پژوهشنامه حقوق کیفری
سال نهم، شماره دوم، پاییز و زمستان ۱۳۹۷
شماره پیاپی ۱۸

آیین کشف و ابراز دلیل در فضای مَجازی

دکتر مصطفی السان[1] ✉
محمدرضا منوچهری[2]

تاریخ دریافت: ۱۳۹۶/۳/۲۷ تاریخ پذیرش: ۱۳۹۷/۸/۹

چکیده

فرایند کشف، تفتیش و حفاظت از ادله الکترونیکی و نیز ابراز چنین دلایلی از سوی ذینفع در دادگاه حاوی مسایل مهمی است که نیاز به بررسی دارند. اصول و تشریفاتی که در این فرایند به کار گرفته می‌شوند و نیز ضمانت اجرای اقداماتی که صورت می‌گیرد، از جمله این مسایل می‌باشند. به طور کلی، ابراز دلیل و نیز آثار خودداری از ابراز دلیل در موارد قانونی، تابع قواعد عمومی مذکور در مقررات آیین دادرسی است؛ در عین حال، در مورد ادله الکترونیکی اغلب لازم می‌آید تا برخی قواعد خاص یا تشریفات ویژه این نوع از ادله به کار گرفته شوند. این مقاله ضمن شناخت ابزارها و دلایل مرتبط با فضای مجازی به بررسی تشریفات کشف جرایم مَجازی و اعتبار داده‌ها و تشریفات ابراز آنها می‌پردازد و بر این نکته مهم تأکید دارد که قواعد و تشریفات حاکم بر کشف، نگاهداری و ابراز و استناد به ادله الکترونیکی باید به صورت استاندارد و بدون تفکیک میان دعاوی حقوقی و کیفری ارایه شوند. در مقاله، آخرین قوانین و مقررات کشورمان مورد تجزیه و تحلیل قرار گرفته و راهکارهای مرتبط به منظور استناد و اعتبار ادله الکترونیکی در دادگاهها و سایر مراجع ارایه می‌شود.

واژگان کلیدی: کشف، ابراز، ادله اثبات دعوا، فضای مجازی، تفتیش و بازرسی

۱. استادیار گروه حقوق خصوصی دانشگاه شهید بهشتی (نویسنده مسئول) ✉ mostafaelsan@yahoo.com
۲. دانشجوی دکتری حقوق خصوصی دانشکده حقوق دانشگاه شهید بهشتی

مقدمه

قدم گذاشتن در فضای مجازی، همانند گام نهادن در یک سیاره ناشناخته یا به تعبیری ملموس‌تر، یافتن خود در طبیعتی بکر با حیاتِ وحشی ناشناخته و کشف نشده است. هرچه این فضا بیشتر توسعه می‌یابد، ضرورت تدوین قواعد حقوقی متناسب یا تطبیق قواعد موجود برای اجرا در فضای جدید بیشتر احساس می‌شود. همین امر، باعث می‌گردد که حقوقدانان بیشتری به تحقیق و پژوهش در خصوص این فضای کشیده شوند. اما این امر، هرگز از بکر بودن این فضا نمی‌کاهد. از آن جهت که دنیای خیالی ما هر روز در حال رشد و تنوع است؛ هرروز نابغه‌ها و نبوغ بیشتری در این فضا پدیدار می‌شود. البته همه نابغه‌ها به فکر پیشرفت و درستکاری در فضای مجازی نیستند. منافع یا حتی کنجکاوی برخی اقتضا دارد که نقاط ضعف این فضا را به چالش بکشند و کجروی‌هایی خلق کنند که اگر فضای مجازی وجود نداشت، هرگز تجربه نمی‌شدند. برای مثال، قاتلی که به رایانه و اینترنت نیز تسلط دارد، ممکن است بمبی را به قربانی خود وصل کرده و آن را طوری برنامه‌ریزی کرده باشد که با افزایش کاربران برخط (آن‌لاین) یک تارنمای مشهور و رسیدن آنها به تعداد معین، عمل کند. در این صورت، کنجکاوی هریک از کاربران اینترنت برای دیدن آمار کاربران آن‌لاین آن تارنما، نتیجه‌ای اسف‌بار را در پی خواهد داشت. برخی هم ممکن است برای دیدن صحنه قتل قربانی که قرار است در صورت عمل کردن بمب منطقی به صورت آن‌لاین پخش شود، درصدد جذب مخاطب برای آن تارنما از طریق تارنماهای اصلی و فرعی خود برآیند.

بررسی جرایم مرتبط با فضای مجازی به‌خوبی نشان می‌دهد که در بسیاری از این جرایم، فضای جرم، شگردها و فنون ارتکاب آن و صنف بزهکاران تغییر می‌یابد. ماهیت جرایم ارتکابی هم، گاه به نحوی است که نمی‌توان معادلی برای آن در خارج از فضای مجازی یافت. به همین دلایل، کشورهای مختلف مجبور شده‌اند قوانینی برای جرم‌انگاری و پیشگیری از جرایمی که در فضای مجازی روی می‌دهد، وضع کنند و به لحاظ ماهیت ویژه این فضا یعنی نداشتن حد و مرز مکانی، اغلب ناچار گشته‌اند که با کشورهای دیگر در پیگرد جرایم فضای مجازی تعامل و همکاری نمایند.

همین حقایق، اقتضاء می‌کند که آیین نسبتاً متفاوتی برای دادرسی کیفری نسبت به جرایم فضای مجازی شکل گیرد. همچنین پلیس فضای مجازی، باید مجهز به ابزارها، امکانات و نیروی انسانی ویژه‌ای باشد که با فضای جدید، شگردهای پیچیده و نابغه‌هایی که در فضای مجازی مرتکب جرم می‌شوند، هماهنگی داشته باشد.

این مقاله ضمن سه گفتار بدین شرح به بررسی آیین کشف و ابراز دلیل در جرایم فضای مَجازی می‌پردازد: ۱- مفهوم ادله الکترونیکی و شناخت ابزارها و دلایل مرتبط با فضای مجازی

(گفتار اول)، ۲- تشریفات کشف جرایم مَجازی (گفتار دوم) ۳- اعتبار داده‌ها و تشریفات ابراز آن‌ها (گفتار سوم).

جدید بودن ادلهٔ الکترونیکی و نیز متفاوت بودن فضایی که در آن این نوع از ادله تولید، ذخیره، پردازش، بازیافت یا تغییر می‌یابند، اقتضا دارد تا شیوه‌های کشف و ابراز متفاوت و نوپدیدی در مقایسه با فضای سنتی ادله در مورد کشف و ابراز آن‌ها به‌کار گرفته شود. این مقاله درصدد بررسی این موضوع‌ها و مسایل عملی مرتبط با آن‌ها می‌باشد.

گفتار اول. مفهوم ادله الکترونیکی و شناخت ابزارها و دلایل مرتبط با فضای مجازی

بند اول. مفهوم ادله الکترونیکی

دلیل در اصطلاح حقوق جزا عبارت است از هر وسیله قانونی که مقام قضایی را در کشف حقیقت و حصول اقناع وجدانی و اتخاذ تصمیم یاری بخشد (آشوری، ۱۳۸۸: ۲۳۰). دلیل الکترونیکی در مفهوم عام به هر نوع اطلاعاتی تعریف شده که در قالب دیجیتالی (رقومی) ایجاد یا ذخیره شده است. خواه از رایانه برای انجام کاری استفاده شده یا این‌که به‌طور خودکار عمل کرده باشد (Chung, 1997: p.8). بنابراین، دلیل الکترونیکی می‌تواند محصول وضعیت‌های مختلف باشد: شخصی داده‌ای را به رایانه‌ای وارد سازد، رایانه به درخواست کاربر عملیاتی را انجام دهد یا این‌که به‌طور خودکار اطلاعاتی را به‌کار برده یا آن‌ها را پردازش نماید. از این‌رو، ادله الکترونیکی شامل پایگاه‌های داده، سیستم‌های عامل، برنامه‌های رایانه‌ای، مدل‌های ایجاد شده توسط رایانه، پیام‌ها و سوابق الکترونیکی و صوتی و هر نوع اطلاعات یا دستورهایی است که در حافظهٔ رایانه ذخیره شده یا از طریق سامانه‌های رایانه‌ای یا مخابراتی مبادله، پردازش، بازیافت یا تولید می‌شود.

ادله الکترونیکی، از آن جهت که در جایی ذخیره شده و یا قابل چاپ هستند و نیز، اغلب به صورت مستند می‌توان آن‌ها را ارائه داد، به «سند» (نوشته) شباهت بسیاری دارند.[1] در عین حال، ادله الکترونیکی با ادله مرسوم دارای تفاوت‌هایی هستند که نیاز به بررسی جداگانه دارد.

اولین تفاوت میان ادله الکترونیکی و ادله کاغذی آن است که، تحصیل و جمع‌آوری داده‌های الکترونیکی، به‌دلیل این‌که به‌راحتی در واسط‌های الکترونیکی ذخیره شده و از همین طریق انتقال می‌یابند، بسیار آسان‌تر است. مقایسه میان نامهٔ الکترونیکی و نامه‌ای که از طریق اداره پست ارسال می‌شود، گویای این تفاوت می‌باشد.

۱. مطابق با ماده ۱۲۸۴ ق.م، «سند عبارت است از هر نوشته که در مقام دعوی یا دفاع قابل استناد باشد».

تفاوت دوم با قابلیت دسترسی به ادله الکترونیکی ارتباط می‌یابد. داده‌های الکترونیکی با نام مشخص در رایانه ذخیره می‌شوند. بنابراین هر شخصی می‌تواند با ورود به رایانه، در حافظه سخت (هارد) جستجو کرده و جز در مواردی که از نرم‌افزارهای پیشرفته برای مخفی کردن آن‌ها استفاده شده باشد، آن‌ها را بیابد. درحالی‌که یافتن یک مدرک کاغذی، گاه مستلزم جستجو در تمامی پرونده‌های واحد بایگانی است. از سوی دیگر، از بین بردن یا قایم کردن یک پوشه الکترونیکی بسیار سخت‌تر است (Givens, 2003-2004: p.97). به‌ویژه، داده‌هایی که از طریق اینترنت مبادله می‌شوند، را می‌توان با استفاده از رایانه در مناطق مختلف جهان به‌دست آورد. همچنین امکان دارد از داده‌های مهم نسخه پشتیبان تهیه شود که در این صورت دادگاه می‌تواند آن‌ها را برای کشف حقیقت به‌کار گیرد.

حتی داده‌هایی که توسط کاربر حذف می‌شوند، با استفاده از نرم‌افزارهای خاص قابل بازیابی هستند. برای این کار می‌توان از کارشناسانی که در تحقیقات رایانه‌ای تبحر دارند، استفاده کرد.

تفاوت دیگر ادله الکترونیکی و مدارک کاغذی با محتوای هرکدام از آن‌ها ارتباط می‌یابد. برخلاف مدارک کاغذی که محتوای آن‌ها قابل مشاهده است، تبدیل سابقهٔ الکترونیکی به کاغذ (چاپ آن)، نمی‌تواند گویای تمامی ویژگی‌ها و اطلاعاتی باشد که در قالب الکترونیکی وجود دارد.[1] برای مثال، به هنگام چاپ یک نامه الکترونیکی، تأییدیه وصول، مشخصات رایانه و نرم‌افزار مورد استفاده و سایر جزئیات فنی مشخص نمی‌شود و برای کشف این موارد، نیاز به تحقیقات رایانه‌ای وجود دارد. به‌عبارت دیگر، در یک تقسیم‌بندی می‌توان ادلهٔ رایانه‌ای را به ادله در صفحه (صحنه) و پشت صحنه[2] تقسیم‌بندی کرد.

در مقایسه با سایر ادله، ادله الکترونیکی البته نقطه‌ضعف‌هایی دارند که نمی‌توان از آن‌ها چشم‌پوشی کرد. از جمله این‌که، وقتی چند نفر از یک رایانه یا سامانه رایانه‌ای استفاده می‌کنند، امکان انتساب اطلاعات درج شده در آن به هرکدام از آن‌ها دشوار است. به‌علاوه، داده‌های الکترونیکی به رایانه و ابزارهای متناسب با ماهیت خود نیاز دارند و بدون آنها قابل بررسی (بازیابی، تجزیه و تحلیل و کشف) نیستند. داده‌های رایانه‌ای، در مقایسه با مدارک کاغذی، بیشتر در معرض دسترسی غیرمُجاز هستند. چرا که ممکن است از طریق اینترنت برای افراد مختلفی قابل دستیابی باشند (جلالی فراهانی، ۱۳۸۶: ۸۸-۸۷). همچنین، ادلهٔ الکترونیکی را می‌توان در فضای مجازی به طور کامل از بین برد و هیچ ردپایی از وجود آن‌ها به جای نگذاشت.

1. Armstrong v. Executive Office of the President , 1 F.3d 1274 [DC Cir Cir 1993].

2. On–Screen and Non–Screen.

مشکل دیگری که با بررسی حقوقی ادله الکترونیکی ارتباط می‌یابد به نقص قوانین و مقررات مربوط می‌شود. در بسیاری از کشورها، قوانین راجع به ادله اثبات دعوا پیش از پدیدار شدن رایانه و سامانه‌های نوین ارتباطی به تصویب رسیده است. در نتیجه، این احتمال وجود دارد که دادگاه‌ها به‌دلیل نبود قانون در برابر اصل پذیرش این دسته از ادله یا در مورد حدود ارزش اثباتی آن‌ها مقاومت کرده یا تردید داشته باشند.

بند دوم. شناخت ابزارها و دلایل مرتبط با فضای مجازی

در مراحل پیشگیری، تحلیل منسجم ویژگی‌های یک جرم که درصدد پیشگیری از آن هستیم، از حیث مطالعه فضای جغرافیایی موردنظر بزهکاری، تحلیل ساختار آن جرم و مباشران و بزه‌دیدگان آن، بررسی نوسانات این جرم در یک دوره معین، اهمیت خاصی دارد (نجفی‌ابرندآبادی، ۱۳۸۷: ۱۸۱). در واقع، یکی از اهداف کشف جرایم مجازی، مبارزه با آن‌ها و پیشگیری از جرایم مشابه است. این هدف، به‌دست نمی‌آید، مگر این‌که شناخت صحیحی از ابزارهای تهاجم، دفاع و مبارزه در جرایم مجازی داشته باشیم. پس از بررسی این ابزارها به موضوع تشریفات کشف و پیگرد جرایم مجازی خواهیم پرداخت.

مسایل متعددی با کشف جرایم مَجازی ارتباط می‌یابد که چندان با اصول و تشریفاتی که در تحقیق و بازرسی صحنه جرایم معمول به‌کار می‌رود، قابل تطبیق نیست. این فضا محدوده‌ای به نام مرز و قلمرو سرزمینی ندارد و می‌تواند تمامی دهکدهٔ جهانی را شامل شود.

مقصود از «ابزار» در این گفتار، هر چیزی است که در رسیدن به هدف مورد نیاز باشد. این ابزار می‌تواند هر نوع وسیله‌ای را اعم از نرم‌افزار و سخت‌افزار شامل شود. در جرایم مجازی، ابزار، شامل موارد زیر شود:

ـ هر چیزی که مهاجمین (بزهکاران)، برای دسترسی غیرمجاز و اقدامات پس از آن یا برای شناسایی نشدن به‌کار می‌گیرند.

ـ هر چیزی که مدافعین (افراد در معرض بزه‌دیدگی)، برای پیشگیری از دسترس غیرمجاز از سوی مهاجمین یا اقدام علیه آن‌ها مورد استفاده قرار می‌دهند. اقدام علیه مهاجمین شامل گزارش تهاجم به مقامات صالح، طرح دعوا در محاکم یا در مواردی بهره‌برداری از یک حمله بر علیه مهاجم می‌شود.

ـ هر چیزی که پلیس (اعم از نیروهای انتظامی، امنیتی و دادسرا)، برای کشف و پیگرد جرایم مجازی، حفظ صحنه جرم، جمع‌آوری ادله، پیشگیری از جرایم مشابه و بایگانی و گزارش آن‌ها مورد استفاده قرار می‌دهند.

الف. ابزارهای حمله در فضای مجازی

ابزارهای اصلی که بزهکاران مجازی به‌کار می‌گیرند، از دو حالت خارج نیست. یا جنبه فنی و علمی دارد و یا این‌که با آموزه‌های اجتماعی و ضعف جامعه ارتباط می‌یابد.

از نظر فنی، رایانه‌های توانمند، اینترنت، نرم‌افزار و گمنامی در بزهکاری مجازی بیشترین تأثیر را داشته است. رایانه‌هایی که از آن‌ها برای ارتکاب جرم استفاده می‌شود، سرعت بالایی در پردازش و تجزیه و تحلیل داده‌های در حال انتقال (ارسال و دریافت) یا بایگانی شده دارند. قیمت این رایانه‌ها چندان گران نیست. برای به‌دست آوردن رمزهای ورود و انواع مختلف کُدها، بزهکاران اغلب با هم ارتباط برقرار کرده و این رمزها را رد و بدل می‌کنند. در جرمی مانند اخلال در داده یا سامانه رایانه‌ای، به‌طور معمول رایانه‌هایی با توانایی بیشتر، در مقایسه با اکثر جرایم مجازی مورد نیاز می‌باشد.

اینترنت، ابزار توانمند دیگری است که علاوه بر افراد عادی، در اختیار بزهکاران نیز قرار دارد. حضور افراد عادی و کج‌رو در کنار هم، اینترنت را به فضایی آلوده تبدیل می‌کند. جهانی بودن ارتباطات این شبکه و سرعت بالای ارتباطات در آن، در عین این‌که یک نقطه قوت است، برای بزهکاران یک فرصت به‌حساب می‌آید. یک متخصص رمزیابی بنام (Nicholas Weaver)، بر این اعتقاد است که باوجود اینترنت، یک بزهکار می‌تواند تمامی رایانه‌های متصل به اینترنت را ظرف ۱۵ دقیقه تا یک ساعت به کرم رایانه‌ای آلوده کند (Turrini & Ghosh, 2010: p.18).

با توسعهٔ اینترنت به گوشه و کنار جهان، قلمرو سرزمینی جرایم مجازی هم گسترش می‌یابد. به‌علاوه، ابزارهایی که امروزه می‌توان از طریق آن‌ها به اینترنت وصل شد، محدود به رایانه (در مفهوم عرفی آن) نیست. امروزه گوشی‌های تلفن همراه، تلویزیون‌ها، دستگاه‌های ردیاب، دستگاه‌های بازی و سرگرمی و... قابلیت اتصال به اینترنت را دارند. این امکان، باعث می‌شود که افراد غیرحرفه‌ای که احتمال بزه‌دیدگی آن‌ها بیشتر است و شناخت کافی نسبت به تهدیدات فضای مجازی ندارند، با بزهکاران نابغه و حرفه‌ای روبه‌رو شوند. واضح است که اغلب، مهاجم مَجازی پیروز خواهد شد و به اهداف مجرمانه خویش دست خواهد یافت.

۱. نرم‌افزار. در فضای مجازی، نرم‌افزار ابزار جنگی مهاجمین به‌حساب می‌آید. چراکه در بسیاری از جرایم مجازی از نرم‌افزار استفاده می‌شود. از حیث بزهکاری، نرم‌افزارها دو نوع هستند. ۱) خود نرم‌افزار وسیله جرم است و کاربرد دیگری ندارد. این نرم‌افزارها اسامی مختلفی همچون ویروس، کرم رایانه‌ای، جاسوس (Spyware) یا اسب تروا (Trojan Horse) دارند. کارکرد مشترک آن‌ها هم این است که در رایانهٔ هدف نصب شده و اقدام به خرابکاری یا هر عملیاتی می‌کنند که برای آن طراحی شده‌اند. ۲) برنامه‌هایی که برای تجاوز به حریم داده‌های افراد به‌کار می‌روند. این نرم‌افزار به

مهاجم کمک می‌کند که حسب مورد، کنترل تمام یا بخشی از برنامه‌ها و اطلاعات رایانه هدف را در اختیار گیرد. بر خلاف اسلحه‌های نظامی که در کشورهای مختلف، تجارت آن‌ها ممنوع بوده یا با محدودیت‌های شدیدی روبه‌رو می‌باشد، تقریباً هیچ منعی برای مبادله ویروس‌ها و سلاح‌های نرم‌افزاری وجود ندارد. بنابراین، آن‌ها به راحتی در سراسر جهان به اشتراک گذاشته شده و همگام با پیشرفت‌های جهانی در زمینهٔ ارتقای ایمنی و دفاعی سامانه‌های رایانه‌ای، از طریق تعامل میان بزهکاران حرفه‌ای که با استفاده از اینترنت صورت گیرد، به‌روز شده و در صورت لزوم، قالب، استانداردها و شیوه‌های هجومی خود را تغییر می‌دهند.

۲. گمنامی. ساختار و نحوهٔ تعامل در اینترنت و پیکربندی (Configuration) بسیاری از رایانه‌ها، ایجاب می‌کند که بزهکاران مجازی از سرپوشی به نام گمنامی (Anonymity) یا استفاده از نام ساختگی بهره‌مند شوند. نتیجه این امر آن است که احتمال شناسایی هویت واقعی بزهکار برای پیگرد کیفری و یا مدنی او و اعمال مجازات در مورد وی، کاهش می‌یابد. در تجارت الکترونیکی، احتمال گمنامی تنها در مورد افرادی وجود دارد که خارج از تعامل بوده و درصدد نفوذ و سوء استفاده از روابط تجاری الکترونیکی هستند. زیرا، برای مثال در یک معاملهٔ الکترونیکی، ابزارها و نرم‌افزارهای تقریباً امنی طراحی شده که از طریق آن‌ها، هویت واقعی طرفین معامله، احراز می‌شود. برای نمونه، وقتی از کارت پرداخت استفاده می‌شود، صرف استفاده، هویت دارنده کارت را مشخص می‌سازد. چراکه شخص، با ارائه کارت شناسایی معتبر و اطلاعاتی که صحت آن‌ها به تأیید کارمند بانک رسیده، موفق به دریافت کارت شده است.

صرف‌نظر از بحث فوق، گمنامی گاه، به ساختار رایانه برمی‌گردد. در طراحی رایانه‌ها، هیچ ساز و کاری برای تشخیص هویت شخصی که از آن استفاده می‌کند، در نظر گرفته نشده است. البته، امروزه برای ورود به برخی از رایانه‌ها (به‌ویژه رایانه‌های همراه)، دارنده می‌تواند از فناوری اثر انگشت یا تشخیص چهره برای پیشگیری از ورود سایر افراد استفاده نماید. در محتوای رایانه هم می‌توان از نرم‌افزارهایی بهره گرفت که استفاده از آن‌ها نیازمند وارد کردن رمز یا طی مراحل خاصی باشد. به‌علاوه، پوشه‌ها و مدارک رایانه‌ای را می‌توان رمزگذاری کرد تا از استفاده افراد غیرمجاز مصون باشد. در اکثر موارد، وقت‌گیر و گاه هزینه‌بر بودن این فرایندها باعث می‌شود که رایانه‌ها و اطلاعات موجود در آنها در معرض دسترسی افراد گمنام باشد. این سهل‌انگاری‌ها، زمینه جرایمی همچون دسترسی غیرمجاز و سرقت هویت را فراهم می‌سازد.

در روند کشف و پیگرد جرایم مجازی، گمنامی گاه باعث می‌شود که یافتن بزهکار واقعی مشکل شود و افرادی متهم شوند که تنها دسترسی آنها به سامانه اثبات شده، اما واقعاً معلوم نیست که خرابکاری از سوی آن‌ها بوده یا شخص دیگری از رایانه آن‌ها سوء استفاده کرده است. برای مثال،

وقتی پلیس در روند کشف جرم، ارتکاب آن را از آی.پی معین ردیابی می‌کند و آن نقطه تماس به یک مرکز تحقیقاتی تعلق دارد، معلوم نیست که واقعاً کارمندان مرکز مذکور مرتکب جرم شده‌اند یا پژوهشگرانی که به آنجا رفت و آمد دارند، با نصب نرم‌افزارهای تهاجمی یا نفوذ غیرمجاز در سامانه، زمینه سوء ظن به سامانه آن مرکز را فراهم کرده‌اند.

در هر حال، باید به این نکته توجه کرد با توجه به پذیرش اسناد و مدارک الکترونیکی به‌عنوان دلیل اثبات، باید متخصصان لازم برای احراز اصالت این اسناد در دستگاه قضایی موجود باشند. نکته دیگری که باید بدان توجه کرد، نقش مهم حفظ حریم خصوصی اسناد الکترونیکی در فضاهای مجازی است. این امر به‌ویژه در زمینه سوء استفاده از این اسناد مهم به‌نظر می‌رسد (جمالی و رزاقی، ۱۳۹۴: ۸۵).

ب. ابزارهای اجتماعی مورد استفاده در فضای مجازی

بزهکاران مجازی از هر دسیسه‌ای که امکان ارتکاب جرایم مدنظر آنها را فراهم نماید، استفاده می‌کنند. نمونه بارز آن‌ها، استفاده از نقاط ضعف افراد از طریق ارسال نامهٔ الکترونیکی یا حتی مذاکره شفاهی از طریق رو در رویی فیزیکی یا الکترونیکی با آن‌ها است.

مجموعه ابزارهای اجتماعی که بزهکاران مجازی از آن‌ها استفاده می‌کنند، نوعی مهندسی اجتماعی برای ارتکاب جرم به‌وجود می‌آورد. در این ساختار، همیشه لازم نیست که برای به‌دست آوردن رمز ورود یا سایر اطلاعاتی که برای شروع به جرم لازم است، از فناوری‌های پیچیده استفاده شود. بلکه تنها یک اشتباه یا سهل‌انگاری برای بزهکار حرفه‌ای کفایت می‌کند.

بزهکار باهوش می‌تواند مهندسی اجتماعی را با توانایی و امکانات فنی در هم آمیزد؛ در این صورت، حملهٔ مرگباری شکل گیرد. برای مثال، راهبرد ویروس ملیسا (Melissa Virus) همین بود. این ویروس از طریق یک نامهٔ الکترونیکی که عنوان آن به دقت انتخاب شده بود، ارسال می‌شد. در عنوان نامه ذکر می‌شد: «این همون مدرکیه که می‌خواستی ... به کسی نشونش نده».[1] با این تیتر، وانمود می‌شد که نامه را یک دوست ارسال کرده است. اوایل، عدهٔ زیادی از گیرندگان نامه را باز می‌کردند. به محض بازکردن نامه، حمله همه‌جانبه ویروس آغاز می‌گشت (السان، ۱۳۹۶: ۱۴۲).

اغلب نامه‌ها و پیام‌های خطرناک، عناوین جذابی مشابه ویروس ملیسا دارند. تیتر کرم معروف به «نامه عاشقانه» (Love Letter Worm) این بود: «دل‌انگیز، نامه عاشقانه پیوست را که ازم رسیده،

1. “Here is that document you asked for … don't show anyone else”.

چک کن».[1] عناوین خطرناک دیگر، اعلام برنده شدن گیرنده در بخت‌آزمایی یا اعلام انتخاب شانسی وی برای دریافت گرین‌کارت (اقامت) است. در چنین مواردی، اغلب از شخص گیرنده خواسته می‌شود که فرم خاصی را پر کرده و با پیوست کردن برخی از مدارک به آن، به نشانی پستی یا الکترونیکی ذکر شده در نامه الکترونیکی ارسال نماید. نامه مذکور به لحاظ ظاهری، هیچ چیز فریبنده‌ای ندارد و حتی شماره و نشانی تماس فرستنده در آن قید می‌شود. آنچه که در سراسر این فرایند از نظر کیفری اهمیت دارد آن است که یکی از مدارک مورد نیاز برای طی تشریفات بعدی، واریز مبلغ مشخصی پول به حساب فرستنده می‌باشد. در این مرحله هم، روحیات و افکار عمومی در نظر گرفته می‌شود. زیرا، معمولاً مبلغی که از گیرنده نامه الکترونیکی درخواست می‌شود، چندان زیاد نیست که در او ایجاد ظن نماید یا توان پرداخت آن را نداشته باشد.

مسالهٔ اصلی در خصوص قابل اعتماد بودن محتوای نامه الکترونیکی، اثبات هویت نویسنده آن است. از نظر علمی، این امکان وجود دارد که چند نفر از یک نشانی برای ارسال و دریافت نامه الکترونیکی استفاده کنند. به‌علاوه، ممکن است شخصی بدون اجازه صاحب شناسه (نام عبور) به درون صندوق پستی دسترسی پیدا کند و به جای دارنده شناسه اقدام به ارسال نامه الکترونیکی نماید.

بنابراین ارسال نامه از شناسه معین لزوماً دلالت بر این نمی‌کند که دارنده آن شناسه، فرستنده آن بوده است. بلکه این دلالت زمانی از سوی دادگاه پذیرفته می‌شود که با قراینی همچون محتوا، شرایط و اوضاع و احوال همراه نامه (مانند فایل‌های پیوست) و دلایل خارجی دیگر همراه باشد. در پرونده (Kevin Michael Shea v. The State of Texas (Tex 2005))، دادگاه شهادت زنی را که ۶ بار از مردی نامهٔ الکترونیکی دریافت کرده بود، بر انتساب نامه‌ها به خوانده پذیرفت (السان، ۱۳۹۶: ۱۶۱).

ج. مدیریت و واکنش در فضای مجازی

افرادی را که در برابر جرایم مَجازی، قصد مقاومت و یا دفاع دارند، می‌توان به دو دسته تقسیم‌بندی کرد. دستهٔ اول شامل دولت (قوای عمومی) و دستهٔ دوم شامل بخش خصوصی (اعم از اشخاص حقیقی یا حقوقی) می‌شود. مجموعه اقدامات بخش خصوصی شامل تهیه رهنمودهای امنیت اطلاعات، سامانه‌های رمز، دیواره آتش، برنامه‌های ضد ویروس، ضد جاسوسی و نیز آموزش‌های اجتماعی به کارکنان و افراد مرتبط و نیز تعیین و ابلاغ سیاست‌های امنیتی و ایمنی سازمان است. شرط اساسی موفقیت بخش خصوصی در اقدامات پیشگیرانه و بازدارنده خود در برابر جرایم مجازی

1. Kindly Check the Attached LOVELETTER Coming from Me.

آن است که این فعالیت‌ها، بدون هیچ‌گونه وقفه‌ای استمرار داشته باشد. همچنین اقدامات مذکور باید با تمرکز دقیق بر کمیت و کیفیت سامانه‌های رایانه‌ای طراحی و اجرا شده و بر حسب نیازهای فنی و یا ایمنی، به‌طور مستمر به‌روزرسانی شود.

اقدامات دولت در برابر جرایم مجازی را می‌توان از جنبه‌های مختلف مورد بررسی قرار داد. راهبرد مستقیم دولت، برخورد با بزهکاران مجازی، از طریق جرم‌انگاری دقیق کج‌روی‌های زیانبار فضای مجازی و به کیفر رسانیدن متخلفین است. اقدامات غیر مستقیم دولت، کمک به بخش غیردولتی از طریق وضع، اجرا و نظارت بر مقررات ایمنی را در بر می‌گیرد. در این مفهوم، دولت شامل تمامی قوای حاکم می‌باشد. نیروی نظامی، ارتباطی و اطلاعاتی، از طریق تقویت و نوسازی زیرساخت‌های ارتباطی و مخابراتی، احتمال ارتکاب جرایم مجازی در سطح کلان آن را به حداقل ممکن می‌رساند. همچنین، نهادهای اطلاعاتی و قضایی می‌توانند با شنود الکترونیکی داده‌های در حال مبادله، هر نوع محتوای مجرمانه و ناهنجار را شناسایی کرده و مبادله‌کنندگان آن‌ها را مورد پیگرد قرار دهند.

موفقیت هر نوع راهبردی که برای پیشگیری و پیگرد بزهکاری مجازی، اتخاذ و اجرا می‌شود، مستلزم تعامل مؤثر و مستمر بخش دولتی و غیردولتی است (Turrini & Ghosh, 2010: p.21). در واقع، به‌جای این‌که هر کس حصاری به دور سامانهٔ رایانه‌ای خود بکشد، تعامل دولت و مردم باعث می‌شود که یک محدوده ایمن ملی شکل گیرد که در آن، همه شهروندان به راحتی می‌توانند تجارت الکترونیکی انجام داده و سایر ارتباطات الکترونیکی خود را با استانداردهای بالای فنی و ایمنی برقرار نمایند.

همچنین آموزش صحیح کلیه نیروهای مرتبط با کشف و ابراز دلیل و دادرسی الکترونیکی ضروری است. به موجب ماده ۶۶۲ قانون آیین دادرسی نیروهای مسلح و دادرسی الکترونیکی، «قوه قضائیه موظف است برای آموزش دادرسی الکترونیکی به قضات، کارکنان قضائی، دستگاه‌های تابعه قضائی و مراجع انتظامی اقدام کند».

گفتار دوم. تشریفات کشف جرایم مَجازی

به موجب ماده ۱۱ آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی، «مقام قضایی در جریان تحقیق و فرآیند رسیدگی می‌تواند دستور حفاظت هر نوع داده رایانه‌ای ذخیره شده را از جمله داده‌های رمزنگاری شده، حذف، پنهان، فشرده یا پنهان‌نگاری شده و یا داده‌هایی که نوع و نام آن‌ها موقتاً تغییر یافته و یا داده‌هایی که برای بررسی آنها نیاز به سخت‌افزار مخصوصی می‌باشد، صادر نماید».

کشف جرایم مَجازی، در مقایسه با روند معمول کشف و پیگرد جرایم، نیازمند فنون و توانمندی‌های خاصی است. در این گفتار، به‌طور خلاصه، تشریفات و ضوابطی که می‌توان، به‌طور عملی برای کشف جرایم مجازی مورد استفاده قرار داد، معرفی می‌شود.

منظور از «پلیس» در این گفتار، ضابطین دادگستری و به‌طور کلی، همه اشخاصی است که وابسته به دادسرا بوده و وظیفه کشف جرایم و ادله، حفظ و نگهداری دلایل و ارائهٔ آن‌ها به دادگاه را بر عهده دارند.

بند اول. اصول اولیه حاکم بر تحقیقات مجازی

تحقیقات مربوط به جرایم مجازی، از اصولی تبعیت می‌کند که در تمامی جرایم ـ صرف‌نظر از ماهیت آنها ـ باید مورد توجه نهاد پیگرد قرار گیرد. بسیاری از این ضوابط، همان اصولی هستند که دادسرا و نهادهای ذیربط، برای کشف و پیگرد جرایم معمول به‌کار می‌گیرند. در عین حال، باتوجه به اوصاف خاص فضای مجازی، تعدیل شده‌اند.

به‌عنوان اصل اول، اقدامات تحقیقی نباید باعث تغییر یا تخریب داده‌هایی شود که در سامانه ذخیره شده یا در حال مبادله هستند. همچنین، کشف و پیگرد جرایم نباید موجب اخلال در عملکرد سامانه شود. در همین راستا صدر ماده ۶۷۲ قانون آیین دادرسی نیروهای مسلح و دادرسی الکترونیکی مقرر می‌دارد: «تفتیش و توقیف داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی در حضور متصرفان قانونی یا اشخاصی که به‌نحوی آن‌ها را تحت کنترل قانونی دارند، نظیر متصدیان سامانه‌ها انجام می‌شود».

در ماده۶۸۲ قانون مذکور تصریح شده: «متضرر می‌تواند در مورد عملیات و اقدامات مأموران در توقیف داده‌ها و سامانه‌های رایانه‌ای و مخابراتی، اعتراض کتبی خود را همراه با دلایل ظرف ده روز به مرجع قضایی دستوردهنده تسلیم نماید. به درخواست یادشده خارج از نوبت رسیدگی می‌شود و قرار صادره قابل اعتراض است».

در ماده ۶۶۱ همین قانون برای متخلفین تعیین کیفر شده و مقرر گردیده: «چنانچه اشخاصی که مسؤول حفظ امنیت مراکز، سامانه‌های رایانه‌ای و مخابراتی و اطلاعات موضوع این بخش هستند یا داده‌ها یا سامانه‌های (سیستم) مذکور در اختیار آنان قرار گرفته است بر اثر بی‌احتیاطی یا بی‌مبالاتی یا عدم مهارت یا عدم رعایت تدابیر متعارف امنیتی موجبات ارتکاب جرائم رایانه ای به‌وسیله یا علیه داده‌ها و سامانه‌های رایانه‌ای و مخابراتی را فراهم آورند، به حبس از شش ماه تا دو سال یا انفصال از خدمت تا پنج سال یا جزای نقدی از ده تا صدمیلیون ریال محکوم خواهند شد».

اصل دوم این است که هر جا ـ به‌طور استثنایی ـ نیاز به بازرسی سامانه، داده یا ارتباطات وجود داشته باشد، این امر باید توسط شخص خبره انجام شود. همچنین دلایل توجیهی امر، نتایج به دست آمده از بازرسی و میزان ارتباط آنها با احتمال‌های اولیه ضمن یک گزارش مستند، مشخص گردد.

اصل سوم با بایگانی و ثبت سوابق ارتباط می‌یابد. همه داده‌ها و مدارک به‌دست آمده یا ایجاد شده در فرایند پیگرد کیفری، باید در محلی ایمن نگاهداری شده و دارای برچسب مشخصات ـ و در صورت لزوم، جزئیات ـ باشد. در همین مورد ماده ۱۶ آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی مقرر می‌دارد: «حفاظت از داده‌ها باید به نحوی باشد که محرمانگی، تمامیت، صحت و انکارناپذیری داده‌ها رعایت شود». همچنین به موجب ماده ۶۷۵ قانون آیین دادرسی نیروهای مسلح و دادرسی الکترونیکی، «در توقیف داده‌ها، با رعایت تناسب، نوع، اهمیت و نقش آن‌ها در ارتکاب جرم، به روش‌هایی از قبیل چاپ داده‌ها، تصویربرداری از تمام یا بخشی از داده‌ها، غیرقابل دسترس کردن داده‌ها با روش‌هایی از قبیل تغییر گذرواژه یا رمزنگاری و ضبط حامل‌های داده عمل می‌شود».

آخرین اصل آن است که شخص یا اشخاص معینی باید مسؤولیت اجرای اصول فوق را بر عهده گیرد و حدود اختیارات و وظایف آن‌ها و ضمانت اجرای تخلف از اختیارات از سوی ایشان مشخص شود. ذیل ماده ۶۶۹ قانون فوق در این مورد مقرر می‌دارد: «چنانچه هریک از کارکنان دولت یا ضابطان قضایی یا سایر اشخاص از اجرای این دستور خودداری یا داده های حفاظت شده را افشاء کنند یا اشخاصی که داده‌های مزبور به آنها مربوط می‌شود را از مفاد دستور صادره آگاه کنند، ضابطان قضائی و کارکنان دولت به مجازات امتناع از دستور مقام قضائی و سایر اشخاص به حبس از نود و یک روز تا شش‌ماه یا جزای نقدی از پنج تا ده میلیون ریال یا هر دو مجازات محکوم می‌شوند».

بند دوم. جمع‌آوری و حفظ ادله

در فضای مجازی، جمع‌آوری و نگاهداری ادله شامل شناسایی، تعیین، توقیف و تأمین ادله دیجیتالی، تهیهٔ گزارش از صحنهٔ جرم و مکان‌ها و سامانه‌هایی که ادله در آن یافت شده‌اند، می‌شود. به‌علاوه، در صورت لزوم باید بر روی هرکدام از ادله‌ای که به‌دست می‌آید، توضیح مربوط به مشخصات آن قید شود و ادله به‌دست آمده (اعم از سخت‌افزار و نرم‌افزار) به مکان امنی انتقال یابد.

شخصی که ادله در اختیار وی قرار دارد، باید اطمینان یابد که جمع‌آوری ادله از سوی شخص مجاز انجام می‌گیرد. صرف داشتن کارت شناسایی پلیس، کفایت نمی‌کند. بلکه مأمور قانون باید

اثبات کند که مجوز اقدام خاصی را که درصدد انجام آن است، دارد. همچنین، باید از نیروی ماهر و ابزارهای دقیق استفاده شود تا کشف جرم موجب خسارت به داده‌ها و/یا سامانه‌های رایانه‌ای نشود.

موضوع مهم دیگر، ارزش تحقیقاتی ادله است. پلیس باید بداند که دقیقاً دنبال چه چیزی می‌گردد و برای کشف جرم مجازی مشخص باید از چه سخت‌افزارها و نرم‌افزارهایی استفاده کند. برای این منظور، شناخت فنی پلیس مجازی، نسبت به ویژگی‌های فضای مجازی، افزارهای مورد استفاده در آن و کاربرد هرکدام از افزارها ضرورت دارد.

در این خصوص باید تذکر داد که محتوای دستور مقام قضایی نیز باید روشن و شفاف باشد. به موجب ماده ۶۷۳ قانون آیین دادرسی نیروهای مسلح و دادرسی الکترونیکی، «دستور تفتیش و توقیف باید شامل اطلاعاتی از جمله اجرای دستور در محل یا خارج از آن، مشخصات مکان و محدوده تفتیش و توقیف، نوع و میزان داده‌های موردنظر، نوع و تعداد سخت‌افزارها و نرم‌افزارها، نحوهٔ دستیابی به داده‌های رمزنگاری یا حذف شده و زمان تقریبی انجام تفتیش و توقیف باشد که به اجرای صحیح آن کمک می‌کند».

ادله‌ای که کشف می‌شود، شامل سامانه رایانه‌ای، ابزارهای ذخیرهٔ داده (اعم از هارد، سی‌دی، دیسکت، فلش و کارت‌های حافظه) می‌شود. همچنین رایانه ممکن است قالب‌های مختلفی از قبیل تلفن همراه، رایانه همراه (لپ‌تاب) و دستگاه بازی و سرگرمی داشته باشد (Learner, 2009: pp.11-13). ابزارهای قابل اتصال به رایانه مانند دوربین شبکه (وِب‌کم)، کارت‌خوان‌ها، میکروفون، گوشی و... هم می‌تواند برای ارتکاب جرایم مجازی مورد استفاده قرار می‌گیرد. دستگاه‌هایی همچون ماهواره، دوربین دیجیتالی، انواع مختلف چاپگر، لوازم اتاق گفتگوی اینترنتی (چَت، اعم از صوتی و یا تصویری) و ابرحافظه‌ها هم ممکن است در جهت ارتکاب جرم به‌کار گرفته شوند.

وجود سخت‌افزارهایی همچون کارت شبکه، مودم (سامانه اتصال به اینترنت از طریق تلفن)، رایانه همراه (که قابلیت اتصال به اینترنت را دارد)، سامانه اینترنت بی‌سیم، سامانه اینترنت ماهواره‌ای و موارد مشابه در صحنه (مشکوک به ارتکاب) جرم، نشان می‌دهد که متهم امکان دسترسی به اینترنت را داشته و قرینه‌ای ابتدایی برای قابلیت انتساب بزهکاری اینترنتی به وی می‌باشد.

پلیس، برای کشف ادله، جمع‌آوری و حفظ آن‌ها باید ابزارهای لازم را در اختیار داشته باشد. این ابزارها، از جمله شامل رایانه، انواع کارت حافظه و کارت‌خوان، دوربین دیجیتالی، دستگاه‌های تشخیص وجود شبکه و ردیاب ارتباطات الکترونیکی می‌باشد. از آن جهت که به صرف اتهام نمی‌توان شخص را از حق دسترسی به اموال و اطلاعات خود محروم کرد، پلیس باید تا حد امکان از به هم زدن صحنه خودداری کرده و در صورت لزوم، دستگاه‌ها و سامانه‌ها را در همان محل تحت

بازرسی و کنترل قرار دهد. بدیهی است که اگر امکان ورود به رایانه یا سامانه‌ای، به دلایل مختلف، از جمله رمزگذاری، وجود نداشته باشد، پلیس اختیار توقیف یا مهر و موم آن را خواهد داشت؛ مشروط بر اینکه توجیه کافی برای این اقدام وجود داشته باشد.

قانون آیین دادرسی نیروهای مسلح و دادرسی الکترونیکی فرض کرده است که در مورد تفتیش داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی اصل بر این است که نمی‌توان در وهله اول خود سامانه را توقیف کرد و باید طبق ماده ۶۷۴ این قانون، تفتیش داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی از طریق «دسترسی به تمام یا بخشی از سامانه‌های رایانه‌ای و مخابراتی، دسترسی به حامل‌های داده از قبیل دیسکت‌ها یا لوح‌های فشرده یا کارت‌های حافظه و دستیابی به داده‌های حذف یا رمزنگاری شده» انجام گیرد. مگر این‌که «داده‌های ذخیره شده به سهولت در دسترس نباشد یا حجم زیادی داشته باشد یا تفتیش و تجزیه و تحلیل داده‌ها بدون سامانه سخت‌افزاری امکان‌پذیر نباشد یا متصرف قانونی سامانه رضایت داده باشد یا تصویربرداری از داده‌ها به لحاظ فنی امکان‌پذیر نباشد و یا این‌که تفتیش در محل باعث آسیب داده‌ها شود»؛ که در این صورت خود سامانه رایانه‌ای یا مخابراتی توقیف می‌شود (ماده ۶۷۶ قانون آیین دادرسی نیروهای مسلح و دادرسی الکترونیکی).

بند سوم. ادارهٔ صحنهٔ جرم

در زمان بازرسی و پیگرد، پلیس باید حدود صحنه جرم را مشخص کرده و از ورود و دسترسی افراد غیرمجاز به نرم‌افزارها و سخت‌افزارهای آن محدوده جلوگیری کند. همچنین، اگر رایانه یا سامانه‌ای مشکوک باشد، باید مشخصات دقیق آن، مشخصات کامل کاربر یا کاربران، نوع دسترسی به اینترنت، ابزارها و شیوه‌های مورد استفاده، اطلاعات، کلیه ابزارها، نرم‌افزارها و استانداردهای مورد استفاده، اطلاعات مربوط به نشانی‌های پست الکترونیکی، شبکه‌های اشتراکی،[1] (اگر کاربر یا کاربران در آن‌ها عضویت دارند) و نرم‌افزارهای اصلی و مشکوک نصب شده در سامانه (با تعیین امکان یا عدم امکان بهره‌گیری از آن‌ها در اینترنت)، ثبت و ضبط شود.

۱. برخی از پایگاههای اینترنتی، در تهیه، افزایش و مبادله داده‌های خود به طور کامل یا غالب بر مشارکت کاربران مبتنی هستند. بدین نحو که کاربران متعدد می‌توانند در آنها اقدام به اشتراک گذاشتن انواع مختلف داده (به طور معمول، فیلم، صدا، عکس و متن) نموده یا از داده‌هایی که دیگران به اشتراک گذاشته‌اند، استفاده کنند. تارنماهای مشهوری همچون (Facebook, Youtube, 4shared) مثالهایی برای این وضعیت می‌باشد. شبکه‌های اجتماعی مانند تلگرام، واتس‌آپ، ایمو نیز در این راستا، بعدها توسعه یافته‌اند.

در صورتی‌که توقیف سامانه رایانه‌ای یا مخابراتی لازم باشد، «متناسب با نوع و اهمیت و نقش آن‌ها در ارتکاب جرم با روش‌هایی از قبیل تغییر گذرواژه به‌منظور عدم دسترسی به سامانه، مهر و موم (پلمب) سامانه در محل استقرار و ضبط سامانه صورت می‌گیرد».

بند چهارم. تهیه صورت‌جلسه ثبت جزئیات در صحنه جرم

هرگاه وقوع جرمی احراز شود یا احتمال ارتکاب آن بسیار قوی باشد، باید صورت دقیقی از جزئیات و مشخصات جرم ارتکابی یا احتمالی تهیه شود. گزارش مذکور، به همراه ثبت سوابق و ادله عینی (اعم از سخت‌افزار و نرم‌افزار)، می‌تواند زمینهٔ تحقیق و بررسی‌های بیشتر را فراهم نماید. از این رو، باید در تهیه گزارش و ثبت سوابق، دقت کافی به عمل آید.

هرگاه لازم باشد تا رایانه‌ای به‌منظور کشف رمز یا بازیابی اطلاعات مخفی یا رمزگذاری شده در آن به اداره پلیس منتقل شود، این کار باید با نهایت احتیاط انجام گیرد تا به سخت‌افزار یا اطلاعات موجود در آن صدمه‌ای وارد نشود. همچنین باید دقت کرد که پیش از هر نوع جابجایی، رایانه خاموش باشد. قبل از خاموش کردن، باید با رعایت حریم خصوصی کاربر (دارنده) آن، کلیه اطلاعات ظاهری و مدارک در دسترس صورت‌جلسه شود تا در تحقیقات بعدی مورد استفاده قرار گرفته یا محتوای آن تجزیه و تحلیل شود. به هر حال، برای پیشگیری از بروز مشکلات احتمالی، باید مشخصات دقیق رایانه و لوازم همراه آن ثبت گردد.

هرگاه اطلاعات بر روی صفحه نمایشگر نشان دهد که داده‌هایی در حال پاک شدن بوده یا نرم‌افزاری در حال تخریب، ربایش، جابجایی، رمزگذاری یا اخفای اطلاعات می‌باشد، مامور پلیس باید مهارت لازم را برای خاموش کردن فوری سامانه یا بهترین اقدام فنی لازم برای توقف عملیات خرابکارانه در اولین فرصت ممکن، داشته باشد.

به هنگام بازرسی، باید فعال (در حال انجام) بودن موارد زیر، بررسی گردد و در صورت مثبت بودن پاسخ، در صورت جلسه مربوطه قید شود:

- معامله یا هر نوع تعامل الکترونیکی/ اینترنتی در حال انجام یا انجام یافته.
- چت‌روم (اتاق مَجازی گفتگو).
- مدرک، نوشته یا هر پوشه باز (فعال).
- صفحه ارسال، دریافت یا مشاهده هر نوع پیام.
- صفحه مربوط به تصاویر، فیلم‌ها یا هر نوشته مبتذل.
- اطلاعات و مدارک مالی.
- رمزگذاری در حال انجام داده‌ها.
- هر نوع عملیاتی که غیر قانونی بودن آن محسوس یا محتمل باشد.

گفتار سوم. اعتبار داده‌ها و تشریفات ابراز آن‌ها

در این گفتار به ترتیب اعتبار داده‌های الکترونیکی و سپس تشریفات ابراز و استناد به این داده‌ها به طور تطبیقی مورد بررسی قرار می‌گیرد.

بند اول. اعتبار داده‌های الکترونیکی

امروزه در مورد اعتبار ادلهٔ الکترونیکی و همسانی ارزش اثباتی آن‌ها با ادلهٔ سنتی و کاغذی تردیدی وجود ندارد. هرچند که در ایالات متحده در پرونده‌های متعددی این نتیجه حاصل گردیده که آنچه در شبکه‌های اجتماعی (مانند فیسبوک، اینستاگرام، تلگرام و..) مبادله می‌شود، ممکن است به اندازه آنچه از طریق نامه الکترونیکی یا شبکه‌های معتبر و تحت کنترل ارسال یا مبادله می‌گردد دارای اعتبار و قابل استناد نباشد.[۱]

اما قوانین و مقررات کشورمان از حیث قابلیت استناد بین انواع مختلف داده‌های رایانه‌ای و مخابراتی قایل به تفکیک نشده و تمامی آن‌ها را به شرط ایمنی قابل استناد دانسته است (مؤذن‌زادگان و دیگران، ۱۳۹۴). به موجب ماده ۶۵۵ قانون آیین دادرسی جرائم نیروهای مسلح و دادرسی الکترونیکی، «در هر مورد که به موجب قوانین آیین دادرسی و سایر قوانین و مقررات موضوعه اعم از حقوقی و کیفری، سند، مدرک، نوشته، برگه اجرائیه، اوراق رأی، امضاء، اثر انگشت، ابلاغ اوراق قضائی، نشانی و مانند آن لازم باشد صورت الکترونیکی یا محتوای الکترونیکی آن حسب مورد با رعایت سازوکارهای امنیتی مذکور در مواد این قانون و تبصره‌های آن کافی و معتبر است».

در کامن‌لا، بحثی به نام اصالت (Authentication; Genuineness) یا تصدیق به‌عنوان لازمه اعتبار ادله، به ادله الکترونیکی هم تسری یافته است. به طور خلاصه، مقصود از اصالت آن است که یک هیأت منصفه معمول (و نه دادرس یا کارشناس) آن را اصل بداند یا در مورد ادله‌ای که موضوعی را توضیح می‌دهند، آن دلیل به‌نحوی باشد که موضوع را به‌طور دقیق توصیف نماید (Goode, , 2009-2010: p. 8). اصالت در این توصیف و منحصراً در مورد نوشته یا معادل آن، به معنای واقعی بودن و تنظیم آن بدون قصد و غرض (با صداقت) می‌باشد. از این‌رو، می‌توان به‌جای

۱. از جمله پرونده های زیر:
United States v. Jackson, 208 F.3d 633 (7th Cir. 2000); Commonwealth v. Williams, 926 N.E.2d 1162 (Mass. 2010); People v. Lenihan, 30 Misc. 3d 289, 911 N.Y.S. 2d (N.Y. Sup. Ct. 2010); (See: Rashbaum, Kenneth N. et al, 2011-2012: p. 60).

آن در زبان فارسی، اصطلاح «قابل اعتماد بودن» را به‌کار برد.[۱] زیرا اصالت در برابر مجعول بودن، بیشتر کاربرد دارد.

قابل اعتماد بودن یا معتبر بودن دلیل الکترونیکی، یک مساله عرفی است[۲] و جز در مواردی که میان اصحاب دعوا یا در کشورهایی که از هیأت منصفه در روند دادرسی استفاده می‌کنند، میان اعضای این هیأت اختلاف پیش نیاید، لازم نیست صرف اثبات اصالت (اعتماد) به کارشناس ارجاع شود.

در حقوق ایالات متحده، برای احراز اصالت دلیل الکترونیکی از معیارهای مختلفی اثبات می‌شود که در مواد ۹۰۱ و ۹۰۲ قواعد فدرال درباره ادله[۳] آمده است. از جمله این معیارها، شهادت یک شاهد دارای اطلاع شخصی از اصالت، ویژگی متمایزکننده دلیل مورد تردید، سوابق یا گزارش‌های عمومی، پردازش یا قرار داشتن در یک سامانه، انتشار رسمی، سند تجاری و مواردی از این قبیل می‌باشد.

بند دوم. ابراز داده‌های الکترونیکی

در بحث تفتیش و ابراز داده‌ها باید توجه داشت که به‌عنوان یک اصل پذیرفته شده جهانی، در روند دسترسی به داده نباید اقدامات خلاف قانون یا خلاف حقوق اساسی اشخاص صورت گیرد. زیرا به موجب اصل ۳۸ قانون اساسی جمهوری اسلامی ایران و ماده ۸ کنوانسیون اروپایی حقوق بشر، تحصیل دلیل از طریق نامشروع مجاز نیست و دلیل حاصله به این شیوه‌ها قابل استناد نمی‌باشد (Arslan, 2013: p. 32).

به‌عنوان قاعده دیگر، پیش‌شرط ابراز داده، همکار متهم/خوانده در این زمینه می‌باشد. بنابراین هرگاه دستور مقام قضایی یا قانونی مبنی بر تأمین دلیل یا تفتیش (بازرسی/ معاینه محل) صادر شده باشد، طرف دعوا نمی‌تواند در برابر اجرای آن مانع ایجاد کند.[۴] ماده ۳۱ آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی، «اشخاصی که داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی را تحت کنترل و یا تصرف دارند، موظف به همکاری در اجرای دستور تفتیش و توقیف می‌باشند».

---

۱. یکی از پژوهشگران حقوق سایبر از واژه «اعتبار» و معتبر بودن استفاده کرده است. ر.ک.: (جلالی‌فراهانی، ۱۳۸۶، ص ۹۵).

2. Ricketts v. City of Hartford, 74 F.3d 1397 (2nd Cir. 1996).

3. Fedral Rules of Evidence; See: www.law.cornell.edu/rules/fre/

4. Celanese Canada Inc. v. Murray Demolition Corp., [2003] O.J. No. 4211 (QL); See: (Sells and Collins, 2010: p. 314).

هرچند، «اصولاً در امور کیفری، دلایل از قبل آماده نمی‌شوند بلکه بعد از واقعه مجرمانه باید در پی جمع‌آوری آنها بود. به عبارت دیگر، برخلاف امور حقوقی که معمولاً طرفین یک رابطه حقوقی در هنگام ایجاد حقوق و تکالیف ناشی از آن، به ایجاد دلیل اثبات آن مبادرت می‌ورزند تا در موقع لزوم نسبت به الزام طرف مقابل به اجرای تعهدات خود اقدام نمایند، در امور کیفری، اصولاً اثبات وقایعی مطرح است که تحقق آنها از پیش معلوم نبوده و کسی درصدد تهیه دلیل اثبات آن نیز برنیامده است» (خالقی، ۱۳۸۸: ۴۰۴ـ۴۰۳). به نظر می‌رسد که در فرایند تفتیش و ابراز داده نباید مقررات و تشریفات حاکم بر این مورد را در دعاوی حقوقی و کیفری از هم تفکیک و متمایز کرد. همان گونه که در برخی کشورهای دیگر نیز استانداردها و معیارهای قابلیت استناد به ادله الکترونیکی بدون تمایز میان دعاوی مقرر شده است. برای مثال در کانادا استانداردهایی باعنوان «سوابق الکترونیکی به عنوان ادله استنادی»[1] تدوین گردیده است (Chasse, 2011: p. 298).

در ایالت متحده نیز باتوجه به مسایل و چالش‌هایی که ادله الکترونیکی ـ به‌ویژه مدارک مرتبط با رایانه‌ها و تلفن‌های همراه ـ به‌وجود آورده، دادگاه‌ها استانداردها و میعارهای ارزیابی ادله را بر مبنای نوع دلیل و نه نوع وسیله‌ای که برای تولید، بازیافت، فرآوری، ذخیره یا مبادله و استفاده از دلیل به‌کار گرفته شده، به نحو موسعی به‌کار می‌گیرند (Thomson, 2013: p. 32).

در صورتی‌که متهم/خوانده از ابراز ارادی دلیل در موارد موجه قانونی خودداری نماید، نوبت به کشف و تفتیش دلیل می‌رسد. در امارات متحده عربی، ورود به متصرفات متهم برای کشف دلیل توسط پلیس قضایی حداقل در دو مورد مستلزم أخذ مجوز قبلی از مقام قضایی نمی‌باشد. اولین مورد این‌که به موجب ماده ۵۳ قانون آیین دادرسی کیفری امارات، اگر جرم در حال وقوع (مشهود) باشد و قراین قوی مبنی بر این امر وجود داشته باشد که متهم در منزل خود وسایل یا مدارکی را که می تواند منجر به کشف حقیقت شود، مخفی کرده است نیازی به چنین مجوزی نیست. همچنین به موجب ماده ۵۴ همان قانون، در مواردی که متهم به موجب قانون یا دستور قضایی به اتهام جنایت یا جنحه تحت پیگرد باشد، پلیس می‌تواند در فرایند تعقیب و شنود متهم، بدون نیاز به أخذ مجوز از مقام قضایی در متصرفات وی وارد شود (Aljneibi, 2013: p. 121).

در حقوق کشورمان به موجب ماده ۲۷ آیین‌نامه جمع‌آوری و استنادپذیری ادلۀ الکترونیکی، «تفتیش و توقیف در مواردی که مستلزم ورود به منازل و اماکن خصوصی باشد، مطابق مقررات مندرج در آیین دادرسی کیفری خواهد بود». وفق ماده ۵۵ قانون آیین دادرسی کیفری، «ورود به منازل، اماکن تعطیل و بسته و تفتیش آن‌ها، همچنین بازرسی اشخاص و اشیاء در جرائم

1. Electronic Records as Documentary Evidence, Standard by Canadian General Standards Board, 03/01/2017.

غیرمشهود با اجازه موردی مقام قضائی است، هر چند وی اجرای تحقیقات را به‌طور کلی بـه ضـابط ارجاع داده باشد». همچنین به موجب ماده ۱۴۱همان قانون، «دستور مقـام قضـائی بـرای ورود بـه منازل، اماکن بسته و تعطیل، تحت هر عنوان باید موردی باشـد و موضـوعی کـه تفتـیش بـرای آن صورت میگیرد، زمان، دفعات ورود، اموال، اماکن و نشانی آنها به صـراحت مشـخص شـود. ضـابطان مکلفند ضمن رعایت دستورهای مقام قضائی، کیفیت تفتیش و بازرسی و نتیجه را در صورت اجلس تنظیم کرده، آن را به امضاء یا اثر انگشت متصرف برسانند و مراتب را حداکثر ظرف بیسـت و چهـار ساعت به مقام قضائی اعلام کنند».

بند سوم. روند کشف جرایم در داده‌های در حال مبادله

مداخله در فرایند رد و بدل کردن داده‌هایی که توسط بزهکاران در حال جابجایی می‌باشـد، یکـی از شیوه‌های نوین پیشگیری از جرم به‌شمار می‌آید. در واقع، پیشـگیری از جـرم مـوردنظر در رویکـرد جدید به جرم‌شناسی (جرمشناسی نو) بر شناسایی عامـل‌هـای بزهکـاری بـه‌منظـور تعریـف تـدابیر پیشگیرنده اجتماعی – فردی مبتنی نیست بلکه با هـدف تشـخیص و شناسـایی سـیمای جنـایی و ویژگی‌های گروه‌های خطردار (عامل‌های اجتماعی به مثابه عامل‌های خطر بزهکاری) و وضعیت‌های خطردار (عامل‌های وضعی، فنی، فناورانه) برای نظارت بهتر بر آنان به منظـور تـوانگیری در زمـان و مکان صـورت مـی‌گیـرد (Criminology, A Sociological Introduction, p.107 بـه نقـل از: نجفی‌ابرندآبادی، ۱۳۸۸: ۷۴۵).

پلیس ممکن است به این نتیجه برسد که داده‌های در حال مبادله، می‌توانـد کمـک زیـادی بـه کشف جرایم تحت پیگرد نماید یا حاوی اطلاعاتی است که مبادله آن به‌دلیل نقض حریم خصوصی، مغایرت با منافع عمومی یا دلایل دیگر قانونی نیست. هرگاه مبادله داده از داخل کشور بـه خـارج از آن صورت گیرد، یافتن اطلاعات جزئی در خصوص مشخصات گیرنده داده‌ها، هدف نهایی از مبادلـه داده و اقداماتی همچون استرداد آن‌ها، اغلب از طریق رایانه و شـبکه امکـان‌پـذیر نبـوده و نیازمنـد همکاری و تعامل میان کشورهاست.

در انگلیس، اصل بر این است که مبادله داده و محتوای هـر ارتبـاطی، امـری قـانونی محسـوب می‌شود؛ اما هرگاه در مورد داده‌های خصوصی، عدم رضایت ذینفـع داده اثبـات گـردد یـا در مـورد داده‌های دارای محتوای عمومی، ثابت شود که بدون اجازه مقام صالح انتشار یافته یـا مبادلـه شـده است، عنوان مجرمانه خواهد داشت.[1] در حقوق کشورمان، به موجب ماده ۱۷ ق.ج.ر، انتشار یا فراهم

1. UK, Regulation of Investigatory Powers Act 2000; (Reed & Angel, p.323).

کردن امکان دسترسی به داده‌های خصوصی، بدون رضایت ذینفع جرم اعلام شده است. علاوه بر آن، ماده ۷۵ ق.ت.ا، نقض اسرار تجاری را در بستر مبادلات الکترونیکی، جرم شناخته است.

همچنین وفق ماده ۶۸۳ قانون آیین دادرسی نیروهای مسلح و دادرسی الکترونیکی، «کنترل محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی مطابق مقررات راجع به کنترل ارتباطات مخابراتی مقرر در آیین دادرسی کیفری است». تبصره همین ماده نیز تصریح دارد: «دسترسی به محتوای ارتباطات غیرعمومی ذخیره شده، نظیر پیام‌نگار (ایمیل) یا پیامک در حکم کنترل و مستلزم رعایت مقررات مربوط است».

همانطور که بررسی قوانین و مقررات مختلف کشورمان در خصوص ادله الکترونیکی نشان می‌دهد، مقنن در امور حقوقی، نظام قانونی ادله را پذیرفته و کوشش کرده که حتی ادله الکترونیکی را نیز در یکی از قالب‌های سنتی ادله قرار دهد. ماده ۱۳ ق.ت.ا به وضوح بر همین امر دلالت دارد (ساعی و باباخانی، ۱۳۹۱: ۱۷۵). این در حالی است که در دادرسی کیفری، همچنان نظام اقناعی حکومت دارد و دادرس می‌تواند از هر دلیل یا اماره الکترونیکی به حقیقت رسیده و آن را قرینه‌ای برای کشف حقیقت لحاظ نماید. به علاوه، ادله در دادرسی کیفری طریقت داشته و راهی برای رسیدن دادرس به علم محسوب می‌شوند؛ از این‌رو، دادرس می‌تواند بنابر یک تعبیر از هر دلیل و قرینه‌ای برای رسیدن به علم بهره گیرد که در این صورت، صدا و تصویر ضبط‌شده نیز قابل استناد خواهد بود.

در یک رویکرد دیگر، در نظام ادله قانونی که می‌توان آن را «اقناع وجدانی قانون‌گذار» نامید، مقنن دلیل یا ادله قابل قبول و ارزش اثباتی هر یک یا مجموعه‌ای از آن‌ها را پیشاپیش تعیین و دادرسی را در صورت ارائه دلیل یا ادله مورد نیاز و صرف از اعتقاد درونی او، موظف به صدور حکم محکومیت نموده است و در صورت عدم ارائه دلایل مورد نظر مقنن، قاضی مکلف به تبرئه نمودن متهم است و حق ندارد به‌دلیل دیگر استناد کند (آشوری، ۱۳۸۸: ۲۳۳).

باوجود طریقیت ادله در حقوق کیفری باید در مورد صدای ضبط شده قبول کرد که «در صورت احراز اخطار و هشدار قبلی، به واسطهٔرعایت اخلاق آن صدا قابل استناد خواهد بود و اگر چنین نباشد، با توجه به این‌که هدف وسیله را توجیه نمی‌کند و عقاب بلابیان قبیح است و ماهیتاً میان استراق سمع و شنود غیرمجاز و تحصیل و ضبط صدا بدون اخطار، تفاوتی نیست و این احتمال وجود دارد که صدای ارائه شده تقلیدی باشد که به‌خودی خود مذموم و غیراخلاقی است، به‌نظر می‌رسد چنین اطلاعاتی به‌عنوان دلیل قابل استناد و حتی بررسی نباشد» (محسنی و رضایی‌نژاد، ۱۳۹۰: ۸۰).

بند چهارم. سهم دلیل و دادرسی الکترونیکی در نظام دادرسی

اگرچه به موجب ق.ت.ا و قوانین و مقرراتی دیگری که در این مقاله بررسی شد، داده‌پیام در حکم نوشته محسوب می‌شود و ارزش اثباتی آن مورد تردید نیست؛ اما هنوز هم قضات و داورانی که مسلط به رایانه باشند، بسیار کم هستند. با توجه به این‌که مقام رسیدگی‌کننده باید بر موضوع و فرایند دادرسی تسلط داشته باشد، نمی‌توان انتظار داشت که برای تمامی امور از کارشناس استفاده شود.

علاوه بر این، ارائه تمامی دلایل و امارات به‌صورت الکترونیکی، یا غیرممکن و یا بسیار هزینه‌بر است. در مشاهده و ارزیابی دلایل هم دادرسان و داوران به کاغذبازی و میزِ کاری که بتوانند در آنجا همه چیز را در کنار هم ببینند، عادت کرده‌اند (Philippe, 2002: p. 169).

در مقابل باید قبول کرد که به دلایل مختلف، قالب الکترونیکی مدارک و سوابق بسیار مفید است. اول این‌که، انتقال الکترونیکی اطلاعات (در قالب‌های مختلف)، بسیار سریع‌تر و ارزان‌تر از ارسال پستی یا ابلاغ از طریق مامور انجام می‌شود. دوم این‌که، جستجوی اطلاعات در رایانه بسیار راحت‌تر از گشتن به دنبال آن‌ها در بایگانی نامنظم دفاتر شعب دادگاه می‌باشد. سوم این‌که، بایگانی انواع اطلاعات و سوابق به‌صورت الکترونیکی، بسیار ارزان و مدیریت سوابق بایگانی شده بسیار آسان است.

البته امکاناتی که ارتباطات الکترونیکی فراهم سازد، نباید ناقص اصل «دسترسی به دادگاه صالح» باشد. به این معنا که تنها در صورتی می‌توان دادرسی الکترونیکی را (در قالب رسیدگی قضایی، داوری و..) مجاز دانست که از دسترسی هر دو طرف دعوا و مرجع رسیدگی به ابزارهای مناسب ارتباط الکترونیکی اطمینان حاصل شود. انجام مستمر تجارت الکترونیکی و پذیرش شیوه حل و فصل الکترونیکی اختلافات احتمالی، به‌عنوان شرط ضمن عقد، داشتن تارنمای فعال و تاکید بر پذیرش شیوهٔ دادرسی الکترونیکی و یا ارجاع به رسیدگی مرجعی که تنها به‌صورت الکترونیکی اقدام به دادرسی می‌کند، از جمله اماراتی هستند که نشان می‌دهد شخص یا اشخاص مرتبط با یک اختلاف، امکانات لازم را برای دادرسی الکترونیکی در اختیار دارند و اقدام به دادرسی با استفاده از وسایل ارتباط الکترونیکی، موجب نقض حق دسترسی آن‌ها به فضای شایسته نمی‌شود (السان، ۱۳۹۶: ۲۸۲).

نتیجه‌گیری و پیشنهاد

دادرسی جرایم مجازی، همانند سایر جرایم، نیازمند توجه به ادله و مدارک مرتبط است. در این راستا، دادگاه می‌تواند ارائه‌دهندگان خدمات دسترسی، کاربران سامانه‌های رایانه‌ای و مخابراتی،

ارائه‌دهندگان خدمات میزبانی داخلی و سایر افراد مرتبط با داده‌ها را به ارائه آن‌ها ملـزم کنـد. ایـن الزام قضایی با ضمانت اجرای کیفری همراه است. چرا که بنابر مـاده ۳۵ ق.ج.ر، متخلـف از دسـتور دادگاه به حکم همان دادگاه، به حبس یا جزای نقدی یا هر دو مجازات محکوم خواهد شد.

ارائه و ابزار داده‌ها در دادگاه، با همان محدودیت‌های روبـرو مـی‌باشـد کـه در جهـت صـیانت از حقوق متهم و اشخاص ثالث برقرار است. بنابراین، دادگاه در دستور خود، باید نوع داده و محـدوده و نحوه ابراز آن‌ها را به‌طور دقیق مشخص سازد. همچنین اگر شخص ثالث در داده‌هـایی کـه ابـزار یـا ارائه آن‌ها موضوع دستور است، ذینفع باشد، اجرای دستور باید حتی‌الامکان بـا اطـلاع یـا در مـوراد مهم، با رضایت شخص ثالث باشد. بدیهی است که رعایت نکردن این محدودیت‌ها می‌توانـد حسـب مورد مسؤولیت دادرس یا مقام مجری دستور را در پی داشته باشد.

قواعد و تشریفات حاکم بر کشف، نگاهداری و ابراز و استناد به ادلهٔ الکترونیکی باید بـه صـورت استاندارد و بدون تفکیک میان دعاوی حقوقی و کیفری ارائه شوند. در واقع، وجود قانون یا مقرره‌ای که این دسته از ادله اثباتی را به‌صورت یکجا و مشخص ذکر کرده و در صورت ضرورت به‌روزرسـانی شود، از شکل‌گیری رویه‌ها و دیدگاه‌های متعارض یا متفاوتی که می‌تواند آثار منفـی در پـی داشـته باشد، پیشگیری خواهد کرد.

منابع

آشوری، محمد، (۱۳۸۸)، **آیین دادرسی کیفری**، جلد دوم، تهران: انتشارات سمت.

آیـــین‌نامـــه جمـــع‌آوری و اســـتنادپذیری ادلـــه الکترونیکـــی، مصـــوبه شـــماره ۱۰۰/۲۸۱۹۹/۹۰۰۰ـ۱۳۹۳/۰۵/۱۲ ریـیس قـوه قضـاییه، روزنامـه رسـمی (ویـژه‌نامـه) شـماره ۷۰۳ـ۱۳۹۳/۰۵/۱۵.

السان، مصطفی، (۱۳۹۶)، **حقوق تجارت الکترونیکی**، چاپ چهارم، تهران: انتشارات سمت.

السان، مصطفی، (۱۳۹۶)، **حقوق فضای مجازی**، چاپ ششم، تهران: انتشارات شهر دانش.

جلالی‌فراهانی، امیرحسین (۱۳۸۶)، «استنادپذیری ادله الکترونیکی در امور کیفری»، **فصلنامه فقه و حقوق**، شماره ۱۵، زمستان.

جمالی، جعفر و رزاقی، افشین (۱۳۹۴)، «نقش و ارزش اسناد کتبی و الکترونیکی در نظـام حقـوقی ایران»، **مجله تحقیقات حقوق خصوصی و کیفری**، شماره ۲۳، بهار ۱۳۹۴.

خالقی، علی، (۱۳۸۸)، **آیین دادرسی کیفری**، تهران: نشر مؤسسه پژوهش‌های شهر دانش.

ساعی، سید محمدهادی، و رضا باباخانی (۱۳۹۱)، «بررسی ارزش اثباتی اسناد الکترونیک در حقوق ایران»، **پژوهشنامه حقوق اسلامی**، شماره ۳۵.

محسنی، حسن و رضایی‌نژاد، امیرحسین (۱۳۹۰)، «حقوق و اخلاق؛ اخلاق و دادرسی: تأملاتی پیرامون اعتبار صدای ضبط شده بدون اخطار»، **مجله حقوقی دادگستری**، دوره ۷۵، شماره ۷۳، بهار.

قانون آیین دادرسی نیروهای مسلح و دادرسی الکترونیکی، مصوب ۱۳۹۳/۰۷/۰۸ کمیسیون قضایی و حقوقی مجلس شورای اسلامی.

مؤذن‌زادگان، حسن‌علی؛ سلیمان دهکردی، الهام؛ یوشی، مهشید (۱۳۹۴) «حفظ صحت و استنادپذیری ادله الکترونیک با استفاده از بیومتریک و رمزنگاری»، **مجله پژوهش حقوق کیفری دانشگاه علامه طباطبایی**، شماره ۱۲، پاییز ۱۳۹۴.

نجفی‌ابرندآبادی، علی‌حسین (۱۳۸۸)، «کیفرشناسی نو، جرم‌شناسی نو، درآمدی بر سیاست جنایی مدیریتی خطرمدار»، **تازه‌های علوم جنایی** (مجموعه مقاله‌ها)، تهران: انتشارت میزان.

نجفی‌ابرندآبادی، علی‌حسین (۱۳۸۷)، **مختصر جرم‌شناسی** (خلاصه مباحث جرم‌شناسی دکتر نجفی‌ابرندآبادی)، تدوین مجتبی جعفری، (بی‌نا)، فروردین.

Aljneibi, Khaled, (2013), Search and Seizure for Electronic Evidence: Procedural Aspects of UAE's Legal System, Evidence and Electronic Signature Law Review, Vol. 10.

Arslan, Çetin, (2013), An Evaluation of Evidence Obtained through Electronic Surveillance in Criminal Procedure, Ankara Bar Review, Vol. 6.

Chasse, Ken, (2011), Electronic Records for Evidence and Disclosure and Discovery, Criminal Law Quarterly, Vol. 57.

Chung, Christine Sgarlata & Byer, David J, (1997), The Electronic Paper Trial: Evidentiary Obstacles to Discovery and Admission of Electronic Evidence, Boston University Journal of Science & Technology Law, Vol.4.

Electronic Records as Documentary Evidence, Standard by Canadian General Standards Board, 03/01/2017.

Givens, Shane J, (2003-2004), The Admissibility of Electronic Evidence at Trial: Courtroom Admissibility Standards, Cumberland Law Review, Vol. 34.

Goode, Steven, (2009-2010), The Admissibility of Electronic Evidence, Review of Litigation, Vol. 29 (1).

Learner, David E (2009), (Editor) Electronic Crime Scene Investigation, Nova Science Publishers, New York, pp.11-13.

Philippe, M, (2002), Where is Everyone Going with Online Dispute Resolution, International Business Law Journal, No. 2.

Rashbaum, Kenneth N. (2011-2012), et al, Admissibility of Non-US Electronic Evidence, Richmond Journal of Law & Technology, Volume XVIII, Issue 3. 1.

Reed, Chris and Angel, John (2003), (Editors), Computer Law, Fifth Edition, Oxford University Press, New York.

Sells, Berkley D. and Ian Collins, (2010), Strategies to Obtain Electronic Evidence, The Advocates' Quarterly, Volume 36, Number 3, January.

Thomson, Lucy L., (2013), Mobile Devices New Challenges for Admissibility of Electronic Evidence, SciTech Lawyer, Volume 9, Number 3, Winter/Spring.

Turrini, Elliot & Ghosh, Sumit (2010), A Pragmatic, Experimental Definition of Computer Crimes, In: Ghosh, Sumit & Turrini, Elliot (Editors), Cybercrimes: A Multidisciplinary Analysis, Springer.

UK, Regulation of Investigatory Powers Act 2000.

US Fedral Rules of Evidence; See: www.law.cornell.edu/rules/fre/

پرونده‌ها و رویه قضایی مرتبط:

Armstrong v. Executive Office of the President , 1 F.3d 1274 [DC Cir Cir 1993].

Celanese Canada Inc. v. Murray Demolition Corp., [2003] O.J. No. 4211 (QL).

Commonwealth v. Williams, 926 N.E.2d 1162 (Mass. 2010)

People v. Lenihan, 30 Misc. 3d 289, 911 N.Y.S. 2d (N.Y. Sup. Ct. 2010).

United States v. Jackson, 208 F.3d 633 (7th Cir. 2000)