ تأیید و پس از آن تجویز، آغاز می‌شود. در اینجا نیز با قدری تسامح، این دو، در کنار یکدیگر آورده شده‌اند. زیرا در نگاه کلی، هدف واحدی را دنبال می‌کنند. البته تأیید، به دنبال شناسایی صورت می‌گیرد و ناظر به شخصیت فردی است، ولی تجویز، ناظر به صلاحیت فرد برای حضور در حوزهٔ خاص است. بنابراین می‌توان گفت، میان اینها نظم منطقی حاکم است. به همین دلیل ممکن است برای هر یک از آنها شناسه / ویژگی‌های متمایزی در نظر گرفته شود. برای مثال، برای حضور در یک فرایند کارگزاری دولت الکترونیکی، باید شناسه / ویژگی‌هایی را ارائه کرد که وضعیت استخدامی و صلاحیت ورود به‌کارکردهای اجرایی را تأیید می‌کند (T. Kent, op.cit: 33).

این بخش از فرایند احراز هویت نیز از منظر استنادپذیری ادلهٔ الکترونیکی، اهمیت اساسی دارد. ابزارها و شیوه‌هایی که برای شناسایی، تأیید و تجویز هویت، براساس شناسه / ویژگی‌ها به‌کار می‌روند، باید در حد منطقی اطمینان‌پذیر باشند. حساسیت این مراحل باعث شده است که قانون‌گذاران، به اصول و موازین کلی اکتفا نکرده و حتی در مورد ابزارهای کاربردی نیز تعیین تکلیف کنند.

۲. ابزارهای احراز هویت پدیدآورندهٔ داده‌های الکترونیکی

به‌طور کلی، برای تولید ابزارهای احراز هویت پدیدآورندگان اطلاعات، از جمله داده‌های الکترونیکی، بر روی سه نوع شناسه / ویژگی تمرکز می‌شود:

- آنچه شخص می‌داند، مانند: گذرواژه (password)؛
- آنچه شخص دارد (به وی اعطا می‌شود)، مانند: کارت‌های هوشمند؛
- آنچه در وجودش هست، مانند: اثر انگشت و عنبیهٔ چشم.

اما ابزاری که به‌طور خاص نظر قانون‌گذاران کشورها را به خود جلب کرده است، امضای الکترونیکی (electronic signature) است (بختیاروند، ۱۳۸۳: ۵۵). همانطور که در دنیای فیزیکی، امضا به عنوان یک نشانهٔ ابراز هویت در اطلاعات مستند، رسمیت یافته است، متخصصان فناوری اطلاعات کوشیده‌اند با آزمون برنامه‌های اطمینان‌بخش،

سازوکار مشابهی را در مورد مستندات الکترونیکی ایجاد کنند. قدری دقت در شناسه / ویژگی‌هایی که تاکنون به آنها اشاره شد، نشان می‌دهد که اکثر آنها، به‌ویژه در سطح گسترده و در مناسبات شبکه‌ای، این قابلیت را ندارند و هر یک با محدودیت‌های جدی مواجه‌اند. برای مثال، با اینکه عنبیهٔ چشم اطمینان‌پذیری بالایی دارد، اما هزینهٔ آن بسیار بالاست و نمی‌توان در حجم انبوه به‌کار برد.

از سوی دیگر، گزینه‌هایی که هزینهٔ چندانی ندارند، ولی هم‌اکنون در سطح گسترده‌ای به‌کار گرفته شده‌اند، با نقاط ضعف دیگری مواجه‌اند و نمی‌توانند همهٔ انتظارات نظام ادلهٔ اثبات، به‌ویژه در امور کیفری را برآورده سازند. برای مثال، با اینکه گذرواژه به یک فرد تعلق می‌یابد و می‌تواند در احراز هویت مناسب باشد، ولی نسبت به اعتبار داده‌های الکترونیکی اثر چندانی ندارد. بنابراین ابزاری کارآمد است که در عین حفظ هویت فردی، اعتبار داده‌ها را هم تضمین می‌کند.

این مهم به مدد فناوری رمزنگاری (cryptography) محقق شده است. در اینجا فرد می‌تواند داده‌های خود را رمزگذاری (encryption) کند و متن خود را به یک رمزنوشته (cipher text) تبدیل کند. بنابراین، نه تنها تمامیت داده‌ها تضمین می‌شود، بلکه از آنجا که کلید (key) اعطا شده جنبهٔ انحصاری دارد، به نوعی امضای دارندهٔ آن نیز به شمار می‌آید و هویتش را اثبات می‌کند. سپس هنگامی که داده‌های رمزگذاری شده به دریافت‌کننده می‌رسد، با کلید رمزگشایی (decipher) که دارد، متن اصلی (plain text) را بازیابی می‌کند (قاجار قیونلو، ۱۳۸۱: ۲۲).

این ابزارها با وجود دقت بسیار بالا از لحاظ اطمینان‌پذیری، به درجاتی تقسیم شده‌اند. گزینه‌ای که عموماً مورد توجه قانون‌گذاران کشورها واقع شده است، امضای الکترونیکی مطمئن (secure electronic signature) است. برای مثال، قسمت ٤,٣١ اصلاحیِ قانون حمایت از اطلاعات شخصی و اسناد الکترونیکی کانادا، مصوب ۲۰۰۰، (personal information protection and electronic documents act, S.C. 2000) با عنوان «فروض راجع به امضاهای الکترونیکی مطمئن» مقرر داشته است:

رئیس شورا می‌تواند در خصوص فروض دلیل‌انگاری (evidentiary presumption) اسناد الکترونیکی، که با امضاهای الکترونیکی مطمئن امضا شده‌اند، مقرراتی را وضع

کند. از جملهٔ این مقررات، عبارتند از: الـف. رابطـهٔ امـضاهای الکترونیکـی مطمـئن بـا اشخاص؛ ب. تمامیت اطلاعات موجود در اسناد الکترونیکیِ امـضا شـده، بـا امـضاهای الکترونیکی مطمئن (Gahtan, 1999: 162).

در اینجا علاوه بر هویت، به تمامیت که عامل اصلی اعتبار داده‌هـای الکترونیکـی و موضوع بحث قسمت بعد است نیز اشاره شده است.

از میان پرونده‌های کیفری، چندین نمونه قابل ذکر است، که متهمان کوشـیده‌انـد بـا زیر سؤال بردن هویت دارندهٔ داده‌های الکترونیکی، در استنادپذیری آنهـا تردیـد ایجـاد کنند. برای مثال، در دعوای ایالات متحده علیه سیمپـسون (U.S. v. Simpson, 1998)، مقامات تعقیب، به دنبال اثبات این موضـوع بودنـد کـه مـتهم در محـیط گفـت‌وگـوی اینترنتی‌ای که به هرزه‌نگاری کودکان اختصاص داشت، بـا مـأمور مخفـی FBI ارتبـاط برقرار کرده است. پلیس از گفت‌وگوی اینترنتی کـه بـین مـأمور و آن شـخص کـه نـام مستعارش استاورن (Stavron) بود، یک پرینت ارائه کرد. دادگاه ناحیه پذیرفت کـه بـه این پرینت، در میان دیگر ادله در محاکمه، استناد شود. در مرحلهٔ تجدیدنظر که به دنبال محکومیت متهم مطرح شد، سیمپسون چنین استدلال کرد:

> از آنجا که مجریان قانون نتوانستند تشخیص دهند اظهارات منتسب به وی همان بـوده که از دست‌خط یا شیوهٔ نگارش یا صدایش به‌دسـت آمـده، پـس نـسخهٔ چـاپی معتبـر نیست و باید از عداد دلایل خارج شود.

شعبهٔ دهم دادگاه سیّار (10th circuit court) این استدلال را نپذیرفت و متذکر شـد، ادلهٔ قابل توجهی از شرایط و اوضاع و احوال وجود دارد که نشان می‌دهد مـتهم، خـود «استاورن» است. زیرا برای مثال، استاورن به مأمور مخفی گفته بـود کـه نـام واقعـی‌اش «بی. سیمپسون» است و آدرس منزلش را ضمیمهٔ نامش کـرده و از طریـق اعتبـاری، بـه اینترنت دسترس یافته است که به نام سیمپسون ثبت شده است. علاوه بر این، پلـیس از منزل وی سوابقی کشف کرده که حاوی نام، آدرس و شمارهٔ تلفن مأمور مخفی‌ای بوده است که برای استاورن فرستاده بود. به این ترتیب، دادگاه احراز کرد که مجریان قـانون دلایل کافی ارائه کرده‌اند که از موضع اتهامی استاورن دفاع می‌کند و پرینت تهیـه شـده نیز معتبر است (Department of Justice of the United States, 2002: 88).

مسئلهٔ بسیار مهم دیگری که دربارهٔ احراز هویت پدیدآورندهٔ داده‌های الکترونیکی، به‌ویژه در امور کیفری مطرح است، حمایت از داده‌های شخصی (personal data protection) آنهاست. بنابراین هرچه داده‌های شخصی بیشتری در فرایند احراز هویت به‌کار گرفته شوند، ضریب موفقیت فنون و ابزارهای به‌کار رفته، بیشتر خواهد بود، ولی به همان نسبت، ملاحظات راجع به حریم خصوصی (privacy) نیز برانگیخته می‌شود. این امر باعث شده است، در کشورهای توسعه‌یافته، ضوابطی به اجرا درآید که در عین رعایت قواعد ناظر بر احراز هویت پدیدآورندگان داده‌های الکترونیکی، به حریم داده‌های شخصی آنها نیز تعرض نشود (T. Kent, op.cit: 55).

گفتار دوم: اعتبار ادلهٔ الکترونیکی

دومین اصلی که رعایت آن در کنار احراز هویت پدیدآورندهٔ داده‌های الکترونیکی موجب استنادپذیری آنها می‌شود، اعتبار (authenticity) است. برخی به لحاظ جایگاه انکارناپذیر اصل داده‌ها (genuineness)، این واژه را «اصالت» معنا کرده‌اند. شکی نیست که در مورد اطلاعات فیزیکی، این مسئله صادق است و این تطابق مفهومی وجود دارد، اما باید دید، در رابطه با داده‌های الکترونیکی تا چه حد قابل اتّکاست. به عبارت دیگر، آیا در اینجا نیز باید اصل داده‌ها مطالبه شود و اصولاً چنین چیزی امکان‌پذیر و منطقی است یا باید قواعد و فرایند جدیدی را بنیان نهاد؟

در مقدمه اشاره شد که فناوری اطلاعات و ارتباطات، قانون‌گذاران نظام حقوق عرفی را به تکاپوی جدی‌تری واداشته است. زیربنای نظام ادلهٔ اثبات حقوق عرفی را دو قاعدهٔ «بهترین دلیل» و «ادلهٔ سماعی» تشکیل می‌دهند. لذا نحوهٔ رویارویی آنها با داده‌های نوظهور الکترونیکی، نکات آموزنده‌ای در پی دارد.

۱. قاعدهٔ بهترین دلیل

این قاعده (the best evidence rule) ادلهٔ مستند (documentary evidence) را هدف قرار می‌دهد. هدف اصلی از وضع آن هم این بوده که، دقت و صحت رسیدگی‌ها را فقط با مراجعهٔ به اصل مستندات، تضمین کند. به همین دلیل از پذیرش مستنداتِ به اصطلاح دست دوم، مانند کپی یا گواهی، جلوگیری می‌شده است.

در گذشته ابزارهای کپی وجود نداشت و تنها راه تکثیر، رونوشت‌برداری از اصل بود که به دلیل خطای بشری، احتمال نقصان سند، دور از انتظار نبود. اما به مرور زمان و با تولید دستگاه‌های پیشرفتهٔ کپی‌برداری، به تدریج از میزان دغدغه‌ها کاسته شد و اسناد کپی، در کنار اسناد اصل، جایگاه خود را به‌دست آوردند (Gahtan, op.cit: 151).

انعطاف‌پذیری نظام حقوق عرفی، به دلیل پایبندی به اصول بنیادین؛ مانند ضرورت (necessity)، تناسب (proportionality) و انصاف (fairness)، باعث شد اینگونه قواعد حقوقی متناسب، با تحول جامعه سازگاری یابند و محاکم را از بلاتکلیفی رها سازند.

با این حال، باید برای برخی مسائل مربوط به داده‌های الکترونیکی، چاره‌جویی اساسی صورت می‌گرفت. واقعیت این است که آنچه در یک رسانهٔ ذخیره‌ساز الکترونیکی قرار دارد، با آنچه به عنوان خروجی مشاهده می‌شود، یکسان نیستند. در سیستم رایانه‌ای، مجموعه‌ای از صفر و یک، براساس الگوریتم‌های دقیق ریاضی، پردازش و ذخیره می‌شوند. اما آنچه به نمایش درمی‌آید و چاپ می‌شود؛ متن، صدا، تصویر، نمودار و... است. بنابراین سؤال اصلی این است که: خروجی یک سیستم رایانه‌ای، اصل داده‌هاست یا کپی آن؟ اگر اصل است، تکلیف صفر و یک‌ها چیست و اگر کپی است، چه نسبتی با منشأ خود دارد؟

وجود اینگونه مسائل اساسی جدید، باعث جدا شدن حساب داده‌های الکترونیکی از مستندات فیزیکی شده است. زیرا از دنبال کردن وجوه تشابه احتمالی و تسری قواعد مربوط به این دسته، نتیجهٔ قابل قبولی به‌دست نمی‌آید. قانون‌گذار باید خودش وارد عمل شود و برای اصالت داده‌های الکترونیکی چاره‌جویی کند؛ که چنین نیز شده است. برای مثال، قسمت (۳) ۱۰۰۱ مقررات فدرال، راجع به ادلهٔ ایالات متحده (U.S. Federal Rules of Evidence)، پرینت‌های رایانه‌ای را به‌طور صریح در حکم اصل قرار داده است. مطابق این قسمت، یک سند تکثیر شده (duplicate)، به اندازهٔ اصل، استنادپذیر است مگر اینکه:

۱. نسبت به اعتبار اصل، ایرادی اساسی مطرح شود؛

۲. مطابق شرایط و اوضاع و احوال، پذیرش سند تکثیر شده به جای اصل، غیرمنصفانه باشد.

در ادامه هم آمده است:

اگر داده‌ها در رایانه یا دستگاه مشابهی ذخیره شده باشد، هرگونه خروجی چاپی یا دیگر خروجی‌های قابل خواندن با چشم، که داده‌ها را به دقت منعکس می‌کند، اصل (original) محسوب خواهد شد.

به تبع این ضابطهٔ فدرالی، ایالت‌های این کشور نیز قوانین خود را اصلاح کرده‌اند. برای مثال، قانون ادلهٔ کالیفرنیا (California Evidence Act) مصوب ۱۹۸۳، در بخش جدید 1500.5 اصلاحی خود مقرر کرده است:

اطلاعات ضبط شدهٔ رایانه‌ای یا برنامه‌های رایانه‌ای یا کپی اطلاعات ضبط شدهٔ رایانه‌ای یا برنامه‌های رایانه‌ای، نباید براساس قاعدهٔ بهترین دلیل، استنادناپذیر تلقی شوند.

در چارچوب این نظام، برخی دیگر، تسری این قاعده را به رعایت شیوه‌ها و به‌کارگیری ابزارهای خاصی منوط کرده‌اند. در فوق به قانون ادلهٔ کانادا اشاره شد و تأکید آن بر امضای الکترونیکی مطمئن، احراز شد. در زیربخش ۲,۳۱ با عنوان «اجرای قاعدهٔ بهترین دلیل» آمده است:

۱. «قاعدهٔ بهترین دلیل» نسبت به اسناد الکترونیکی، در موارد زیر رعایت شده محسوب می‌گردد:

الف. تمامیت سیستم اسناد الکترونیکی که سند الکترونیک در آن یا به‌وسیلهٔ آن ضبط یا ذخیره شده است، به اثبات رسد؛

ب. فرض دلیل‌انگاری مقرر در زیربخش ٤,۳۱ به اجرا درآید.

پیش از این اشاره شد که زیربخش مذکور، به پیش‌فرض‌های مربوط به امضاهای الکترونیکی مطمئن اختصاص دارد. قسمت دوم آن هم با عنوان «پرینت‌ها» چنین مقرر می‌کند:

علاوه بر موارد مندرج در قسمت (۱)، در صورت عدم وجود ادلهٔ مغایر، یک سند الکترونیکی در قالب پرینت، در صورتی که به عنوان سابقهٔ اطلاعات ضبط یا ذخیره شده، در پرینت به‌طور آشکار یا منظم مورد اقدام، استناد یا استفاده قرار گیرد، مطابق قاعدهٔ بهترین دلیل خواهد بود.

۲. استنادناپذیری ادلهٔ سماعی

در نظام حقوق عرفی، برای اینکه ادلهٔ ارائه شده به دادگاه از اعتبار بالایی برخوردار باشند، تنها در صورتی پذیرفته می‌شوند که شخص براساس علم یا آگاهی خودش آن

را به‌دست آورده باشد. بنابراین آگاهی ناشی از منابع ثانویه مانند دیگر اشخاص، کتابها یا سوابق، در مجموع در قالب ادلهٔ سماعی (hearsay evidence) قرار می‌گیرند که معتبر و استنادپذیر نیستند. در این رابطه، قسمت 801(c) مقررات فدرال، راجع به ادلهٔ ایالات متحده چنین مقرر کرده است:

ادلهٔ سماعی، هرگونه ادعا از سوی کسی جز اظهارکنندهٔ آن، به هنگام شهادت در محاکمه یا استماع است که به عنوان دلیل ابراز می‌شود تا صحت مدعی‌به را ثابت کند.*

با این حال، اجرای بی‌چون و چرای این قاعده، به‌ویژه در عصر حاضر و نسبت به جلوه‌های نوین اطلاعات، منطقی به نظر نمی‌رسد و به همین دلیل با توجه به اصول پیش‌گفته، موارد استثنای مهمی بر این قاعده وارد شده است.

در رابطه با موضوع این نوشتار و این استثنائات می‌توان به: سوابق شغلی، پذیرش طرف مقابل و سوابق الکترونیکی صِرف اشاره کرد.

الف. استثنای سوابق شغلی (business records exception)

در توجیه این استثنا، دادگاه (کیفری) پروندهٔ ایالات متحده علیه اشنایدر (U.S. v. Snyder: 1986) مطلب جالب توجهی را بیان کرده است:

استثنای سوابق شغلی، مبتنی بر فرض دقت است. زیرا اطلاعات، بخشی از یک فعالیت متداول را تشکیل می‌دهد و کسانی از آنها نگهداری می‌کنند که دقت در کار را آموزش دیده‌اند و به صورت یک عادت آن را انجام می‌دهند و به‌طور منظم آن را از لحاظ درستی بررسی می‌کنند. زیرا دقت فعالیت شغلی، مستلزم دقت در تهیهٔ این سوابق است (Gahtan, op.cit: 141).

از این رأی می‌توان چند ضابطه را استخراج کرد: ۱. سابقه باید در جریان متداول شغلی ایجاد شده باشد؛ ۲. سابقه باید توسط شخصی که از آن اطلاعات آگاهی دارد ایجاد شده باشد؛ ۳. سابقه باید به هنگام یا نزدیک به زمان تحصیل اطلاعات ایجاد شده باشد (Ibid: 147).

تاکنون براساس این استثنا، به داده‌های الکترونیکی گوناگونی ترتیب اثر داده شده است، از جمله: در دعوای ایالات متحده علیه لین (U.S. v. Linn: 1989)، سوابق رایانه‌ای قبض

* http://www.law.cornell.edu/rules.htm.

تلفن پذیرفته شد. در دعوای ایالات متحده علیه بونالو(U.S. v. Bonallo: 1988)، خلاصه مبادلات ATM پذیرفته شد. در دعوای ایالات متحده علیه اسکول (U.S. v. Scholle: 1977)، پرینت رایانه‌ای تجزیه و تحلیل آزمایشگاهی مواد مخدر پذیرفته شد (Ibid).

در همین رابطه، بخش 69(a) قانون پلیس و ادلهٔ کیفری انگلستان (The Police and Criminal Evidence Act) مصوب ۱۹۸٤ آمده است:

ادعای موجود در یک سند رایانه‌ای، در صورتی قابل استناد است که علاوه بر شرایط کلی استنادپذیری اسناد، ضوابط ذیل نیز در خصوص آنها رعایت شده باشد:

- هیچ‌گونه زمینهٔ متعارفی مبنی بر بروز این اعتقاد وجود نداشته باشد که آن اظهار به دلیل استفادهٔ ناشایست از رایانهٔ مورد نظر، دقیق نیست؛
- رایانهٔ مورد نظر در تمام مدت، به‌طور مناسب کار می‌کرده و چنانچه به هر دلیل کارکرد مناسب نداشته یا از کار افتاده است، در تولید این سند یا دقت محتوای آن خللی ایجاد نکرده است؛

و... (Gahtan, Ibid: 165).

ب. استثنای پذیرش طرف دعوا

این استثنا هم ریشه در دنیای فیزیکی دارد و بر این مبنا مطرح می‌شود که اگر دلیلی توسط طرف دعوا به وجود آید، علیه خودش قابل استناد است. زیرا نوعی اقرار به شمار می‌آید و معتبر است. قاعدتاً یک انسان عاقل وقایعی را که به وضعیت قانونی‌اش لطمه بزند یا مسئولیتی را متحمل شود نخواهد پذیرفت، مگر اینکه آن وقایع صحیح باشند. همچنین می‌توان به دلایل ایجاد شده توسط فردی که هیچ نقشی در دعوای مورد نظر ندارد و تحت نظر طرف ذی‌نفع دعوا، ادله را ایجاد نکرده باشد، استناد کرد (Ibid: 148).

در رابطه با اجرای این قاعده نسبت به ادلهٔ الکترونیکی، قسمت‌های دوم و سوم زیربخش ۳,۳۱ پیش‌گفتهٔ قانون اصلاحی ادلهٔ کانادا مقرر می‌دارند:

... ب. چنانچه اثبات شود سند الکترونیکی توسط طرفی ضبط یا ذخیره شده که منافع آن در تعارض با طرفی است که قصد دارد آن را ارائه دهد؛ یا ج. چنانچه اثبات شود سند الکترونیکی توسط شخصی که طرف دعوا محسوب نمی‌شود و آن را تحت کنترل طرف دعوایی که قصد ارائهٔ آن را دارد، ضبط یا ذخیره نکرده است، در جریان متداول و عادی شغلی، ضبط یا ذخیره شده باشد.

ج. استثنای سوابق رایانه‌ای صِرف

این استثنا برخلاف دو استثنای قبل، ریشه در دنیای فیزیکی ندارد و برآمده از ویژگی‌های خاص سوابق الکترونیکی است. برای درک آن لازم است به مفهوم ادلهٔ سماعی توجه شود. آنها از ذهنیت بشر نشأت می‌گیرند و به همین دلیل برای جلوگیری از ورود اظهارات غیرقابل اطمینان به نظام دادرسی استنادپذیر نیستند. بنابراین چنانچه یک دلیل از حیوان یا دستگاه ناشی شود، در این تعریف نمی‌گنجد. بند الف مادهٔ ۸۰۱ مقررات فدرال، راجع به ادلهٔ ایالات متحده، اظهار (statement) را چنین تعریف می‌کند:

> سخن کتبی یا شفاهی یا یک ارتباط بی‌کلام از شخص، که قصد ادای آن به عنوان سخن را دارد.

همچنین، در بند ب این مادّه اظهارکننده کسی است که سخن را ادا می‌کند (Department of Justice of the United States, 2002: 83).

اما در خصوص دلایل و سوابق الکترونیکی، برای شناسایی مصادیق، رویکردهای متفاوتی دنبال شده‌اند. برای مثال، وزارت دادگستری ایالات متحده، سوابق الکترونیکی دارای متن را در سه دسته قرار داده است: ۱. سوابق دارای منشأ رایانه؛ ۲. سوابقی که فقط در رایانه نگهداری یا ذخیره شده‌اند؛ ۳. سوابقی که از ماهیت هر دو سوابق اول و دوم برخوردارند (Ibid: 85). برای مثال، پیام‌های پست الکترونیکی، فایل‌های واژه‌پرداز (Word) و پیام‌های محیط گفت‌وگو، مثال‌های رایجی از سوابق ذخیره شدهٔ رایانه‌ای هستند. اما سوابق دارای منشأ رایانه، خروجی برنامه‌های رایانه‌ای هستند که بشر در تولید آنها دخالتی ندارد، مانند سوابق ناشی از برقراری ارتباط با شبکه نزد ارائه‌دهندهٔ خدمات اینترنتی، سوابق تلفن و ورودی‌های ATM. این برنامه‌ها به گونه‌ای طراحی شده‌اند که طی فرایند الگوریتمی خاص، یک سری نتایج را ارائه دهند. در خصوص طبقهٔ سوم نیز می‌توان به جرم کلاهبرداری اشاره کرد که از یک برنامهٔ رایانه‌ای صفحه گسترده (spreadsheet) جهت پردازش طرح‌های مالی مرتبط با کلاهبرداری استفاده می‌کند. سابقهٔ رایانه‌ای که خروجی برنامه را تشکیل می‌دهد، هم شامل اظهارات بشری (داده‌هایی که متهم به برنامهٔ صفحهٔ گسترده وارد کرده است) و هم شامل پردازش رایانه‌ای (عملکردهای ریاضی این برنامه) می‌شود.

فصل دوم: قواعد خاص ناظر بر استنادپذیری ادلهٔ الکترونیکی

برخلاف نظام ادلهٔ اثبات در امور مدنی، در نظام عدالت کیفری علاوه بر کنش‌گران اصلی جرم، یعنی بزهکار و بزهدیده، ذی‌نفعان جدی دیگری هم حضور دارند؛ مجموعهٔ عواملی که از آنها به عنوان مجریان قانون (law enforcement) یاد می‌شود و به مقامات قضایی و در رأس آن به دادستان، در کشف حقیقت کمک می‌کنند.

به همین منظور به آنها اختیاراتی تفویض شده است تا بتوانند در انجام وظایفشان ابتکار عمل لازم را به خرج دهند، اما در عین حال برای اینکه از اختیارات قانونی‌شان سوء استفاده نکنند، تضمین‌هایی نیز پیش‌بینی شده است. تا حدی که در صورت عدم رعایت مقررات، ادلهٔ ارائه شده، بی‌اعتبار خواهند بود (آشوری، ۱۳۸۰: ۲۲۳).

با توجه به این مسائل، باید دید مجریان قانون چگونه با داده‌های الکترونیکی، به منزلهٔ ادلهٔ استنادپذیر کیفری مواجه می‌شوند. به‌ویژه آنکه همهٔ صاحب‌نظران حقوق کیفری معتقدند، این فناوری، نظام آئین دادرسی کیفری به‌ویژه بخش کشف علمی جرایم را به کلی متحول کرده است و حوزهٔ جدید، نیازمند ضوابط و دستورالعمل‌های جدیدی است. به همین دلیل، بخش عمده‌ای از سیاست‌گذاری‌های کیفری‌ای که تاکنون در دستور کار کشورها قرار گرفته است، به این بخش تعلق داشته است. برای احراز این مسئله، کافی است دو بخش ماهوی و شکلی کنوانسیون جرایم سایبر، از لحاظ کمّی و کیفی و از آن مهم‌تر، الزام کشورها به تحقق آنها و عدم پذیرش هرگونه حق شرط، با یکدیگر مقایسه شوند.

با وجود مسائل گوناگون و مفصلّی که در این رابطه قابل بحث و بررسی است، در این فصل به اختصار قواعد علوم قانونی و حقوقی ناظر بر اقدامات مجریان قانون مطرح می‌شود.

گفتار اول: قواعد علوم قانونی ناظر بر اقدامات مجریان قانون

به‌طور کلی، هستهٔ اصلی فعالیت‌های مجریان قانون را علوم قانونی (forensic science) شکل می‌دهد. این دانش، اصول و فنونی را که جهت تسهیل تحقیق (investigation) و تعقیب (prosecution) جرایم به‌کار می‌رود، ارائه می‌دهد. در یک نگاه، می‌توان علوم

قانونی را جلوهٔ کاربردی قانون دانست. به عبارت دیگر، هر اصل یا فنی کـه بتوانـد بـه شناسایی، بازیابی، بازسازی یا تجزیه و تحلیل ادله، در جریان تحقیقات کیفری کمک کند، در زمرهٔ علوم قانونی قـرار مـی‌گیـرد. در اینجـا اصـول و قواعـدی منطقـی نیـز پی‌ریزی مـی‌شـود. اصـل تبـادل لوکـارد (Locard's exchange principle) از جملـهٔ آنهاست. طبق این اصل هر شخص یا شیئی که وارد صحنهٔ جرم می‌شود، چیزهایی از آن را به خود می‌گیرد و هنگامی که از آن جدا می‌شـود، چیزهـایی از آن را بـا خـود می‌برد (کیسی، همان: ۱۸).

در رابطه با علوم قانونی ناظر بر فناوری اطلاعات و ارتباطات، به‌طور کلی دو حوزهٔ «سیستم‌های رایانه‌ای» و «فضای شبکه‌ای» از یکدیگر قابل تفکیک‌انـد. زیـرا عـلاوه بـر مسائل فنی ـ اجرایی، از لحاظ موازین حقوقی نیز موضوعات متمایزی را دربرمی‌گیرند. نمونهٔ آشکار آن، گسترهٔ عملکرد مجریان قانون است. با اینکه از فضای سایبر به عنـوان یک دنیای بدون مرز یاد می‌شود، اما به معنای بی‌ضابطگی آن نیست. اگر مجریان قانون بخواهند از طریق شبکه‌های رایانه‌ای، به داده‌های واقع در سیستم‌های رایانـه‌ای مـستقر در دیگر کشورها دسترس یابند، به قلمرو حاکمیتی آنها تعرض می‌شود.*

طبق ضوابط علـوم قـانونی، بـرای اینکـه دلایـل ابـرازی از سـوی مجریـان قـانون استنادپذیر باشند، باید زنجیرهٔ حفاظتی (chain of custody) در مورد آنها رعایت شـده باشد. به این معنـا کـه، چهـار مرحلـهٔ پیوسـتهٔ: ۱. شناسـایی (recognition)؛ ۲. محافظـت (preservation)، جمع‌آوری (collection) و مستندسازی (documentation)؛ ۳. طبقه‌بندی (classification)، مقایـسه (comparison) و ماهیـت‌انگـاری (individualization)؛ و ٤. بازسازی (reconstruction)، به اجرا درآید (همان: ۸۵).

* برای مثال، در بند ۲ مادهٔ ۱۹ کنوانسیون تفتیش و توقیف داده‌های رایانه‌ای ذخیره شده اینگونـه آمـده است: «...۲. هر یک از اعضاء باید به گونه‌ای اقدام به وضع قوانین و دیگر تدابیر کنند که در صـورت لزوم، این اطمینان را بدهند؛ در جایی که مقامات ذی‌صلاح آنها، سیستم رایانه‌ای یـا بخـشی از آن را مطابق بند ۱ (الف) مورد تفتیش یا دسترس مشابه قرار می‌دهند و زمینـه‌هـای موجـد ایـن اعتقـاد در اختیار دارند که دادهٔ مورد نظـر آنهـا در سیـستم رایانـه‌ای دیگـر یـا بخـشی از آن در منطقـهٔ تحـت قلمروشان قرار دارد و داده‌های مذکور به‌طور قانونی از سیستم اولیـه قابـل دسـترس اسـت، بتواننـد هرچه سریع‌تر دامنهٔ تفتیش یا دسترس مشابه را نـسبت بـه سیـستم ثانویـه گـسترش دهنـد» (مرکـز پژوهش‌های مجلس شورای اسلامی، همان: ۲٦).

۱. اجرای ضوابط علوم قانونی بر روی سیستمهای رایانه‌ای

یادآور می‌شود، منظور از سیستم‌های رایانه‌ای «هر دستگاه یا مجموعه‌ای از دستگاه‌های مرتبط یا متصل به یکدیگر است که یک یا چند تا از آنها، مطابق یک برنامه، پردازش خودکار داده‌ها را انجام می‌دهند» (مادهٔ ۱ کنوانسیون جرایم سایبر). بنابراین باید نگاه خود را از رایانه‌های رومیزی (desktop computers) و قابل حمل (laptop) فراتر برد.

شروع فرایند زنجیرهٔ حفاظتی با شناسایی است:

الف. شناسایی

این مرحله شامل دو قسمت «سخت‌افزار» و «داده‌های رایانه‌ای» می‌شود. ابتدا باید هر نوع دستگاهی که یک سیستم رایانه‌ای به شمار می‌آید و همچنین کلیهٔ رسانه‌های ذخیره‌ساز الکترونیکی، مانند لوح‌های فشرده را که با جرم ارتکابی مرتبط می‌باشند، شناسایی کرد. سپس باید برای داده‌های الکترونیکی اقدام کرد. البته این به معنای نادیده انگاشتن اطلاعات فیزیکی نیست. نکتهٔ مهم این است که در عین حفظ نگاه جامع به حوزهٔ تحقیق، از اطلاعات غیرمرتبط چشم‌پوشی کرد.

ب. محافظت، جمع‌آوری و مستندسازی

پاشنهٔ آشیل زنجیرهٔ حفاظتی در این مرحله نهفته است. اگر مجریان قانون از دلایل گردآوری شده، به نحوی حفاظت نکنند که در دادگاه وضعیت اصلی‌شان را انعکاس دهند و همچنین، مشخصات هر یک به انضمام مأموران دست‌اندرکار، در فرم‌های مخصوص به‌طور کامل درج نشده باشد، استنادپذیری‌شان با تردید جدی مواجه خواهد شد.

ج. طبقه‌بندی، مقایسه و ماهیت‌انگاری

طبقه‌بندی ادله، فرایندی است که براساس آن ویژگی‌هایی کشف می‌شود و می‌توان از آن جهت بیان موضوعات کلی استفاده کرد و از میان نمونه‌های مشابه تمیز داد. یکی از مزایای بزرگ طبقه‌بندی ادلهٔ الکترونیکی، احراز هویت پدیدآورندگان آن است. اما مقایسهٔ قسمتی از ادلهٔ دیجیتال با یک نمونهٔ تحت کنترل، علاوه بر آشکار ساختن

ویژگی‌های مربوط به یک طبقه مانند شمارهٔ شناسایی مرتبط با یک رایانه، ابعاد منحصر به فردی از آن را که به ابعاد ماهیت‌انگار نیز موسوم است، پدیدار می‌سازد.

د. بازسازی

بازسازی ادلهٔ الکترونیکی، دو وجه متمایز اما مرتبط دارد: ۱. بازسازی ادلهٔ غیرقابل استفاده؛ ۲. به‌کارگیری ادله در بازسازی جرم (کیسی، همان: ۱۱۳). ادلهٔ الکترونیکی غیرقابل استفاده، ادلهٔ پاک شده، آسیب‌دیده، پنهان و یا رمزگذاری شده است. در مقدمه اشاره شد که یکی از ویژگی‌های داده‌های الکترونیکی این است که به سختی می‌توان آنها را از بین برد. امروزه دستگاه‌های پیشرفته‌ای در اختیار متخصصین و مجریان قانون قرار گرفته است که می‌توانند ادلهٔ غیرقابل استفاده را بازیابی کنند. پیشرفت این حوزه به حدی است، که سایهٔ داده‌ها (shadow data) را که در نتیجهٔ بی‌دقتی جزئی بازوی نگارش‌کنندهٔ داده‌ها بر روی دیسک ایجاد می‌شوند، شناسایی و نوع و ماهیت آن را مشخص می‌کنند. به این ترتیب، هرچه داده‌ها روی‌هم‌نویسی (overwrite) شوند، باز هم با به‌کارگیری دستگاه‌های پیشرفته مانند میکروسکوپ‌های کاوشگر اسکن‌کننده یا میکروسکوپ‌های مغناطیسی، می‌توان تکه‌های دست‌نخوردهٔ داده‌ها را شناسایی کرد و با کنار هم قرار دادن آنها، به محتوای اصلی دست یافت.

۲. اجرای ضوابط علوم قانونی بر روی شبکه‌های رایانه‌ای

برای اینکه مجریان قانون وظایف خود را در فضای شبکه‌ای به نحو قابل قبولی انجام دهند، باید با ماهیت و سازوکار آن آشنایی کافی داشته باشند. براساس مدل مرجع OSI (open system interconnection)، محیط شبکه به هفت لایه تقسیم شده است (همان: ١٤٤):

۱. لایهٔ اجرا (application layer): برقراری ارتباط میان اشخاص و شبکه‌ها را فراهم می‌سازد و به آنها امکان تبادل پست الکترونیک، مشاهدهٔ صفحات وب و بسیاری از کارکردهای دیگر شبکه‌ای را می‌دهد. بدون این لایه نمی‌توان به شبکه‌ها دسترس داشت.

۲. لایهٔ نمایش (presentation layer): در صورت لزوم، داده‌ها را قالب‌بندی می‌کند و تغییر می‌دهد تا بتواند استانداردهای قراردادی رایانهٔ خاصی که مورد استفاده قرار

گرفته را رعایت کند. این تغییر قالب از آن جهت ضرور می‌نماید که رایانه‌ها به یک شکل طراحی و تولید نمی‌شوند تا بتوان به یک شکل با آنها ارتباط برقرار کرد.

۳. لایهٔ جلسه (session layer): گفتگو میان رایانه‌ها، برقراری، استمرار، اداره و نحوهٔ پایان دادن ارتباطات را هماهنگ می‌کند. برای مثال، این لایه تأیید می‌کند که دستورالعمل‌های پیشین، توسط شخصی ارسال شده که پیش از آنکه دستورالعمل بعدی را ارسال کند، به‌طور موفقیت‌آمیز عملکرد خود را انجام داده است.

٤. لایهٔ انتقال (transport layer): مدیریت ارسال داده‌ها را به عهده دارد و تقریباً مشابه لایهٔ جلسه عمل می‌کند. برای مثال، ارتباط میان رایانه‌ها را برقرار و اداره می‌کند، استمرار می‌بخشد و به پایان می‌رساند. بدون این لایه، اجرای عملیات‌های پیچیده بر روی شبکه با مشکلات بسیاری همراه است و دیگر نمی‌توان با رایانه‌های دوردست ارتباط برقرار کرد.

۵. لایهٔ شبکه (network layer): بسیار شبیه خدمات پستی عمل می‌کند. یعنی موظف است اطلاعات را مسیریابی کند و با استفاده از آدرس آنها، مقصدشان را مشخص کند. به این منظور، دستورالعمل‌های ویژه‌ای را بر روی پیام مورد نظر پیاده می‌کند تا بتواند با عبور از رایانه‌های واسط، از نقطه‌ای به نقطهٔ دیگر منتقل شود.

٦. لایهٔ پیوند ـ داده (data-link layer): مسئولیت برقراری یک ارتباط اساسی میان رایانه‌های نزدیک به هم را به عهده دارد. برای مثال، زمانی که دو رایانه به وسیلهٔ یک سیم به یکدیگر متصل‌اند، این لایه امکان انتقال داده‌ها از طریق آن سیم را فراهم می‌آورد. بنابراین، کار آن شبیه لایهٔ شبکه است، ولی ساده‌تر از آن عمل می‌کند. بدون این لایه، داده‌ها از لایه‌های فوق فرو می‌افتند و به نقطهٔ نامعلومی می‌رسند. بنابراین رایانه‌ها نمی‌توانند با یکدیگر ارتباط برقرار کنند.

۷. لایهٔ فیزیکی (Physical Layer): همان وسیله یا رسانهٔ واقعی است که مانند سیم‌های تلفن، کابل‌های فیبر نوری و ارسال‌های ماهواره‌ای، داده‌ها را انتقال می‌دهد. این لایه، با آنچه انتقال می‌یابد هیچ ارتباطی ندارد، ولی بدون آن، هیچ‌گونه ارتباطی میان رایانه‌ها برقرار نخواهد شد.

لایهٔ اجرا، به لحاظ موقعیت خاصی که دارد، حجم عمده‌ای از ادلهٔ دیجیتال را در

خود جای داده است. لایهٔ نمایش، از این بابت چندان ارزشمند نیست. لایـهٔ جلـسه، بـا اینکه جذابیت و اهمیت زیادی دارد، اما از لحاظ ادله، منبع غنی و مهمی تلقی نمی‌شود. لایهٔ انتقال، همانند لایهٔ اجرا، به لحاظ موقعیت خاص خود، دلایل مهم و بسیاری دارد و لایهٔ شبکه نیز چنین است. اما دو لایـهٔ اتـصال بـه داده‌هـا و فیزیکـی، اهمیـت چنـدانی ندارند. هرچند می‌توان با ابزارهای ویـژه، از همـان رسـانه‌هـای واقعـی نیـز، داده‌هـا را جمع‌آوری کرد (کیسی، همان: ۱۷٤).

گفتار دوم: قواعد حقوقی ناظر بر اقدامات مجریان قانون

به دلیل گـستردگی حـوزهٔ عملکـرد مجریـان قـانون، بـه‌ویـژه نـسبت بـه داده‌هـای الکترونیکی، می‌توان اقداماتـشان را در پرتـو قواعـد حقـوقی گونـاگونی بررسـی کـرد. همان‌طور که در مباحث گذشته، به ملاحظات قلمرو حاکمیتی و ضرورت دسـتیابی بـه داده‌های الکترونیکی فراسرزمینی اشاره شد.

در این قسمت با توجه به موضوع بحث، مهم‌ترین حوزهٔ حقوقی که با سـایه‌افکنـی بر نظام عدالت کیفری جنبه‌های انسانی آن را حفظ و تقویت کرده است، گزینش شـده و آن، «موازین حقوق بشری» است که مهم‌ترین مانع اقدامات خودسرانهٔ مجریان قـانون به شمار می‌آید. به همین دلیل، هرجا ضابطه‌ای در رابطه با اقدامات آنها وضع شود، بـر این موازین هم تأکید می‌شود. کنوانسیون جرایم سایبر با ارج نهادن بر این موازین، پیش از ورود به ضوابط مربوط به آئین دادرسی کیفری، در بند ۱ مادهٔ ۱۵، به‌طور واضـح بـر رعایت آنها تأکید ورزیده است:

> ۱. اعضا باید اطمینان دهند که تصویب، اجرا و اعمال اختیارات و رویه‌های پـیش‌بینـی شده در این بخش، در شرایط و تضمین‌های حقوق داخلی‌شـان گنجانیـده‌انـد و در راستای حمایت شایسته از حقوق و آزادی‌های بشری است که از جملهٔ آنها، حقوق برخاسته از تعهداتی است که آنها در کنوانسیون شورای اروپا راجـع بـه حمایـت از حقوق و آزادی‌های اساسی بشر (۱۹۵۰) و میثاق حقوق مـدنی و سیاسـی سـازمان ملل متحد (۱۹٦٦) و دیگر اسناد بین‌المللی لازم‌الاجرای حقوق بشر پذیرفته‌اند. این شرایط و تضمین‌ها باید به دنبال برقراری اصل تناسب باشند ....

به‌طور کلی در پرتو این موازین، داده‌های الکترونیکی به دو دسته تقسیم مـی‌شـوند:

داده‌های شکلی و داده‌های محتوایی. این تقسیم‌بندی با عنایت به ارتباطات الکترونیکی، به عنوان آسیب‌پذیرترین نوع داده‌های الکترونیکی بـه عمـل آمـده اسـت تـا از حـریم خصوصی افراد حمایت جدی به عمل آید.

۱. داده‌های شکلی

منظور از این داده‌ها، هرگونه اطلاعات اعم از الکترونیکی و غیرالکترونیکی راجع به مشخصات محتوای ارتباطات الکترونیکی است. از جملهٔ مهـم‌تـرین آنهـا، داده ترافیـک (data traffic) و اطلاعات راجع به مـشترک (subscriber information) هـستند. طبـق مادّهٔ ۱ کنوانسیون جرایم سایبر:

> داده ترافیک: دادهٔ رایانه‌ای است که به ارتباط برقـرار شـده از طریـق سیـستم رایانـه‌ای مربوط می‌شود. این داده را سیستم رایانه‌ای ایجاد می‌کند که بخشی از زنجیرهٔ ارتبـاطی را تشکیل داده است و مبدأ، مقصد، مسیر، مدت، تاریخ، اندازه، دوام یـا نـوع خـدمات اصلی ارائه شده را نشان می‌دهد.

طبق بند ۳ مادهٔ ۱۸ نیز:

اطلاعات راجع به مشترک: هرگونه اطلاعات در قالب داده‌هـای رایانـه‌ای یـا دیگـر اشکال است که توسط ارائه‌دهندهٔ خدمات نگهـداری مـی‌شـود و دربـارهٔ مـشترکین آن خدمات است. این اطلاعات شامل داده ترافیک یا داده محتوا نمی‌شود و می‌توان آنها را به صورت زیر معین کرد: الف. نوع خدمات ارتباطی و پیش‌نیازهای فنی به‌کـار رفتـه و دورهٔ استفاده از خدمات؛ ب. هویت مشترک، آدرس جغرافیایی یا پستی، شمارهٔ تلفن و سایر شماره‌های دسترس، اطلاعات مربوط به صورت‌حساب و پرداخت، کـه براسـاس توافق یا ترتیب خدمات موجود است؛ ج. دیگر اطلاعات راجع به محل نصب تجهیزات ارتباطات، که براساس توافق یا ترتیب خدمات در دسترس قرار می‌گیرد.

برای در امان داشتن بیشتر این داده‌ها از تعرضات مجریان قـانون، میـان جمـع‌آوری زنده (real time)، یعنی در همان زمـان برقـراری ارتبـاط، و مـوارد ذخیـره شـدهٔ آنهـا، تفکیک ایجاد شده است. طبق کنوانسیون، برای دسترس به داده ترافیـک ذخیـره شـده، باید ضوابط مواد ۱۶ (حفظ فوری داده‌های رایانه‌ای ذخیره شده) و ۱۷ (حفظ فـوری و افشای جزئی داده ترافیک) را رعایت کرد، اما برای جمع‌آوری زندهٔ این داده‌ها مقررات

متمایزی در مادهٔ ۲۰ پیش‌بینی شده است. اطلاعات متعلق به مشترک نیز تحت شمول مقررات مادّهٔ ۱۸ (دستور تولید) قرار می‌گیرد.

اما در ایالات متحده، برای دسترس به اینگونه داده‌ها، کافی است احضاریه (subpoena) صادر شود. در این صورت می‌توان به اطلاعاتی که فهرست آن در بند ۲ قسمت ج بخش ۲۷۰۳ عنوان ۱۸ کد ایالات متحده (united states code) آمده است، دست یافت: ۱. نام؛ ۲. آدرس؛ ۳. سوابق مربوط به تماس تلفنی محلی و راه دور یا سوابق مربوط به تعداد دفعات و مدت زمان هر یک از آنها؛ ٤. مدت زمان استفاده از این خدمات (که شامل زمان شروع نیز می‌شود) و نوع خدمات بهره‌برداری شده؛ ٥. شمارهٔ تلفن یا وسیلهٔ دیگر یا شناساگر دیگر هویت مشترک که شامل آدرس شبکه‌هایی که به‌طور موقت استفاده می‌کرده نیز می‌شود؛ ٦. ابزار و منابع پرداخت استفاده از اینگونه خدمات که شامل کارت‌های اعتباری و شمارهٔ حساب بانک‌ها نیز می‌شود.

۲. دادهٔ محتوا (content data)

برخلاف انواع داده‌های شکلی، از این نوع داده‌ها در مقررات تعریفی وجود ندارد، ولی مفهوم آن روشن است و هر نوع داده‌ای را که منعکس‌کنندهٔ منظور و مضمون یک ارتباط الکترونیکی باشد، دربرمی‌گیرد.

در اینجا مسایل راجع به‌دسترس زنده به محتوا، که شنود (interception) نامیده می‌شود، به‌طور جدی مطرح است. در کنوانسیون جرایم سایبر نیز میان این نوع دسترس و دسترس به داده محتوای ذخیره شده، تفکیک صورت گرفته است. در مطالب پیشین به ضوابط کنوانسیون راجع به داده‌های رایانه‌ای ذخیره شده اشاره شد. مادّهٔ ۲۱ به‌طور مشخص به شنود اختصاص یافته است. باید توجه شود که صدر مادّه، حوزهٔ شمول خود را به جرایم شدید (serious crimes) محدود کرده است و نسبت به هر جرمی قابلیت اجرا ندارد:

> مادّهٔ ۲۱. شنود داده محتوا: ۱. هر یک از اعضاء باید به گونه‌ای به وضع قوانین و تدابیر دیگر اقدام کنند که به مقامات ذی‌صلاح خود این اختیار را بدهند تا در صورت لزوم، در رابطه با طیف جرایم شدیدی که در قانون داخلی معیّن شده است، اقدامات ذیل را انجام دهند: الف. جمع‌آوری یا ضبط، از طریق به‌کارگیری ابزارهای فنی در قلمرو آن

عضو؛ ب. الزام ارائه‌دهنده (خدمات در حیطهٔ توانایی فنی که در اختیار دارد)، برای: ۱. جمع‌آوری یا ضبط، از طریق به‌کارگیری ابزارهای فنی در قلمرو آن عضو؛ یا ۲. همکاری و کمک به مقامات ذی‌صلاح در جمع‌آوری یا ضبط زندهٔ داده محتوای ارتباطات معیّن که از طریق سیستم رایانه‌ای واقع در قلمرو آن عضو انتقال می‌یابد. ۲. در جایی که یک عضو به خاطر اصول حاکم بر نظام حقوق داخلی‌اش، نمی‌تواند تدابیر مقرر در بند ۱ (الف) را به تصویب برساند، به جای آن، قوانین و تدابیر دیگری را می‌تواند به تصویب برساند که جمع‌آوری یا ضبط زندهٔ داده محتوای ارتباطات خاص در قلمروش را با به‌کارگیری ابزارهای فنی در آن قلمرو تضمین کنند. ۳. هر یک از اعضاء باید به گونه‌ای به وضع قوانین و تدابیر دیگر اقدام کنند که در صورت لزوم، به ارائه‌دهندهٔ خدمات دستور دهند، هر موضوعی از اطلاعات راجع به اختیارات مندرج در این مادّه را محرمانه نگهدارد. ٤. اختیارات و رویّه‌های مندرج در این مادّه، باید با رعایت مواد ١٤ و ١٥ باشد.

این ضوابط در ایالات متحده دقیق‌تر تنظیم شده است. علاوه بر تفکیک محتوای ذخیره شده از محتوای ارتباط زنده، اینکه چه مدت زمانی ذخیره شده نیز در نوع دستوری که باید از مقام ذی‌صلاح اداری یا قضایی دریافت کرد، تأثیر دارد. پس از ضابطهٔ دریافت احضاریه، جهت دسترس به داده‌هایی که ماهیت شکلی دارند، برای دریافت داده‌های رایانه‌ای محتوایی (به‌طور عمده) و شکلی (در برخی اوقات) نیز چهار نوع دستور پیش‌بینی شده است (Department of Justice of the United States, 2002: 62):

۱. احضاریه با ابلاغ پیشین به مشترک یا مشتری مورد نظر: مأمورانی که احضاریه تحصیل می‌کنند، چه به مشترک پیشاپیش ابلاغ کنند یا مقررات ابلاغ با تأخیر، مندرج در قسمت الف بخش ۲۷۰۵ را رعایت کنند، می‌توانند موارد زیر را تحصیل کنند: ۱. همهٔ مواردی که با استفاده از احضاریهٔ بدون ابلاغ می‌توان به‌دست آورد؛ ۲. محتوای ارتباطات الکترونیکی یا کابلی که ارائه‌دهندهٔ خدمات رایانه‌ای راه دور (remote computing service) به جای مشترک یا مشتری خود نگهداری می‌کند؛ ۳. محتوای ارتباطات الکترونیکی یا کابلی که بر روی سیستم‌های ارتباطات الکترونیکی، در ذخیرهٔ الکترونیکی (electronic storage) به مدت بیش از ۱۸۰ روز نگهداری شده باشد (قسمت الف بخش ۲۷۰۳).

۲. دستور دادگاه، مطابق قسمت د بخش ۲۷۰۳: این دستور توسط قاضی فدرال، قاضی دادگاه ناحیه یا قاضی دادگاه معادل ایالتی صادر می‌شود و به موجب آن این موارد را می‌توان به‌دست آورد: ۱. تمام مواردی که با صدور احضاریهٔ بدون ابلاغ می‌توان اخذ کرد؛ ۲. تمام سوابق یا اطلاعات راجع به مشترک یا مشتری اینگونه خدمات، که البته محتوای ارتباطات نگهداری شده توسط ارائه‌دهندگان خدمات ارتباطات الکترونیکی و رایانه‌ای راه دور را شامل نمی‌شود. برای اخذ این دستور که به «دستور قضایی مبتنی بر حقایق قابل تشریح» (articulable facts court order) نیز معروف است، یا به‌طور خلاصه دستور d نامیده می‌شود، مجریان قانون باید دلایل مشخص و قابل تشریح خود را که نشان‌دهندهٔ زمینه‌های متعارف می‌باشد و این اعتقاد را ایجاد می‌کند که محتوای ارتباطات کابلی یا الکترونیکی یا سوابق دیگر اطلاعاتی که دنبال می‌کنند، جزئی از جرم یا در ارتباط با جرمی هستند که آنها قصد تحقیق آن را دارند، ارائه دهند. به این ترتیب، این معیار به مجریان قانون اجازه نمی‌دهد که صرفاً گواهی کنند، یک سری حقایق مشخص و قابل تشریح وجود دارد، بلکه باید مدارک واقعی ارائه دهند تا بتوانند چنین دستوری را اخذ کنند.

۳. دستور دادگاه، مطابق قسمت د بخش ۲۷۰۳، با ابلاغ پیشین به مشتری یا مشترک مورد نظر: چنانچه مجریان قانون بتوانند این دستور را اخذ کنند، موارد زیر به‌دست می‌آید: ۱. تمام مواردی که با استفاده از دستور بدون ابلاغ قسمت د بخش ۲۷۰۳ می‌توان به‌دست آورد؛ ۲. محتوای هرگونه ارتباطات الکترونیکی یا کابلی که ارائه‌دهندهٔ خدمات رایانه‌ای راه دور به جای مشترک یا مشتری خود نگهداری می‌کند؛ ۳. محتوای ارتباطات الکترونیکی یا کابلی که در ذخیرهٔ الکترونیکی سیستم ارتباطات الکترونیکی بیش از ۱۸۰ روز موجود بوده است. البته مأموران در اینجا نیز با رعایت مقررات ابلاغ با تأخیر، باز هم می‌توانند این موارد را به‌دست آورند.

٤. قرار تفتیش (warrant): مأمورانی که مطابق مادهٔ ٤١ آئین دادرسی کیفری فدرال (federal rules of criminal procedure) قرار تفتیش یا معادل ایالتی آن را دریافت می‌کنند، به موارد زیر می‌توانند دست یابند: ۱. تمام مواردی که می‌توان با استناد به‌دستور دادگاه با ابلاغ پیشین به‌دست آورد؛ ۲. محتوای ارتباطات الکترونیکی یا کابلی

که در ذخیرهٔ الکترونیکی سیستم ارتباطات رایانه‌ای به مدت ۱۸۰ روز یا کمتر، ذخیره شده است؛ ۳. به‌طور خلاصه، مأموران با تحصیل قرار تفتیشی که بر پایهٔ سبب محتمل (probable cause) و مطابق مادّهٔ ٤١ صادر شده است، هرگونه سابقه و همهٔ محتویات اعتبار مشترک یا مشتری مورد نظر را می‌توانند به‌دست آورند که به این ترتیب، شنود ارتباطات الکترونیکی و کابلی نیز تحت شمول این مقررات قرار می‌گیرد. اما نکتهٔ مهم این است که اثبات سبب محتملی که در اصلاحیهٔ چهارم قانون اساسی (fourth amendment) آمده است و از مجریان قانون خواسته است برای اثبات آن سوگندنامه (affidavit) ارائه دهند و گواهی خود را به آن ضمیمه کنند، به مراتب از ارائهٔ حقایق قابل تشریح، برای اخذ دستور دادگاه مشکل‌تر است.

در پایان یادآور می‌شود، همواره تفکیک محتوای زنده از ذخیره شده، به آسانی میسّر نبوده است و چالش‌هایی را ایجاد کرده است. در پروندهٔ جنجالی شرکت استیوجکسون گیمز (Steve Jackson Games v. U.S. secret service 1990) در سال ۱۹۹۰، مأموران سرویس امنیتی، پیام‌های باز نشده و ذخیره شده در سیستم تابلوی اعلانات (bulletin board system) متعلق به‌کاربران شرکت جکسون را باز، مطالعه و سپس پاک کرده بودند. این شرکت پس از آن در پی شکایات متعددی که علیه سرویس امنیتی مطرح کرد، به این موضوع اشاره و ادعا کرد که مأموران بدون مجوز شنود، آن پیام را باز کرده‌اند. اما دادگاه اظهار داشت، از آنجا که این پیام‌ها به صندوق پست الکترونیکی وارد شده‌اند، دیگر نمی‌توان آنها را پیام در جریان دانست و تحت ضوابط شنود قرار داد، فقط داده‌های رایانه‌ای ذخیره شده محسوب می‌شوند.

نتیجه‌گیری

تنوع مطالب در این نوشتار مختصر، به خوبی طیف گستردهٔ مباحث راجع به استنادپذیری ادلهٔ الکترونیکی در امور کیفری را نشان می‌دهد. در حالی که هیچ‌یک از آنها کم‌اهمیت نیستند و در جای خود، نقش تعیین‌کننده‌ای در سرنوشت پرونده‌های کیفری سایبری ایفا می‌کنند. کشورهایی که به تازگی با انواع سوء استفاده‌های مجرمانه از فناوری اطلاعات و ارتباطات مواجه‌اند و درصدد اصلاح قوانین جزایی‌شان برآمده‌اند

یا قوانین جدیدی را در شرف تصویب دارند، باید در پرتو جمیع موازین حقوقی، برای هر یک از این مسایل، راهکارهای قانون‌مند منطقی و قابل اجرایی ارائـه دهنـد. در غیـر این صورت، جز متروک ماندن آنها نباید انتظار دیگری داشته باشند. در اینجـا بـه دلیـل نبود مجال، امکان ریزنگری در هر یک از رئوس مطالب، و به‌ویژه امکان‌سنجی قـوانین و مقررات داخلی فراهم نبود. به همین دلیل بـه طـرح کلـی مباحـث اکتفـا شـد و ایـن موضوعات، به نوشتارهای آتی موکول می‌شود.

منابع

أ. فارسی

۱. آشوری، محمد. ۱۳۸۰. *آئین دادرسی کیفری*. ج ۲. نشر سمت.

۲. بختیاروند، مصطفی. ۱۳۸۳. «امضای الکترونیکی و انقلاب قواعد مربوط به ادلهٔ اثبات دعوی». *خبرنامهٔ انفورماتیک*. ش ۹۱.

۳. دبیرخانهٔ شورای عالی انفورماتیک کشور. ۱۳۷٦. *جرایم کامپیوتری*. ج ۱.

٤. قاجارقیونلو، سیامک. ۱۳۸۱. «مقدمه‌ای بر زیرساخت کلید عمومی». *خبرنامهٔ انفورماتیک*. ش ۸۵.

۵. کیسی، اوئن. ۱۳۸٦. *دلایل دیجیتالی و جرم رایانه‌ای (علم قانونی. رایانه‌ها و اینترنت)*. مترجمان: امیرحسین جلالی‌فرهانی و علی شایان. معاونت حقوقی و توسعهٔ قضایی قوّهٔ قضائیه (مرکز مطالعات توسعهٔ قضایی). نشر سلسبیل.

٦. مرکز پژوهش‌های مجلس شورای اسلامی. ۱۳۸٤. کنوانسیون جرایم سایبر و گزارش توجیهی آن. ش ۷٦٤٦.

ب. لاتین

7. Department of Justice of the United States, 2002. *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*.

8. M. Gahtan, Alan. 1999. *Electronic Evidence*. Carswell.

9. T. Kent, Stephen & I. Millett Lynette. 2003. *Who Goes There? Authentication Through the Lens of Privacy*. National Academy Press.