

چالش‌ها و خلأهای موجود در فرایند رسیدگی به جرایم سایبری

جواد طهماسبی*

خیرالله شاهمرادی**

چکیده

به کارگیری فناوری اطلاعات و ارتباطات و به تبع آن استفاده از فضای سایبر، جوامع بشری را در تمامی عرصه‌های اجتماعی، اقتصادی، فرهنگی و مذهبی با چالش‌های نوینی مواجه نموده است. جرایم ارتكابی در این فضا از ویژگی‌ها و خصوصیات متمایز از جرایم فضای واقعی برخوردارند. ویژگی‌های منحصر به فردی همچون نامحدود و ناملموس بودن، قابلیت دسترسی آسان و سریع، سهولت در تغییرپذیری و ناشناختگی که بر سرعت ارتكاب جرایم در این فضا افزوده است، مهم‌ترین این ویژگی‌ها است. بالتبع برخورد با این جرایم در فضای سایبر روش خاص خود را می‌طلبد. پس از گذشت زمانی کوتاه از پیشرفت فناوری اطلاعات و ارتباطات، این ضرورت حیاتی محرز گردید که دغدغه حقوق کیفری بر سر پدیده‌های مجرمانه رایانه‌ای، بیشتر در حقوق جزای شکلی یا همان آیین دادرسی کیفری نهفته است، زیرا نه تنها فضای سایبر به کلی مبانی و ارکان تشکیل‌دهنده این حوزه را دستخوش تحولات بنیادین کرده است، بلکه دروازه تبلور و تحقق حقوق جزای ماهوی سایبری نیز به شمار می‌رود. هرگونه نارسایی و ناتوانی در تبیین و اجرای موازین آیین دادرسی کیفری سایبری، بهترین جرم‌انگاری‌ها را هم با شکست مواجه و قوانین کیفری را متروک می‌سازد. همچنین موجب تجری مجرمان می‌گردد، زیرا آنها ملاحظه می‌کنند که کوشش جامعه برای کنترل و پاسخ مناسب با شکست مواجه شده و با توان بیشتری به هنجارشکنی خود ادامه می‌دهند. از این رو نوین بودن جرایم سایبری و شیوه ارتكاب

* دادیار دیوان عالی کشور و عضو هیأت علمی دانشگاه آزاد اسلامی واحد تهران شمال

Tahmasebi.dr@gmail.com

** دانش‌آموخته کارشناسی ارشد حقوق جزا و جرم‌شناسی (نویسنده مسئول)

Shahmoradikhirollah@yahoo.com

تاریخ پذیرش: ۹۶/۰۷/۲۳

تاریخ دریافت: ۹۶/۰۴/۰۹

این‌گونه جرایم، نحوه رسیدگی و تعقیب را از جهت مسائل آیین دادرسی با چالش‌ها و خلأهایی مواجه نموده است که تدابیر کلاسیک حقوقی به هیچ‌عنوان پاسخگو نیستند و رسیدگی به این جرایم با مشکلات عدیده‌ای روبه‌رو است.

کلیدواژه‌ها: فضای سایبر، جرایم سایبری، رسیدگی به جرایم سایبری، آیین دادرسی کیفری.

با پیدایش رایانه و جرم رایانه‌ای و همچنین گسترش شبکه‌های محلی و پیدایش شبکه‌های گسترده در کنار فناوری مخابراتی که منجر به پیدایش فضای جدید به نام فضای سایبر شده است، جرایم جدید با خصوصیات و ویژگی‌های خاص به وجود آمده که به لحاظ همین خصوصیات، در چنین جرایمی قواعد سنتی حاکم بر فرایند در رسیدگی به چالش کشیده شده است. به گونه‌ای که این قواعد فقط پاسخگوی قسمت اندکی از جرایم جدید می‌باشند و برای بخش اعظم این جرایم وضع قواعد تازه مقتضی است.

به دلیل وجود حساسیت‌های مضاعف که نسبت به حوزه‌های شکلی مقررات جزایی وجود دارد، مقررات شکلی فضای سایبر بسیار بیشتر از حوزه‌های ماهوی تحت تأثیر قرار گرفته است. به عنوان مثال، ممکن است یک سوءاستفاده مالی سایبری با عنوان مجرمانه‌ای در قوانین موجود منطبق باشد و در هر حال، قانون‌گذار نیازی به جرم‌انگاری جدید نبیند تا بی‌جهت به تورم کیفری دامن زند. این وضعیت در مورد امور شکلی قدری دشوار است. به عنوان یک مصداق، تعیین محل ارتکاب جرم در فضای سایبر با معیارهای سنتی غیر ممکن است، اولین مسأله‌ای که مطرح می‌شود، مرجع ذی صلاح کیفری است که اگر به فراسوی مرزها کشیده شود، در این وضعیت علاوه بر کشمکش‌های محاکم داخلی، باید منتظر اختلافات ناشی از امکان اعمال صلاحیت کشورهای بسیاری بود. همچنین، مصداق مهم دیگر زمانی است که تمامی عناصر متشکله جرم در دنیای فیزیکی محقق شده و تنها دلایل و امارات مثبت آن در فضای سایبر قرار دارد، اینجا نیز بخش مهمی از مقررات شکلی حقوق جزا، یعنی استناد پذیری کیفری ادله با چالش جدی مواجه است. زیرا داده‌های الکترونیکی به کلی با اسناد و مدارک موجود در فضای واقعی تفاوت دارند و نمی‌توان به ضوابط و مقررات حاکم بر آن استناد نمود.

بدین ترتیب برخلاف قوانین ماهوی که تا حدودی با رجوع به قوانین کیفری موجود امکان تعقیب مجرمان وجود دارد، در حوزه مباحث شکلی، اصل اولیه و ضروری این است که مقررات جدیدی مطابق شرایط خاص و منحصر به فضای سایبر تدوین گردد. به عبارت دیگر، حتی اگر کشوری به طور کلی خود را از جرم‌انگاری جدید مستغنی ببیند، به هیچ وجه نمی‌توان با توجه به شرایط خاص حاکم بر سازوکارهای فضای سایبر حتی به شکل مسامحه‌آمیز از رهگذر مقررات شکلی سنتی برخوردار لازم صورت گیرد. به طور مثال یک بستر واحد و غیرملموس جولانگاه مجریان قانون تمامی

کشورهاست و باید خود را با شرایط و مقتضیات خاص آن وفق دهند. در غیر این صورت، حتی اگر مقرره‌ای در یک سند بین‌المللی یا منطقه آمده باشد، بدون اجرا خواهد ماند. کما اینکه مقررات کیفری کنوانسیون اروپایی جرایم سایبر به چنین سرنوشتی دچار شده‌اند.^۱

وضعیت دیگری که نو بودن جرایم سایبری و شیوه ارتکاب این‌گونه جرایم، نحوه رسیدگی و تعقیب را در قلمرو مسائل آیین دادرسی با چالش‌هایی روبه‌رو نموده است، به طوری که تدابیر کلاسیک حقوقی به هیچ‌عنوان پاسخگو نبوده و با مشکلات عدیده‌ای در این زمینه مواجه است، قواعد شکلی سنتی مربوط به تحصیل و جمع‌آوری دلایل همچنین استنادپذیری آن است. در قلمرو سنتی این امر به صورت فیزیکی بوده و قاضی تحقیق یا ضابطان با مراجعه به محل وقوع جرم و بررسی کیفیت وقوع آن و یا بازجویی و تحقق از افراد محل و یا با دستگیری مجرم و بازجویی از او و یا اقرار متهم می‌توانند به حقیقت امر پی ببرند، در حالی که در فضای سایبر صحنه وقوع جرم کاملاً متفاوت است و مکان وقوع جرم هم مشخص نیست. در نتیجه نه بررسی محل وقوع جرم ممکن است و نه تحقیقات از اهالی محل امکان دارد. از طرف دیگر چیزی به‌عنوان آثار جرم غالباً وجود ندارند که دلالتی بر انتساب آن به متهم و یا حتی وقوع آن داشته باشد.

نوع تحقیق، بازرسی محل وقوع جرم، توقیف اسباب و آلات جرم با جرایم کلاسیک متفاوت بوده و بدون تخصص و مهارت کافی مقامات قضایی، کشف جرم میسر نیست. مأموری که به تحقیقات جنایی مشغول است و تخصص در این زمینه ندارد، نمی‌داند که در محیط سایبری به دنبال چه چیزی بگردد. از طرف دیگر در جرایم جدید سایبری، که اغلب جرایم در غیر محل وقوع جرم و غیرحضور ارتکاب یافته است، تحقیقات و کشف بسیار دشوار و غیرقابل دسترس است.^۲

در یک سری از جرایم بدون اثرگذاری در محیط رایانه‌ای، مسائل خاص و پیچیده‌ای مطرح می‌شود. حق بازرسی و توقیف یک شبکه یا تأسیسات رایانه‌ای خاص تا چه حدی شامل حق بازرسی بانک‌های اطلاعاتی و شبکه‌های مادر می‌شود که فقط در دسترس کاربر و یا یک مؤسسه قرار دارد. درواقع جایگزین شدن موضوعات غیرملموس و مجازی به‌عوض ادله مثبت ملموس و عینی در عرصه تکنولوژی اطلاعات، مسائل حقوقی نوینی در حوزه فرآیند کیفری، مطرح ساخته که ضرورتاً مستلزم نگاه

1. European Convention Cybercrim, 2001.

۲. عبانیه، محمود احمد، جرایم الحاسوب و ابعادها الدولیه، الطبعة الاولى، عمان، دارالثقافة للنشر و التوزیع، ۲۰۰۵.

افتراقی نسبت به این مسائل هست. در ادامه به بررسی خلأها و چالش‌های موجود در قلمرو آیین دادرسی کیفری در مواجهه با جرایم سایبری خواهیم پرداخت.

۱. خلأها و چالش‌های فرآیند کشف و دستگیری در جرایم سایبری

یکی از چالش‌های جرایم سایبری مشکل کشف این جرایم است. در این نوع از جرایم به دلیل واقع شدن در فضای مجازی و غیرواقعی، اثری ملموس و مادی از جرم و رد پای مجرم، آن گونه که در جرایم سنتی بر جای می‌ماند، دیده نمی‌شود و در بیشتر موارد همان اندک آثار باقی‌مانده از جرم که قابلیت ردیابی مجرم را دارد به راحتی قابل امحاء و پاک‌سازی است. به همین دلیل می‌توان با اطمینان گفت که رقم سیاه در جرایم سایبری در مقایسه با جرایم سنتی بسیار بالا است. از سوی دیگر، در صورتی که شخص یا سازمانی به‌طور تصادفی در جریان طبیعی فعالیت شغلی خود با ادله دیجیتال بر روی سیستم خود مواجه شود، چنانچه خود به جمع‌آوری و تحصیل ادله فوق‌بپردازد با این اشکال مواجه خواهد بود که ادله مذکور از راهی غیرقانونی به دست آمده‌اند. لذا قابلیت استناد نخواهند داشت. به همین منظور باید آن را برای مجریان قانون افشا نموده تا ایشان به تحصیل ادله مذکور مبادرت نمایند. پس وجود یک فرآیند اطلاع‌رسانی پرسرعت و کم‌هزینه، نظیر شماره تلفن‌هایی که برای مبادی خدماتی نظیر پلیس، اورژانس و ... اختصاص داده شده است، ضروری به نظر می‌رسد.

اقدامات مربوط به گردآوری و حفظ ادله الکترونیکی در صحنه جرم رایانه‌ای یعنی محلی که مجرم اقدامات خلاف قانون خود را برای ارتکاب جرم در آنجا انجام داده است، به دو دسته اقدامات پیش از ورود به صحنه جرم شامل تبیین نوع داده‌ها و ادله هدف و اخذ مجوزهای لازم برای شروع تفتیش و توقیف و اقدامات پس از ورود به صحنه جرم شامل به‌کارگیری تمهیدات فنی، استفاده از ابزار لازم، تهیه صورت‌جلسه‌های مرتبط، که همگی در جهت حفظ ادله تا زمان ارائه به مقام قضایی انجام می‌شوند، تقسیم می‌گردد که هر یک مختصات و ویژگی‌های خاص خود را دارد. البته اختیار گسترش حیطه تحقیق نیز در مواردی خاص با دستور مقام قضایی و با اجرای ضابطان امکان‌پذیر است. مجریان قانون، اولویت وظایف خود را رسیدگی به جرایم خشونت‌بار قرار داده و رسیدگی به جرایم رایانه‌ای را در موقعیتی پایین‌تر قرار داده‌اند؛ در حالی که خسارات ناشی از جرایم رایانه‌ای می‌تواند با بودجه یک کشور کوچک برابری کند. همچنین تفکیکی که مجریان قانون میان جرایم خشونت‌بار و جرایم مرتبط با رایانه به وجود می‌آورند، باعث می‌شود به طور جدی به دنبال ادله مورد نظر نباشند. اما واقعیت این است که رایانه‌ها می‌توانند حاوی دلایلی در ارتباط با جرایم خشونت‌بار مانند قتل،

تحریق عمدی، خودکشی، آدم‌ربایی، شکنجه و آزار و تجاوز جنسی نیز باشند. از این رو، لزوم آموزش مجریان قانون و متخصصان علوم جنایی در زمینه شبکه‌ها به‌عنوان منابع ادله الکترونیکی امری است که بایستی مدنظر قرار گیرد، زیرا اساساً دلیل و قابلیت استناد به آن از مهم‌ترین حلقه‌های اجرای عدالت قضایی است که لازمه آن حفظ و نگهداری صحیح از ادله می‌باشد. این امر به لحاظ تخصصی بودن در مورد ادله الکترونیکی از اهمیت دوچندان برخوردار است. به همین لحاظ آموزش ضابطان و مقامات ذی‌صلاح قضایی در این زمینه امری ضروری است.^۱

دادرسی جرایم سایبری به دلیل واقع شدن در محیط سایبری و ماهیت ادله از پیچیدگی‌های خاص برخوردار است. به دلایل همچون پیچیدگی‌های خاص، حذف قلمرو مکان و محدوده سیاسی حاکمیت یک کشور، مخفی ماندن هویت مجرم و تغییرپذیری ماهیت دلایل اثبات، تخصصی و فنی بودن تحقیقات مقدماتی در محیط سایبر، تعقیب و دادرسی جرایم سایبری با مشکلاتی همراه است و بزهکاران سایبری به دلیل اینکه می‌توانند در یک محیط امن و در فضا هزینه اندک، به‌عنوان مثال در خانه یا دفتر محل کار خود، با ارتکاب اعمال مجرمانه در فضای سایبر به منافع مادی و معنوی غیر، ضرر و زیان به آبرو و حیثیت دیگران لطمه وارد نماید و از اقدامات منافی عاید گرداند، همواره در پی ارتکاب جرم سایبری هست. صلاحیت مراجع قضایی در محیط سایبر بر اساس قواعد صلاحیت در دادرسی جرایم سنتی چندان کارایی ندارد. برای مثال، اگر فضای سایبر منجر به جابجایی محل ارتکاب جرم گردد، اولین مسأله‌ای که مطرح می‌گردد، مرجع ذیصلاح کیفری است که اگر به فراسوی مرزها کشیده شود، به جای کشمکش‌های محاکم داخلی، باید منتظر اعمال صلاحیت کشورهای بسیاری بود. همچنین، به دلیل محیط مجازی و ماهیت ادله الکترونیکی در آن، ادله همواره در معرض تخریب، حذف یا رمزنگاری هستند که این امر کشف و جمع‌آوری ادله جرم را با محدودیت شدیدی همراه می‌سازد. بنابراین، برای مقابله هرچه کارآمدتر و مؤثرتر در قبال ارتکاب جرم در این محیط، می‌بایست ابتدا با شناخت چالش‌های موجود در قلمرو رسیدگی به جرایم سایبری، قوانینی در زمینه آیین دادرسی در فضای سایبر داشته باشیم که بتواند اهداف فوق را برآورده سازد.

۱-۱. نامعین بودن حیطه جغرافیایی ارتکاب جرایم سایبری

بی‌تردید قوانین و مقررات حاکم بر بستر عبور و مرور در فضای دادوستدهای اینترنتی با مقررات موجود برای دادوستدهای تجاری در جهان واقعی بسیار متفاوت

۱. زندی، محمد رضا، تحقیقات مقدماتی در جرایم سایبری، تهران، انتشارات جنگل، ۱۳۸۹، ص. ۱۳۶.

خواهند بود. بخش عمده‌ای از این تفاوت ناشی از ویژگی‌های است که زمینه حضور راه دور را در اینترنت فراهم کرده، شبکه را به لحاظ فناوری از بعد مکانی و فیزیکی متمایز می‌کند. در حقیقت شبکه آن‌چنان نسبت به موقعیت جغرافیایی بی‌ربط است که تعیین مکان فیزیکی یک منبع یا کاربر اینترنتی اغلب ناممکن است. آگاهی از این موقعیت مکانی برای عملکرد شبکه و ایجادکنندگان آن اهمیتی ندارد. آدرس‌های اینترنتی جایگاه آن را در شبکه مشخص می‌کند نه در مکان و موقعیت زمینی، البته برخی آدرس‌ها، مشخص‌کننده‌های جغرافیایی در خود دارند. برای نمونه یک آدرس الکترونیکی دارای پسوند uk در بریتانیای کبیر قرار دارد ولی بیشتر آدرس‌های اینترنتی فاقد این‌گونه تعیین‌کننده‌های جغرافیایی هستند. مهم‌تر از آن، همه آدرس‌های اینترنتی به راحتی انتقال پذیرند. در این حالت هماهنگی و همسویی میان فضا و مکان واقعی و فضای مجازی رایانه‌ای وجود ندارد. بر اساس قواعد صلاحیت قضایی اگر رکن مادی یک جرم درون حوزه قضایی شروع یا کامل شده باشد آن حوزه قضایی صالح به رسیدگی خواهد بود.^۱

با توجه به ماهیت جرایم سایبری، تعیین محل ارتکاب جرم یا محل حصول نتیجه همیشه به آسانی امکان پذیر نیست. جرایم سایبری به لحاظ ماهیت مجازی خود در حقیقت نمود عینی و ملموس شبیه آنچه در جرایم سنتی مانند ضرب و جرح یا سرقت مشاهده می‌کنیم، از خود به نمایش نمی‌گذارند. جرم سایبر در واقع در بستر دادوستدهای الکترونیکی و علیه داده ارتکاب یافته است و اطلاعات و به‌ندرت علیه سامانه‌های فیزیکی و سخت‌افزاری رخ می‌دهند.

در جایی که جرم سایبر علیه داده‌ها ارتکاب یافته است، تعیین محل ارتکاب جرم کاری بس دشوار به نظر می‌رسد. محل وقوع جرم سایبر به‌طور دقیق عبارت است از محل و مکانی که این داده‌ها دستخوش حملات مجرمانه قرار گرفته و دگرگون شده‌اند. چگونه می‌توان یک رخداد غیرفیزیکی و مجازی را در دنیای فیزیکی و در بعد مکانی جستجو کرد؟ حتی اگر جرم سایبری روی قطعه فیزیکی و سخت‌افزاری ارتکاب یافته و موجب بروز اختلال و یا از کارافتادگی شود، باز هم به‌طور قطع نمی‌توان نظر داد که محل وقوع جرم همان محل وجود قطعه‌های سخت‌افزاری آسیب‌دیده خواهد بود، زیرا در قریب به اتفاق این‌گونه جرایم، عمل مجرمانه در مکانی دیگر انجام گرفته و فقط نتیجه روی قطعه‌های سخت‌افزاری پدیدار شده است. برای نمونه، کاربری در ایران با مخاطب خود در شهر فرانکفورت ارتباط اینترنتی برقرار می‌کند و طی این تماس بانفوذ

۱. آشوری، محمد، آیین دادرسی کیفری، جلد دوم، چاپ سوم، تهران، انتشارات سمت، ۱۳۸۲، ص. ۳۹.

غیرمجاز به بانک داده‌های شخصی مخاطب خود در فرانکفورت شده، دست به سرقت اطلاعات موردنیاز خود از مخاطب زده، سپس با تخریب اطلاعات باقی‌مانده بانک اطلاعات وی را ترک می‌کند. در این نمونه ساده محل ارتکاب این جرایم کجاست؟ زیرا مرتکب در ایران با استفاده از نرم‌افزارهای خاص اقدام به نفوذ غیرمجاز به سامانه‌های مخاطب خود در شهر فرانکفورت کرده، در همین حین مرتکب جرایم دیگری نیز بر داده‌های کاربر فرانکفورتی است و کاربر مذکور در رایانه خود نتیجه این اقدامات مجرمانه را به شکل بروز اختلال در برنامه‌ها و سامانه‌های خود مشاهده می‌کند. اینها همه در حالی است که درواقع پایگاه داده‌ها در شهر تورنتوی کانادا واقع است و اگر سرقت، تخریب و هرگونه جرم علیه داده‌ها رخ داده باشد، درواقع آن پایگاه داده‌ها مورد حمله قرار گرفته و کاربر آلمانی فقط نمایی از آن را مشاهده خواهد کرد.

ملاحظه می‌شود که جرایم سایبری برخلاف جرایم سنتی که در مکان‌های مشخص یا محصور از یک اتاق یا یک ساختمان یا یک منطقه خاص رخ می‌دهد، ممکن است در چند گوشه کره زمین ارتکاب یابند. با این اوصاف قواعد دادرسی سنتی که با پارامترهایی همچون صلاحیت سرزمینی تبدیل شده‌اند، کارایی خود را از دست خواهد داد. چرا که چندان مشخص نیست جرم در کجا واقع شده است. به همین خاطر باید در پی ابداع قواعد جدیدی متناسب با این فضا جهت احراز محل وقوع جرم بود.

۲-۱. پنهان‌سازی جرم سایبری

همان‌گونه که قبلاً مطرح گردید یکی از چالش‌های اساسی مأموران اجرای قانون، دشواری کشف جرایم سایبری است. این‌گونه جرایم در بستری رها و در پوششی ناشناخته و گمنامی نسبی بزهکاران انجام می‌شود و اثری ملموس و مادی از جرم و ردپای مجرم آن‌گونه که در جرایم سنتی برجای می‌ماند، مشاهده نمی‌شود و در بیشتر موارد همان اندک ادله الکترونیکی باقی‌مانده از جرم نیز به راحتی قابل پاک‌سازی است. آنچه بدیهی است نمی‌توان با برنامه‌ها و راهبردهایی که ناظر به جرایم سنتی است، نسبت به مبارزه با این جرایم اقدام نمود. افزون بر این، آن دسته از جرایم برخلاف جرایم سنتی، از الگوهای فیزیکی و محدودیت‌های ناظر بر آن پیروی نمی‌کنند. در نتیجه، بزهکاران می‌توانند بدون تماس چهره به چهره و مجاورت با بزه‌دیده، مرتکب جرم شوند که این ویژگی ممتاز، ردیابی و شناسایی آنان را دشوار می‌سازد.^۱

از این رو تعقیب جرایم سایبری در اکثر موارد به دلیل اخفای این نوع جرایم با مانع مواجه است. برای نمونه کلاهبرداری رایانه‌ای غالباً از طریق دست‌کاری پرینت‌های

۱. جوکر، یونی؛ و همکاران، جرم و اینترنت، برگردان رسول نجار، تهران، انتشارات دانشگاه علوم انتظامی، ۱۳۸۹، ص. ۳۰.

داده‌پردازی کتمان می‌شود. جاسوسی رایانه‌ای از طریق نسخه‌پردازی از فایل‌های داده و سرقت مال معمولاً در شرکت‌های بزه دیده به‌عنوان جرم نمایان نمی‌شود؛ زیرا این شرکت‌ها غالباً فرصت کشف و اثبات استفاده غیرمجاز از داده‌های خود در شرکت رقیب را که به خوبی از آن محافظت می‌شود، نمی‌یابند. خرابکاری رایانه‌ای اغلب به عنوان فقر سیستم و یا اشتباه نمایانده می‌شود. در موارد بسیار، امکان کشف موارد نقض حریم خصوصی اشخاص، برای بزه‌دیدگان و مقامات دولتی فراهم نیست، زیرا اعمال مجرمانه در مراکز رایانه‌ای ارتکاب می‌یابند که از آنها به خوبی محافظت می‌شود.

امکان اخفای جرم از طریق دستکاری داده‌ها به ظهور اصطلاح «ماهیت دست دوم پرینت‌های رایانه‌ای» در ادبیات جرم‌شناسی ایالات متحده آمریکا منجر شده است. مشکل ناشی از این واقعیت برای ممیزان و نیز دادرسان را می‌توان در گزارش رئیس یک مرکز رایانه‌ای ملاحظه نمود که عنوان شده است: «یکی از همکاران وی داده‌های مربوط به فعالیت‌های تجاری بسیار مهم را پیش از انجام حسابرسی در شرکت، از حافظه رایانه‌ها حذف کرده و از این طریق، مانع کنترل داده‌ها بر روی پرینت‌های بعدی شده بود.»^۱

در بسیاری از موارد، کشف و تعقیب جرایم سایبری به این دلیل با مشکل مواجه می‌شود که تغییرات صورت‌گرفته در برنامه‌ها و داده‌ها آثاری مانند آثار ناشی از جعل سنتی اسناد بر جای نمی‌گذارد. امروزه تحلیل و بررسی خط افراد در بانک‌های داده الکترونیکی غیرممکن است. به منظور تقلیل مشکلات مربوط به داده‌های واردشده باید در جهت شناسایی اشخاص تلاش نمود که داده‌ها را از طریق ورود به رایانه و دیگر روش‌های ثبت، وارد کرده و پردازش کنند. روش دیگر برای انجام تحقیقات، پیگیری رد مبالغ سرقت شده است که این مبالغ در اکثر موارد به مرتکب انتقال می‌یابد.

مشکل مربوط به پیگیری آثار و سرنخ‌های مربوط به جرایم رایانه‌ای را می‌توان در پرونده‌ای مشاهده نمود که به کشور آلمان مربوط می‌شود. مجرمان نام و آدرس یک شرکت غیرواقعی را به جای نام و آدرس یکی از تهیه‌کنندگان کالاها و خدمات موردنیاز کارفرمای خود بر روی یک فایل داده اصلی قرار داده بودند که شماره حساب‌های بانکی را با آدرس‌های تهیه‌کنندگان مرتبط و مقایسه می‌نمودند تا از این طریق پرداخت صورت‌حساب‌ها را کنترل کند. در نتیجه این تغییر و جایگزینی، ارائه صورت‌حساب بعدی تهیه‌کننده مذکور به صدور چکی به نام شرکت غیرواقعی (به جای تهیه‌کننده) منجر شد. پرداخت مبلغی در حدود ۱۳۵۰۰۰ مارک آلمان به یک تهیه‌کننده ناشناخته

۱. زیبر، اولریش، جرایم رایانه‌ای، ترجمه محمدعلی نوری، رضا نخجوانی، مصطفی بختیاروند و احمد رحیمی مقدم، تهران، انتشارات گنج دانش، ۱۳۸۳، ص. ۲۳۲.

موجب تردید و مظنون شدن مسئولان این شرکت پرداخت‌کننده شده و در نتیجه دستور عدم پرداخت وجه چک صادر شد. در تحقیقات صورت‌گرفته تلاش شد که از طریق تحلیل ثبت رایانه‌ای تغییرات فایل اصلی سرخ‌هایی از مجرمان به دست آید. با وجود این، از آنجا که ثبت رایانه‌ای دوره زمانی از بین رفته بود، نویسنده آدرس قابل شناسایی نبود. تحقیق در خصوص آدرس نوشته‌شده بر روی چک در ابتدا با موفقیت مواجه نشد، زیرا مجرمان آدرس یک خانه بزرگ را انتخاب کرده بودند که در آن صرفاً یک صندوق پستی اضافی به نام شرکت غیرواقعی نصب‌کرده بودند. بررسی صندوق پستی مذکور موفقیتی در پی نداشت، زیرا مجرمان از کشف اقدامات خود مطلع شده و از وصول چک خودداری کرده بودند. با این وجود بعد از چند هفته، نامه‌ای از طرف بانکی که مجرمان در آن برای دریافت وجه چک حساب باز کرده بودند به صندوق پست شرکت ارسال شد. مقایسه دست خطی که برای تکمیل فرم‌های لازم برای افتتاح حساب بانکی به کاررفته بود با دست خط حدوداً یکصد کارمند به شناسایی و محکومیت برنامه‌نویس شد.

همچنین حجم و کثرت زیاد داده‌هایی که اغلب در یک پی‌جویی مرتبط با سامانه‌های رایانه‌ای و مخابراتی وجود دارد، کشف و تحقیق جرایم دیگری را با مشکل دیگری مواجه می‌نماید. جستجوی ادله مفید در میان حجم انبوه و عظیمی از داده‌های دیجیتال می‌تواند مثل یافتن سوزنی در انبار کاه باشد.

امروزه جرایمی از جمله قاچاق انسان، خرید و فروش مواد مخدر در سطح کلان و پورنوگرافی در بستر دارک‌نت یا وب پنهان اتفاق می‌افتد که به کلی کشف و پی‌جویی آنها ممکن نیست. در واقع آنچه به عنوان وب پنهان بیان می‌گردد، آن بخش از فضای اینترنت است که به هر دلیل، خارج از حوزه جستجوی موتورهای کاوش قرار دارد و بازیابی اطلاعات موجود در آن از طریق استفاده مستقیم از این موتورها میسر نیست و آنچه به عنوان دارک‌نت شناخته می‌شود، مجموعه‌ای از ارتباطات است که به شکلی بسیار عمیق در بخش‌هایی از شبکه‌ها که عملاً غیر قابل دسترس بوده و یا به شکل گسترده‌ای ناشناخته هستند، صورت می‌گیرد. معمولاً این بخش از شبکه به دلایلی از جمله ناشناخته ماندن مورد استفاده قرار می‌گیرد و این امکان را فراهم می‌آورد تا اعضای گروه، اطلاعات را از درهای مخفی سرورهای اینترنت ردوبدل کنند و ناشناس بمانند.

در واقع کاربران دارک‌نت به شبکه‌های محلی یا داخلی برای رد و بدل کردن اطلاعات و پیام‌ها متکی و وابسته هستند. فرض کنید همه کاربران اینترنت در یک شبکه مثل یک شهر با یکدیگر ارتباط دارند و همه شبکه‌های وای فای به گونه‌ای به هم

متصل هستند. در این شرایط فرض کنید، کاربری راهی برای انتقال یک پیام از طریق شبکه اینترنت همسایگان پیدا کند. برای این کار، کافی است پیام را از طریق شبکه به همسایه کناری، از آنجا به خانه بعدی و به همین ترتیب تا مقصد هدایت کند. به این ترتیب پیام مورد نظر به سختی قابل ردیابی و کنترل توسط سایر افراد و نهادها حتی کنترل کنندگان زیرساخت اینترنت خواهد بود.

شبکه معروف تور نمونه یک دارک وب بوده و از مسیریابی پیازی استفاده کرده و مبتنی بر لایه‌های چندگانه امنیتی است، دقیقاً همانند پوست پیاز که لایه به لایه است و این لایه‌های امنیتی یک‌به‌یک از پیام‌های ردوبدل شده در شبکه تور حذف می‌گردند و به همین دلیل بیشتر برای مقاصد غیرقانونی مورد استفاده قرار می‌گیرد و همه فعالیت‌های آن غیرقابل ردیابی و شناسایی است. مرورگر تور متعلق به یک مجرم، یک مدار^۱ را ایجاد نموده که در این مدار سه هاب وجود دارد، که از سرتاسر دنیا به صورت رندوم انتخاب می‌شوند. منبع این هاب‌ها را ۵۰۰۰ داوطلب در سرتاسر دنیا فراهم می‌کنند. لذا مرورگر هاب‌ها را می‌شناسد، ولی هیچکس مرورگر مجرم را نمی‌شناسد.^۲

نکته جالب‌تر این‌که وقتی مرورگر تور مجرم، مدار را ایجاد می‌نماید دقیقاً ده دقیقه بعد مدار را از بین برده و مدار جدیدی را می‌سازد. لذا زمانی که مجریان قانون بخواهند نسبت به ردیابی آی‌پی اقدام نمایند، پس از اخذ دستور قضایی و مراجعه به شرکت ارائه‌دهنده خدمات دسترسی امکان تشخیص هویت فرد استفاده‌کننده از آدرس آی‌پی ممکن نیست، چراکه شبکه تور اولاً در طول ده دقیقه مدار جدیدی را ساخته و ثانیاً به دلیل میزبانی ۵۰۰۰ داوطلب در سرتاسر دنیا که منبع این هاب‌ها می‌باشند قبل از اتمام فرصت نیازمند همکاری سه کشور مختلف هست که عملاً پی‌جویی را غیرممکن می‌سازد. نکته جالبی که در این مدارها وجود دارد این است که اکثر آنها در کشور آلمان قرار دارد، و علت آن استفاده تعداد زیادی از آلمانی‌ها از شبکه تور هست و داوطلبان زیادی در ارتباط با هاب‌های مدار دارد.

۱-۳. ضعف کارکردی مراجع قضایی و انتظامی

نویسنده بودن جرایم سایبر و ویژگی‌های خاص آن لزوم رسیدگی و پی‌جویی متناسب با این جرایم را توجیه می‌نماید. در ادامه به مهم‌ترین مشکلات کارکردی دستگاه عدالت کیفری در برخورد با این جرایم خواهیم پرداخت.

1. Circuit

۲. شاهمرادی، خیرالله؛ بابایی، محسن، جرایم پنهان در فضای سایبر، فصلنامه علمی تخصصی پلیس فتا، شماره ۳،

۱-۳-۱. عدم تخصص کافی مراجع قضایی و انتظامی

از جمله چالش‌ها و خلأهای مهم موجود در این حوزه، نداشتن تخصص کافی مراجعی است که به تعقیب، کشف و رسیدگی ماهوی این جرایم می‌پردازند. عدم آشنایی بازرسان و قضات با رسانه‌های اطلاعاتی و ضعف آنها در برخورد با مسائل فنی جرایم سایبری عاملی است برای تشدید هر چه بیشتر مشکلات موجود. البته با عنایت با ماهیت نوین این جرایم، این مسأله چندان تعجب‌آور نیست. بسیاری از اقدامات و تلاش‌های صورت گرفته در بسیاری از کشورهای فاقد ساختار کیفی مناسب فضای سایبر، برای تعقیب مجرمان متوقف شده و شکایات بسیاری در این زمینه رد شده و احکام بسیاری صرفاً در خصوص جنبه‌های حقوقی دعاوی صادر شده است که همه این امور بیانگر عدم تمایل مجریان قانون به مواجهه با مشکلات خاص پرونده‌های مطرح شده است. این مسأله باعث می‌شود که تعقیب و کشف این جرایم با مشکل مواجه شود و دادگاه‌ها نیز نتوانند به نحو شایسته به جرایم مزبور رسیدگی نمایند.

جرایم سایبری آن گونه که از نام آنها برمی‌آید، در فضای سایبری روی می‌دهند و بر خلاف جرایم سنتی، به جای آنکه شواهد حاصل از آن در بستر مادی، فیزیکی و ملموس باشند، دیجیتالی، شکننده و پیچیده می‌باشند. پیچیدگی آنها از این جهت است که رمزگشایی از این دلایل به مراتب بیش از سایر جرایم به تخصص، آموزش و مهارت نیازمند است. همچنین شکننده‌اند چون تعلق و تساهل مأمورین تحقیق در ضبط، نمونه برداری و نگهداری آنها ممکن است برای همیشه آنان را از شناسایی بزهکار مایوس سازد،^۱ زیرا دلایل دیجیتالی می‌تواند توسط مرتکبان به‌انحاء مختلف به سرعت از بین رود. از همین رو است که قانون‌گذار در موارد اضطراری یعنی مواقعی که داده‌ها را خطر آسیب، تغییر، دست‌کاری و از بین رفتن تهدید می‌کند، حفاظت فوری از این شواهد را حتی بدون دستور مقام قضایی مجاز دانسته و برای مستنکف مجازات تعیین نموده است.^۲

پلیس و دیگر عوامل قضایی باید قادر به تحقیق و تعقیب جرایمی که در محیط‌های رایانه‌ای رخ می‌دهد، باشند و قابل قبول نیست که جرایمی بدون مجازات باقی بمانند، صرفاً به این دلیل که پلیس و سایر عوامل قضایی تسهیلات فنی، متخصصان و اختیارات قانونی برای کسب و استفاده از ادله لازم را در اختیار ندارند. کار مهم دیگر بازیافت و احیاء داده است. تجهیزات به‌روز و تخصص کافی برای این کار باید

۱. تراب‌زاده، حسین، «بررسی صحنه‌های الکترونیکی»، فصلنامه کارآگاه، شماره ۶، ۱۳۸۸، ص. ۷.

۲. ماده ۶۶۹ قانون آیین دادرسی کیفری الحاقی ۱۳۹۳.

وجود داشته باشد، خواه داده عمداً یا سهواً از بین رفته باشد، نیاز به تجهیزات و متخصصان بازیافت‌کننده داده‌ها نه تنها در تحقیقات جنایی بلکه در کارخانه‌ها، شرکت‌ها و مؤسسات که سهواً با مشکل نابودی ظاهری و موقت داده‌ها مواجه شده‌اند، محسوس است. برای رسیدگی به این اهداف علاوه بر فراهم ساختن امکانات فنی لازم و همچنین وضع مقررات شکلی لازم در زمینه اختیارات مقامات تحقیق، باید به آموزش این افراد و تربیت افراد متخصص در این زمینه توجه کافی به عمل آید و آن گاه افراد آموزش‌دیده و متخصص به صورت واحدهای ویژه و تخصصی مبادرت به تحقیق و رسیدگی به جرایم سایبری نمایند.

۱-۳-۲. عدم کنترل و فقدان نهادهای نظارتی

فضای سایبر، دنیایی است که نه تنها هیچ نهاد و سازمان بین‌المللی مشخصی بر آن حکومت و کنترل ندارد، بلکه قابلیت کنترل و نظارت بر آن نیز دشوار است. چرا که محیط شبکه و سایبر یک محیط عرضی است نه طولی و افراد مختلف در گوشه و کنار دنیا با هم ارتباط دارند به یک اندازه در این فضای مجازی صاحب حق هستند. همچنین، نظارت بر این ارتباطات علاوه بر اینکه در اکثر موارد با حریم خصوصی و حق آزادی بیان افراد تعارض پیدا می‌کند، از نظر اجرایی هم غیرممکن به نظر می‌رسد زیرا چپستی پیدایش این فضا فراتر از محدودیت‌های این‌چنینی است. از این نگرش به بهترین شکل در اعلامیه استقلال فضای سایبر در سال ۱۹۹۶ دفاع شده است.^۱ پس به همان اندازه که فضای سایبر از لحاظ فنی و تکنولوژیک پیشتاز است، از نظر ساختارها و قابلیت‌های نظارتی عقب‌مانده است و شاید به جهت سرعت بالای پیشرفت فنی آن باشد که نظارت بر آن همیشه یک گام عقب می‌ماند.

۲. چالش‌ها و خلأهای موجود در روند تحقیقات مقدماتی جرایم سایبری

با گسترش فناوری اطلاعاتی و بروز و نمود جرایم مرتبط با آن همانند سایر بخش‌های حقوق کیفری، آیین دادرسی نیز به‌ویژه در فرایند تحقیقات مقدماتی در برخورد با این‌گونه جرایم دچار چالش‌های جدید شده است تا آنجا که بسیاری از قوانین کهنه و مرسوم توان رویارویی با این چالش‌ها را ندارند. در دنیای واقعی، وقتی در مورد جرایم و نحوه تعقیب آنها صحبت به میان می‌آید ادله فیزیکی و ملموس جمع‌آوری می‌شود. مثلاً اثر انگشت، اسناد، سلاح‌های سرد و

۱. ویلیامز، ماتيو، بزھکاری مجازی؛ بزه، انحراف و مقررات گذاری برخط، ترجمه امیرحسین جلالی فراهانی و محبوبه منفرد، زیر نظر علی حسین نجفی ابرندآبادی، تهران، انتشارات میزان، ۱۳۹۱، ص. ۲۵۷.

گرم و نظایر آنها مورد بررسی قرار می‌گیرد. اما در دنیای مجازی و در عرصه فناوری‌های اطلاعاتی و در فضای شبکه‌های بین‌المللی معنی ادله جرم بسیار متفاوت است. جرایم نسل اول رایانه‌ای تا حدودی نزدیک به موضوعات ملموس و عینی بوده‌اند؛ به گونه‌ای که برخی از جرایم ارتکاب‌یافته در این نسل مانند کلاهبرداری رایانه‌ای مبتنی بر یک سری اعمال فیزیکی بوده و کشف و جمع‌آوری ادله جرم حداقل قسمتی از آن، مبتنی بر روش‌های سنتی بوده ولی با بسط فناوری ارتباطی و گسترش شبکه‌های بین‌المللی و قلمرو جرایم سایبری، آیین دادرسی بیش از گذشته دچار چالش ضعف گردید. جایگزین شدن ادله غیرقابل رؤیت و غیرملموس به جای موضوعات عینی و ملموس مشکلاتی از قبیل نحوه تفتیش توقیف داده‌ها یا ادله دیجیتالی، نحوه اثبات ادله و انتساب آن جلوه‌گر شده‌اند.

از آنجا که غالباً مرتکبان جرایم سایبری از طبقات تحصیل کرده و متخصص می‌باشند و همچنین به دلیل ویژگی‌های خاص فضای سایبر و سهولت امحاء آثار جرم و یا عدم وجود اثری از جرایم در غالب موارد، کشف و پی‌جویی این جرایم سخت و دشوار است. به‌ویژه اینکه بزه دیدگان جرایم سایبری که معمولاً مؤسسات و ادارات می‌باشند، خود با مسأله اخبار در وقوع این جرایم با بی‌میلی برخورد می‌کنند و علاوه بر به‌کارگیری وسیع رایانه برای سهولت امور و ارائه خدمات با این روش، از پخش اخبار مربوط به سوءاستفاده از رایانه که منجر به از بین رفتن اعتبار مؤسسه و نیز بی‌اعتمادی مردم می‌شود، رغبتی نشان نمی‌دهند. بلکه برعکس سعی بیشتری برای مسکوت ماندن قضیه می‌نمایند و از هر گونه تلاش برای کشف جرم خودداری می‌نمایند. در چنین مواردی معمولاً موضوع جرم روشن نیست و این نه تنها در تحقیقات ایجاد خلل می‌نماید، بلکه حتی در مرحله قبل از آن یعنی کشف خود جرم نیز مشکل‌آفرین است. یعنی نمی‌توان به سادگی پی به وقوع جرم برد. از این رو، در اکثر مواقع گزارش جرم توسط بزه‌دیده امری لازم تلقی می‌گردد. در سایر جرایم هم پیچیدگی عملکرد و کاربرد رایانه در فضای سایبر که مبتنی بر فناوری پیشرفته است، بر دشواری تحقیق و رسیدگی افزوده است.^۱

مشکلات اولیه در زمینه تحقیقات مقدماتی بروز می‌کند. چون عنصر مادی جرم سایبری از طریق واردکردن، محو، تغییر داده‌ها، برنامه‌ها و سامانه‌های رایانه‌ای، مخابراتی و شبکه‌های بین‌المللی تحقق می‌یابد. از این رو، تحقیقات متمرکز بر این امور شده و دادرسی نسبت به آنها انجام پذیرفته‌اند.

۱. طاهری جبلی، محسن، «جرم و کامپیوتر»، مجله حقوقی دادگستری، شماره ۹، ۱۳۹۲، ص. ۱۲.

۲-۱. چالش جرایم مشهود در فضای سایبر

همان گونه که در قانون آیین دادرسی کیفری مقرر گردیده است، در یک نوع تقسیم بندی، جرایم براساس عنصر مادی و به اعتبار لحظه مشاهده، به مشهود و غیرمشهود تقسیم می گردند. پایه و مبنای جرم مشهود، ضرورت، فوریت و سرعت است. انجام تشریفات با طبع جرم مشهود ناسازگار بوده و نقض غرض محسوب می شود. در جرم مشهود تجری و جسارت مرتکب زیادتر، دلایل علیه متهم محکم تر و اختیارات ضابطان نیز بیشتر است. در حالت جرم مشهود مأموران انتظامی در امر تعقیب و تحقیق جرم به صورت مستقیم شرکت و مباشرت داشته و این تکلیف تا مداخله مقام قضایی صالح ادامه می یابد و مدت آن ۲۴ ساعت است؛ مگر اینکه از طرف مقام قضایی صالح تمدید شود. قانون آیین دادرسی کیفری در قلمرو جرایم مشهود برای ضابطان دادگستری اختیارات ویژه ای را به رسمیت شناخته است. در واقع، از آنجا که در جرایم مشهود گردآوری ادله و بررسی آنها به مراتب آسان تر از جرایم غیرمشهود است، قانون آیین دادرسی کیفری رعایت بعضی از قواعد را در مورد آنها ضروری ندانسته است. از این رو، اختیارات مأموران کشف جرم در خصوص حفظ آثار جرم و جلوگیری از فرار متهم در جرایم مشهود بیشتر از سایر جرایم هست.

در رسیدگی به جرایم سایبری نیز، بعد زمان از اهمیت خاصی برخوردار می باشد؛ به نحوی که بیشترین آثار و ادله الکترونیکی در کوتاه ترین زمان پس از وقوع جرم قابل حذف، جابه جایی و تغییر شکل می باشند؛ به گونه ای که مجرم با یک کلیک بر روی صفحه کیبورد می تواند کلیه آثار و ادله به جای مانده از خود را بر روی سیستم یا سامانه حذف و به تبع آن امر پی جویی را با مشکل مواجه سازد. لذا واکنش سریع مقام قضایی و ضابطان در این گونه جرایم نیز از اهمیت بسزایی برخوردار می باشد. به عبارتی عدم تسریع در اقدامات قضایی در مواجهه با جرایم این فضا، در بسیاری از موارد موجب از بین رفتن ادله جرم و فرار متهم و بالتبع خسارت و ضرر به مردم و شهروندان می گردد.

از این رو لازم و ضروری است که همانند اختیاراتی که در فضای واقعی به تبع ماده ۴۵ قانون آیین دادرسی کیفری (مصادیق جرم مشهود) برای ضابطان دادگستری وجود دارد، برای ضابطان در حوزه جرایم سایبری نیز در نظر گرفته شود تا ضابط بتواند بدون اتلاف وقت و در کمترین زمان ممکن مجرم را شناسایی و با جمع آوری ادله لازم از جرم وی را دستگیر و تحویل مقام قضایی نماید.

۲-۲. عدم جرم انگاری عبور از فیلترینگ و چالش های ضابطان

جرایم ارتكابی در فضای سایبر از ویژگی های منحصر به فردی همچون نامحدود بودن، ناملموس بودن، قابلیت دسترسی آسان و سریع، تغییرپذیری آسان و ناشناختگی

برخوردارند که بر سرعت ارتکاب جرایم در این فضا افزوده است. ابزارهای ارتکاب جرایم در این فضا نیز کاربرد دوگانه دارند که در برخی از عرصه‌ها زمینه بهره‌برداری از فرصت‌ها را به شکل ایمن و مطمئن فراهم کرده است و در برخی از حوزه‌های دیگر موجب عملی شدن تهدیدها و به خطر افتادن منافع عمومی و خصوصی جامعه می‌شوند. از جمله این ابزارهای فناورانه، ابزار VPN (عبور از فیلترینگ کشور) است که علی‌رغم کاربرد وسیع و گسترده آن در جابجایی داده‌های دارای ارزش مالی، حساس و مهم (همانند تبادل اطلاعات و داده‌ها بین بانک‌ها و مؤسسات مالی و بورس)، امکان سوءاستفاده از آن به منظور پنهان نمودن هویت برای ارتکاب جرایم سایبری، جابجایی یا دسترسی به محتوای مجرمانه و عبور از سیستم فیلترینگ کشور را برای همه بهره‌برداران عرصه سایبر فراهم ساخته که این امر علاوه بر پیچیده نمودن فرایند پی‌جویی جرم، موجب بالا رفتن هزینه کشف جرم برای دستگاه قضایی و ضابطان می‌گردد.

لذا ضرورت سالم نگه داشتن فضای سایبر از طریق فراهم ساختن بستر مناسب برای فعالیت‌های مشروع از یک سو و پاک‌سازی آن از وجود چنین تهدیدهایی، ایجاب می‌نماید که ضوابط و مقررات اثربخش و بازدارنده‌ای در این حوزه به تصویب برسد که در این راستا کمیسیون حقوقی و قضایی مجلس شورای اسلامی با پیشنهاد طرح الحاق یک بند به ماده ۲۵ قانون جرایم رایانه‌ای کوشیده است تا نیازمندی‌های برخورد بازدارنده قانونی با تولید، تکثیر، انتشار، توزیع، معامله و یا در دسترس قرار دادن VPN را تأمین نماید که علی‌رغم برگزاری جلسات متعدد با حضور نمایندگان سازمان‌های ذی‌صلاح این مهم به نتیجه نرسیده است.

۲-۳. صلاحیت رسیدگی به جرایم سایبری و چالش‌های فرا روی آن

یکی از مباحث مهم حقوق جزا در حوزه شکلی، بحث صلاحیت مراجع در هنگام رسیدگی به جرایم می‌باشد که در آیین دادرسی کیفری مورد بحث قرار می‌گیرد. در حقوق کیفری رسیدگی به دعاوی در بعد داخلی بر اساس محل ارتکاب جرم، محل کشف جرم، محل دستگیری متهم و یا محل اقامت او حسب مورد می‌باشد و در بعد بین‌المللی با پیش‌بینی قواعد خاص بر اساس اصول صلاحیت مشخص می‌شود. به گونه‌ای که در هر دو عرصه بین‌المللی و داخلی به‌ویژه در مورد اخیر محل وقوع جرم برای رسیدگی در مراجع قضایی صالح از اهمیت خاصی برخوردار است و حتی در خصوص صلاحیت سرزمینی که مبتنی بر ضابطه محل وقوع جرم می‌باشد بر اساس نظریه‌هایی که دکترین حقوق ارائه کرده‌اند برخی مواقع جرایمی در خارج از سرزمین

ارتکاب می‌یابد که تحت حاکمیت یک کشور صالح دانسته شده است. در مقابل برخی آن را صرفاً ناظر به جرایم واقع شده در حوزه داخلی و تحت حاکمیت کشوری صالح شناخته‌اند. علیرغم وجود اختلافات در خصوص محل وقوع جرم و ضابطه تشخیص آن جهت تعیین مرجع صالح مسأله مهمی که در این زمینه به وجود آمده است، تشخیص محل وقوع جرم در فضای سایبر است. چون معیارهای فوق ناظر به جرایم اتفاق افتاده در قلمرو جغرافیایی می‌باشد؛ در حالی که با گسترش شبکه‌های جهانی اینترنتی، استفاده از شبکه‌های رایانه‌ای به شدت افزایش پیدا کرده و در همین راستا بحث حقوق کیفری در زمینه سایبر ظهور پیدا می‌کند چون فضای الکترونیکی و اینترنت با فضای جغرافیایی که حقوق سنتی ناظر به آن است متفاوت است، به طوری که این فضا کاملاً غیر ملموس و مجازی است و مرز جغرافیایی نمی‌شناسد که این تفاوت مسائلی از قبیل ادله اثبات دعاوی در خصوص جرایم اینترنتی، صلاحیت دادگاه‌های مختلف در رابطه با آن جرایم در حقوق کیفری را برانگیخته است. در محیط فضای سایبر قواعد سنتی با چالش‌هایی از قبیل نامعین بودن حیطه‌های جغرافیایی و به تبع آن مشکل تعیین محل ارتکاب جرم، مشکل تعیین تابعیت مرتکب و در نتیجه عدم وجود ضابطه‌های واحد جهت تعیین مرجع قضایی صالح روبه‌رو می‌شوند که با توجه به اینکه در راستای پاسخگویی به این سؤال حقوق دانان نظریه‌های مختلفی را مطرح کرده‌اند، برخی نظریه‌ها در واقع مبتنی بر ضوابط سنتی تعیین صلاحیت، مانند اصل سرزمینی و شخصی و حمایتی و یا جهانی می‌باشند.

در پاسخ باید گفت که در فضای سایبر مرزی وجود ندارد تا به روشنی بتوان به قاعده صلاحیت سرزمینی استناد کرد. از طرف دیگر امکان بهره‌مند شدن از هویت‌های چندگانه متفاوت در فضای سایبر، اعمال صلاحیت تابعیت را در هاله‌ای از ابهام فرو می‌برد. وجود بزه‌دیدگان بی‌شمار و امکان آسیب رساندن به تأسیسات حیاتی چندین کشور در یک زمان، استناد به قواعد میان‌بری نظیر صلاحیت حمایتی را با مشکلات بسیار مواجه ساخته است. در نهایت با اینکه معضل جرایم سایبری فراگیر شده، ولی هنوز اما و اگرهای بسیاری در خصوص آن مطرح است که این خود تمسک به صلاحیت جهانی را نیز مشکل می‌سازد. بنابراین طرح راهکارها و نظریه‌های جدید اجتناب‌ناپذیر می‌نماید و ناچار باید به فکر قواعد تازه‌ای بود که با ماهیت این فضا سازگاری داشته و قابل اجرا باشد.

۲-۴. ارسال پیام‌های ناخواسته الکترونیکی و چالش‌های ناشی از آن

استفاده از اسپم یا پیام‌های ناخواسته الکترونیکی را باید محصول فقدان کنترل صحیح بر ابزارهای فناوری دانست که به واسطه نبود تدابیر و الزامات کافی و ضعف در

مدیریت ارسال پیام، به طور قابل توجهی گسترش یافته و مشکلات فراوانی را برای کاربران فضای سایبر به وجود آورده و زمینه مراجعه تعداد زیادی از شهروندان را به مراجع انتظامی و قضایی فراهم نموده است. مشکل اسپم امروزه از سطح یک معضل ساده فناوری عبور کرده و به تهدیدی بالقوه برای کاربران فضای سایبر، تبدیل شده است. افزایش فرصت بزهکاری و کاهش خطر ارتکاب جرم به واسطه اسپم و ارتباط آن با انواع خاصی از جرایم مالی و متقلبانه، استفاده روزافزون بزهکاران از این ابزار تسهیل کننده جرم به همراه داشته، تا به راحتی بدون نگرانی از کشف جرم و تعقیب قانونی خویش، به انبوهی از افراد مستعد برای بزه‌دیدگی دسترسی داشته باشند و بتوانند به اهداف مجرمانه خود جامعه عمل بپوشانند. بی تردید با ایجاد محدودیت‌ها و ممنوعیت‌ها برای ارسال کنندگان پیام، می‌توان نقش این ابزار ارتباطی را به‌عنوان وسیله مجرمانه در ارتکاب جرم کم‌رنگ کرد و از بروز بسیاری از جرایم مرتبط با اسپم پیشگیری نمود. در حال حاضر مقابله با ارسال اسپم از طریق اقدامات غیررسمی و تدابیر فنی اثربخشی لازم را نداشته و نمی‌تواند به‌تنهایی در رفع مشکلات ناشی از آن و کنترل جرم موفق باشد. بنابراین اتخاذ تدابیر قانونی اعم از کنشی و واکنشی برای حمایت از دریافت کنندگان پیام و پیشگیری از جرایم مرتبط با اسپم، ضروری است.

در این زمینه در نظام عدالت کیفری ایران هنوز سیاست جنایی تقنینی صریح و روشنی وجود ندارد و با وجود قانون تجارت الکترونیکی و مصوبه کمیسیون سازمان تنظیم مقررات و دو لایحه مسکوت مانده تحت عنوان «پیام دیجیتال و پیام‌های ناخواسته الکترونیکی» مبارزه با ارسال اسپم در ابتدای راه است. در حال حاضر با توجه به قوانین و مقررات موجود، صرف ارسال پیام جرم نیست مگر مواردی که وفق قانون جرایم رایانه‌ای دارای محتوای مجرمانه باشد و یا بر اساس ماده ۶۴۱ قانون مجازات اسلامی مشمول ایراد مزاحمت گردد. همچنین ماده ۵۵ قانون تجارت الکترونیکی نیز که الزاماتی را برای تأمین کنندگان در فعالیت‌های تجاری در نظر گرفته، ناقص و مبهم هست و بدون آنکه هدفش مقابله با ارسال اسپم باشد، قواعدی را به شکل محدود آن‌هم در حوزه تبلیغ تجاری و صرفاً مقید به پست الکترونیکی پیش‌بینی نموده است.

در خصوص تدابیر و اقدامات غیرکیفری، قوانین و مقررات جامع و کاملی در رابطه با مدیریت ارسال پیام وجود ندارد و قوانین تجاری و مدنی نیز در این خصوص ساکت است و اقدامات صورت گرفته محدود به ضوابط و مقررات سازمان تنظیم مقررات و ارتباطات رادیویی و تدابیر خودتنظیمی اپراتورها، در مورد پیامک‌های ناخواسته تلفن همراه هست که آن نیز با چالش‌هایی روبرو است. در این خصوص، ارسال یکجای پیام از سوی اپراتورها به مشترکان جهت کسب رضایت به این شیوه به نظر تنها خلاص

شدن از محدودیت مصوبه کمیسیون سازمان تنظیم مقررات است در حالی که خیلی از افراد ممکن است آن را دریافت نکرده باشند و یا به دریافت پیام‌های خاصی تمایل داشته باشند. همچنین اقدامات صورت گرفته توسط اپراتورها نیز به دلیل محدودیت‌های اجرایی و عدم ضمانت اجرای حقوقی تأثیر چندانی بر توقف ارسال پیامک‌های انبوه نداشته و به راحتی ممکن است توسط اپراتور و به دلیل منافع مادی حاصل از ارسال پیام، نادیده گرفته شود.

۳. چالش‌های اثبات جرایم سایبری

همان گونه که بیان گردید، بسیاری از جرایم در فضای سایبر عملاً کشف نمی‌شوند و لذا رقم سیاه جرایم کشف نشده در این حوزه بسیار است. از سوی دیگر تاکنون روش اثبات شده‌ای برای نظارت مؤثر بر این فضا ایجاد نشده و مواردی نظیر پلیس یا گشت سایبر و امثال آن و حتی روش‌های فنی نظارت کافی نیست. همچنین فناوری‌های نوین این امکان را به مجرمان می‌دهند که آثار و ادله جرایم خود را استتار کنند، به طوری که راهکارهای جدیدی برای نهان‌سازی جرایم رایانه‌ای در این فضا ایجاد شده‌اند که این امکان را به مجرمان می‌دهند تا از طریق روش‌هایی چون رمزنگاری در ظاهری قانونی مرتکب جرم شوند. لذا ارتکاب جرم در فضای سایبر راحت‌تر و امکان دستگیری مجرمان نیز کمتر است. مجرمان سایبر به این نکته واقف هستند، پس بهتر است که به جای ارتکاب سرقت اموال در جهان واقعی که خطرات آن به مراتب بیشتر است، مرتکب کلاهبرداری رایانه‌ای شوند که ریسک دستگیری و کشف کمتری هم دارد. این امر سبب شده است که ارتکاب جرایم سایبر روز به روز فزونی بیشتری یابد. بنابراین، مهم‌ترین چالش‌های اساسی که در برخورد با جرایم سایبری با آن روبه‌رو می‌شویم پویایی ادله است. به این معنا که ادله ارتكابی جرم در فضای سایبر همواره در معرض تغییر، جابه‌جایی، ابهام یا نابودی است که در صورت فقدان تدابیر خاص در برخورد با این ادله احتمالی در مبارزه با جرایم سایبر به هیچ عنوان موفقیتی حاصل نخواهد شد. ذیلاً به این مشکلات در دایره جمع‌آوری ادله و اثبات جرایم سایبری خواهیم پرداخت.

۳-۱. نامرئی بودن مدارک و ادله حاصل از جرم

تعقیب جرایم سایبری مستلزم کنترل گسترده داده‌های رایانه‌ای است. بیشتر این داده‌ها به شکل مرئی که توسط انسان قابل خواندن باشد نگهداری نمی‌شوند، بلکه در قالب‌های نامرئی که فقط دستگاه قادر به خواندن آن است و به صورت بسیار متراکم در

ابزارهای ذخیره‌سازی الکترونیکی نگهداری می‌شوند. بنابراین یکی از مشکلات مراجع تعقیب و دادگاه‌ها در کشف و پیگیری جرایم سایبری فقدان مدارک مرئی و مفهوم است. این معضل به‌ویژه در زمینه دستکاری برنامه‌های رایانه‌ای مسأله جدی تلقی می‌شود، زیرا کنترل کامل یک برنامه رایانه‌ای و کشف روتین‌های برنامه‌های نامرئی و مخفی، مستلزم صرف هزینه و وقت زیادی است که غالباً از نظر اقتصادی قابل توجیه نیست. نمایندگان بخش‌های تخصصی و نیز حسابداران و مأموران بازرسی غالباً قادر به کنترل مستقیم داده‌های مشکوک نیستند. تأثیرات فقدان مدارک مرئی و مفهوم، حتی در موارد بسیار ساده را می‌توان در پرونده‌ای ملاحظه کرد که در سال ۱۹۷۱ در آلمان مطرح شد. بدین ترتیب که آدرس سیصد هزار مشتری که بر روی نوارهای مغناطیسی ضبط شده بود از یک شرکت سفارشی پستی سرقت شده بود. شرکت زیان‌دیده موفق شد علیه رقیب خود که این آدرس‌ها را از مجرمان خریداری کرده بود، حکمی از دادگاه مبنی بر استرداد آدرس‌های مذکور تحصیل نماید. مأموری که وظیفه داشت این دستور را اجرا و آدرس‌ها را استرداد نماید با استقبال محترمانه مسئولان شرکت رقیب مواجه شده و اجازه ورود به ساختمان شرکت را یافته و به سمت مرکز رایانه هدایت شده و باکمال میل از او خواسته شده بود که کارش را انجام دهد. با وجود این، وی با انبوهی از دیسک‌ها و نوارهای مغناطیسی مواجه شد که محتویات آنها نامرئی و غیر قابل شناسایی بود و در نتیجه وی دست خالی از شرکت خارج شد.^۱

۲-۳. کدگذاری مدارک و ادله ناشی از جرم

مجرمان حتی قادرند فعالیت‌های تعقیب و پیگیری جرایم ارتكابی را با به‌کارگیری تدابیر امنیتی مانند استفاده از گذرواژه‌ها، ارائه دستورالعمل‌های مانع و روش‌های کدگذاری با مشکلات حادث‌تری مواجه نمایند. این روش‌ها همچنین مانع عمده‌ای در راه کنترل گردش فرامرزی داده‌ها به شمار می‌روند؛ زیرا افرادی که مایل به پیروی از مقررات نباشند می‌توانند انتقال غیرقانونی داده‌ها را از طریق یک مکالمه تلفنی چندثانیه‌ای کدگذاری شده صورت دهند. همچنین کدگذاری داده‌ها در زمینه تجاوز به حریم خصوصی اشخاص می‌تواند کنترل داده‌های ذخیره‌شده به‌ویژه در رایانه‌های کوچک شخصی را بسیار مشکل نماید.

۳-۳. امحاء و از بین بردن ادله و مدارک ناشی از جرم

از بین رفتن مدارک جرم مشکل دیگری است. جرایم سایبر در لحظه رخ می‌دهند و مدارک و شیوه‌های ارتكابی پس از وقوع جرم به‌شدت نابود می‌شوند، در حالی که

1. Sieber, Ulrich, The International Handbook on Computer Crime: Computer-Related Economic Crime and the Infringements of Privacy, Michigan, Wiley, 1986, p. 231.

اقدام‌های قانونی پس از گذشت مدتی از وقوع جرم آغاز می‌گردند. از این رو، مشکلات دیگر در اثبات جرایم سایبری از این واقعیت ناشی می‌شود که بزهدکاران به راحتی می‌توانند از طریق حذف و پاک کردن داده‌ها دلایل خود را از بین ببرند. گاه تاریخ خاصی را برای فعال شدن ویروس تعیین می‌کنند. به محض اینکه این تاریخ برسد، ویروس اقدامات تخریبی خود را شروع می‌کند. برخی از انواع ویروس‌ها پس از خرابکاری به خواب می‌روند و این خود تعقیب را دشوار می‌سازد. در دنیای واقعی دزدی از بانک کاملاً مشخص است، چرا که بعد از سرقت، در خزانه بانک دیگر پولی موجود نیست. ولی در فناوری رایانه شدن یک خزانه می‌تواند بدون هیچ علامتی خالی شود. برای مثال سارق می‌تواند یک کپی دیجیتال کامل از نرم‌افزار بگیرد و نرم‌افزار اصل را همان گونه که دقیقاً بوده باقی بگذارد. در فضای سایبر کپی عیناً عین اصل است. با کمی کار بر روی سیم، سارق می‌تواند امکان هرگونه تعقیب و بررسی را مثل پاک کردن اثرانگشت تغییر دهد. نگران‌کننده‌ترین جنبه فضای سایبر انتشار سریع اطلاعات در آن هست. مثلاً در لحظه‌ای کوتاه، قسمتی از اطلاعاتی که می‌تواند به طور بالقوه مورد سوءاستفاده قرار گیرد کشف می‌شود.^۱ تنها ردی که از مجرم سایبری بر جای می‌ماند یک سری ردپاهای الکترونیکی است که به راحتی و بدون حضور در محل استقرار تیم رایانه‌ای حامل این ردپا، می‌توان آنها را از بین برد. البته این به معنای عدم امکان بازیابی داده‌ها نیست. اما کار گروه تحقیق را بسیار مشکل و کند می‌نماید.

یک روش خودکار پیچیده برای نابودسازی مدارک در رسیدگی به اتهامات یک قاچاقچی اسلحه در هند افشا شد. این قاچاقچی اسلحه که نشانی مشتریان خود را در رایانه‌ای کوچک ذخیره کرده بود، دستورهای معمولی در سامانه‌های عامل را به‌گونه‌ای تغییر داده بود که وارد کردن دستور چاپی یا کپی از طریق صفحه کلید رایانه موجب حذف همه داده‌ها می‌شد. این حیل که به طور ویژه برای مقابله با تحقیقات احتمالی مراجع امنیتی برنامه‌ریزی شده بود، به‌وسیله متخصصان داده‌پردازی کشف شد. این متخصصان احساس کردند که تغییری در سیستم عامل رایانه صورت گرفته و بنابراین نسخه‌هایی از دیسک‌های ضبط‌شده را بر روی سیستم رایانه‌ای خود تولید کردند.

همچنین در یک پرونده دیگر، مجرم یک صندوق داده ایجاد کرده بود و هدفش از این کار محو همه داده‌ها از طریق میدان الکترونیکی به هنگام گشوده شدن به‌وسیله اشخاص غیرمجاز بود. بنابراین از آنجایی که داده‌های دیجیتالی به راحتی قابل حذف یا تغییر هستند، لازم است هر چه سریع‌تر جمع‌آوری و نگهداری شوند. ترافیک شبکه

۱. باستانی، برومند، جرایم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهدکاری، تهران، انتشارات بهنامی، ۱۳۸۳، ص. ۶۷.

تنها به مدت یک ثانیه به طول می‌انجامد، اطلاعات ذخیره‌شده در حافظه ناپایدار رایانه‌ها فقط به مدت چند ساعت نگهداری می‌شوند. به‌علاوه اگر مجرمان تخصص و فرصت کافی داشته باشند برای حفاظت از خود ادله را نابود کرده یا آنها را تغییر می‌دهند.

۳-۴. نحوه جمع‌آوری، ذخیره و ارائه اطلاعات

مهم‌ترین بخش از دادرسی مربوط به فناوری اطلاعات، ناظر به ادله اثبات دعوا است. ادله اثبات دعوا به تبع جرم مطرح می‌شود. از این رو تعریف دلیل رایانه‌ای، نوع دلیل، منابع آن، طریق حصول، قابلیت قبول، نحوه ارائه و چگونگی صدور حکم بر مبنای آن در محیط‌های رایانه‌ای از موارد متنازع‌فیه است.

در حالت مرسوم سنتی نکته مهم احصاء ادله است. در فضای واقعی ادله احصاء شده‌اند و به‌طور کلی به استناد شهادت، اقرار، معاینه محل و کارشناسی تقسیم می‌شوند و بسته به نوع دلیل، قواعدی نیز بر آن حاکم است. مثلاً در اسناد مهم‌ترین مسأله اصالت سند و نحوه شکل‌گیری آن است. سند رسمی باید برابر قانون با ثبت اسناد تشکیل شود تا بتواند سند رسمی تلقی گردد و رسمیت آن مستلزم کاغذی بودن و مهر و امضاهای لازم هست.^۱

پس از نوع ادله، تحصیل و ارائه دلیل، وظیفه طرفین در اثبات دلایل، و صدور حکم توسط دادرس می‌باشد. با پیدایش و تکامل فناوری اطلاعات و نفوذ آن در امور حقوقی، بحث ادله دیجیتال و الکترونیک به وجود می‌آید. مسائلی همچون کاغذی بودن یا نبودن داده‌ها و اطلاعات رایانه‌ای، دوام، بقا و اصالت آنها مطرح می‌شود. داده‌ها و مدارک قابل مشاهده در صفحه مانیتور ظاهر می‌شود ولی با خاموش کردن دستگاه یا تغییر فایل، ناپدید می‌شود و به‌راحتی اصلاح یا محو می‌گردد. خاصیت بقا و دوام به مفهوم فیزیکی و واقعی را ندارند و اصالت مرسوم در اسناد رسمی را نیز فاقد هستند، زیرا یک نسخه یا چند نسخه با ارزش و واحد را نمی‌توان برای آنها در نظر گرفت.

در خصوص قابلیت قبول ادله ناشی از اسناد دیجیتالی در دادگاه بستگی به اصول بنیادین ادله اثبات در هر کشوری دارد. در این راستا باید بین دو گروه از کشورها تمایز قائل شویم. کشورهای مبتنی بر حقوق نوشته، برابر با اصل آزادی دلیل و ارزیابی آزاد دلایل عمل می‌نمایند. سیستم‌های مبتنی بر این اصول عموماً در پذیرش اسناد الکترونیکی به‌عنوان دلیل، هیچ تردیدی ندارند ولی با این حال این موضوع نسبی بوده

۱. عالی‌پور، حسن، حقوق کیفری و فناوری اطلاعات، تهران، انتشارات خرسندی، ۱۳۹۰، ص. ۸۶.

و در مواردی نیازمند مقررات خاصی برای برخی دلایل یا اسناد هستند. در کشورهای مبتنی بر حقوق کامن‌لا، دادرسی به شیوه ترافعی صورت می‌پذیرد. در این کشورها شاهدان بر مبنای مشاهدات، معلومات و علم خود شهادت می‌دهند و در این سیستم حقوقی طبق قاعده «بهترین دلیل» بایستی اصل مدارک به دادگاه ارایه شود تا مورد استناد قرار گیرد.

ادله اثباتی جرم در محیط سایبر همانند داده‌های اطلاعاتی موجود در سیستم‌های رایانه‌ای، موضوعات غیر ملموس بوده که به دلیل ماهیت خاص جرایم سایبری کشف، نگهداری و استناد پذیری ادله امری بسیار تخصصی و پیچیده می‌باشد. لذا با عنایت به پیچیده بودن و نوین بودن موضوعات متنازع‌فیه در فضای سایبر قوانین و مقررات کشورها در این زمینه با خلأ مواجه بوده که با تلاش متخصصان در این حوزه در حال تکوین است.

نتیجه‌گیری

تحولات ساختاری ناشی از به‌کارگیری فناوری اطلاعات و ارتباطات و به‌تبع آن فضای سایبر، امروزه جوامع بشری را در تمامی عرصه‌های اجتماعی با چالش‌های نوینی مواجه نموده است و حوزه‌ها و افق‌های جدیدی را فرا روی بشر گسترده است. به‌گونه‌ای که طراحان ساختارهای اجتماعی، اقتصادی، فرهنگی و حتی سیاسی نسل نوین، ناگزیرند برای ایجاد مناسب‌ترین بستر و پویاترین ابزار، در فضای قاعده‌مند و قانون‌مدار، کلیه سیاست‌ها و معیارهای موجود را به‌روز نمایند. ویژگی‌های متمایز جرایم فضای سایبر همانند سرعت ارتکاب، کثرت، سهولت ارتکاب، ارزان بودن، بی‌مرز بودن، ناشناختگی و اتوماتیک بودن موجب ظهور گونه‌ای متمایز از جرایم نوین در کنار جرایم سنتی، شده است. مرتکبان این جرایم با استفاده از فناوری نوین و ابزارهای جدید به اهداف شوم خود دست پیدا می‌کنند، بدون آنکه اثری همانند جرم کلاسیک از خود بر جای بگذارند. در این نوع از جرایم به دلیل واقع شدن در فضای مجازی و غیرواقعی، اثری ملموس و مادی از جرم و رد پای مجرم، آن‌گونه که در جرایم سنتی برجای می‌ماند، دیده نمی‌شود و در بیشتر موارد همان اندک آثار باقی‌مانده از جرم که قابلیت ردیابی مجرم را دارد به راحتی قابل امحا و پاک‌سازی است. ویژگی دیگر این دسته از جرایم نامشخص بودن هویت مجرمان و همچنین عدم تشخیص درست طیف بزه دیدگان است، زیرا افراد و سازمان‌های متعددی می‌توانند هدف این مجرمان قرار بگیرند. این موضوع نشان می‌دهد که مجرمان سایبری فارغ از زمان و مکان بوده و این نوع از جرایم هم‌اکنون جنبه فراملی و فراسرزمینی به خود گرفته است. فناوری‌های نوین در این عرصه و پیشرفت تجهیزات ارتباطی، مخابراتی و الکترونیکی و سهولت ارتکاب جرم در فضای سایبر، مجرمان را قادر ساخته که فعالیت‌های خود را بدون داشتن ارتباطی خاص با یک محل معین و مشخص انجام دهند که همه این موارد ضمن ایجاد مشکل در تشخیص صلاحیت قضایی، فرآیند کشف، پی‌جویی و رسیدگی به جرایم سایبری را با مشکل مواجه می‌نمایند. امروزه جرایمی به صورت سازمان‌یافته در بستر وب عمیق و با بهره‌گیری از پول‌های مجازی (مانند بیت‌کوین) ارتکاب می‌یابد که به دلیل استفاده مجرم از بسترها و ابزارهای پنهان‌سازی هویت همچون شبکه تور کاملاً غیرقابل ردگیری و پیگیری می‌باشند.

به دلیل ویژگی‌های خاص فضای سایبر ادله اثباتی جرم در این فضا کاملاً متمایز از ادله اثباتی جرم در فضای واقعی بوده و در صورت عدم اقدام به‌موقع ضابط و مقام قضایی به راحتی قابل امحا می‌باشند که این امر همانند جرایم مشهود در فضای واقعی

ضرورت مداخله سریع و آنی پلیس را می‌طلبد تا بتواند در کوتاه‌ترین زمان ممکن ادله مثبت جرم را جمع‌آوری و مجرم را دستگیر نماید. یکی از چالش‌ها و خلأهای دیگر ما در مقابله با جرایم سایبری، عدم وجود دادرهای جرایم سایبری در استان‌ها و همچنین عدم تخصص کافی قضات و دادرسان رایانه‌ای می‌باشد که بعضاً با صدور دستورات و قرارهای نامربوط امر پی‌جویی جرایم سایبری را با مشکل مواجه می‌نمایند. از این رو لازم و ضروری است جامعه حقوقی ما به عنوان یکی از زیرساخت‌های اجتماعات انسانی، در حوزه سایبر متناسب با پیشرفت فناوری اطلاعات و ارتباطات، ابزارها و روش‌های خود را در رسیدگی به جرایم به‌روز و کارآمد نماید. طراحی و ساختارهای کیفری منطبق با ماهیت و ویژگی‌های جرایم سایبری، شفاف‌سازی آیین رسیدگی به جرایم سایبری دادرها و دادگاه‌ها، بهره‌گیری از سیاست‌های مشارکتی از طریق شرکت و مداخله سازمان‌های مردم‌نهاد در تعقیب امور کیفری سایبری، شفاف‌سازی و نظارت دقیق بر ضابطان و تعیین حدود وظایف آنها در پی‌جویی جرایم سایبری (به‌ویژه در زمینه جرایم مشهود)، صلاحیت‌ها و پیش‌بینی دادرسی افتراقی در رسیدگی به جرایم سایبری علیه اطفال و نوجوانان از جمله سازوکارها و مقولات ضروری است که باید در فرآیند رسیدگی شکلی به جرایم سایبری لحاظ گردد.

در ادامه در راستای رفع کلیه خلأها و چالش‌های پیش‌گفته در حوزه رسیدگی شکلی به جرایم سایبر، به بیان پیشنهادهای خواهیم پرداخت:

۱- همان‌گونه که بیان گردید جرایم سایبری به‌صورت لحظه‌ای و آنی ارتکاب می‌یابند و با توجه به این امر که ادله حاصل از این نوع جرایم کاملاً از ماهیت ناملموس و دیجیتالی برخوردارند، به‌سادگی و در کمترین زمان ممکن قابل احصا هستند. لذا دریافت دستور قضایی به روش سنتی در این نوع جرایم (که گاه تا چند روز به طول می‌کشد) امر کشف و پی‌جویی جرم را برای ضابطان با مشکل مواجه می‌نماید. لذا پیشنهاد می‌گردد در این راستا یک نرم‌افزار امن ارتباطی به وسیله یک اپلیکیشن (نرم‌افزار کاربردی) طراحی شود تا ضابط بتواند در کوتاه‌ترین زمان ممکن با اخذ دستور از مقام قضایی، بر سر صحنه جرم حاضر شود و ضمن جمع‌آوری ادله جرم از فرار وی جلوگیری نماید. یا اینکه با آوردن مصادیق جرم مشهود و نیازمند اقدام فوری ذیل ماده ۴۵ قانون آیین دادرسی کیفری، کلیه اختیارات ضابط در مقابله با جرایم مشهود در فضای واقعی برای ضابطین سایبری نیز در نظر گرفته شود و اختیارات این ضابطان افزایش یابد.

۲- با عنایت به ویژگی‌های جرایم سایبری، امروز زمان در تعقیب و رسیدگی به جرایم سایبری، نباید بیش‌ازاندازه کوتاه باشد، زیرا مشکلات مربوط به کشف این جرایم و تحقیق در مورد آنها، ایجاب می‌نماید که در مقایسه با جرایم واقعی، فرصت بیشتری برای تعقیب و پی‌جویی جرایم سایبری در نظر گرفته شود.

۳- بروز نمودن تجهیزات و آزمایشگاه‌های موجود در حوزه جرم‌یابی و آموزش ضابطان در این حوزه قطعاً تأثیر بسزایی در کشف، پی‌جویی و اثبات جرایم سایبری خواهد داشت. لذا پیشنهاد می‌گردد ضمن بروز نمودن تجهیزات، کلاس‌های آموزشی متناسب در این حوزه از سوی نهادها و سازمان‌های صلاحیت‌دار برای ضابطان سایبری برگزار گردد.

۴- همان‌گونه که گفته شد قضات رسیدگی‌کننده به جرایم رایانه‌ای از تخصص کافی در این حوزه برخوردار نمی‌باشند. پیشنهاد می‌گردد در این حوزه نیز آموزش‌های لازم از سوی دادستانی محترم ارائه گردد تا قضات و دادرسان محترم با شناخت و آشنایی کافی نسبت به جرایم بتوانند مأمورین پلیس را در مقابله فوری با جرایم سایبری یاری رسانند. همچنین اختصاص شعبی از داسراها در استان‌ها و شهرستان‌ها جهت رسیدگی ویژه به جرایم سایبری می‌تواند در زمینه رسیدگی مؤثر به جرایم سایبری بسیار مؤثر باشد.

۵- در نهایت ساختار شکلی قانون آیین دادرسی کیفری و اصلاح آن با رویکرد سایبری به‌ویژه در زمینه صلاحیت‌ها و احاله قضایی می‌تواند در امر کشف، پی‌جویی و تحقیقات جرایم سایبری بسیار کارگشا باشد.

منابع

- آشوری، محمد، آیین دادرسی کیفری، جلد دوم، چاپ سوم، تهران، انتشارات سمت، ۱۳۸۲.
- باستانی، برومند، جرایم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری، تهران، انتشارات بهنامی، ۱۳۸۳.
- تراب‌زاده، حسین، «بررسی صحنه‌های الکترونیکی»، فصلنامه کارآگاه، شماره ۶، ۱۳۸۸.
- جوکر، یونی؛ و همکاران، جرم و اینترنت، برگردان رسول نجار، تهران، انتشارات دانشگاه علوم انتظامی، ۱۳۸۹.
- زندی، محمدرضا، تحقیقات مقدماتی در جرایم سایبری، تهران، انتشارات جنگل، ۱۳۸۹.
- زیبر، اولریش، جرایم رایانه‌ای، ترجمه محمدعلی نوری، رضا نخجوانی، مصطفی بختیاروند و احمد رحیمی مقدم، تهران، انتشارات گنج دانش، ۱۳۸۳.
- شاهرمدادی، خیرالله؛ بابایی، محسن، جرایم پنهان در فضای سایبر، فصلنامه علمی تخصصی پلیس فتا، شماره ۳، ۱۳۹۲.
- طاهری جلیلی، محسن، «جرم و کامپیوتر»، مجله حقوقی دادگستری، شماره ۹، ۱۳۹۲.
- عالی‌پور، حسن، حقوق کیفری و فناوری اطلاعات، تهران، انتشارات خرسندی، ۱۳۹۰.
- عبانیه، محمود احمد، جرایم الحاسوب و ابعادها الدولیه، الطبعة الاولى، عمان، دارالثقافه للنشر و التوزیع، ۲۰۰۵، ۲۰۱۲.
- ویلیامز، ماتیو، بزهکاری مجازی؛ بزه، انحراف و مقررات گذاری برخط، ترجمه امیرحسین جلالی فراهانی و محبوبه منفرد، زیر نظر علی حسین نجفی ابرندآبادی، تهران، انتشارات میزان، ۱۳۹۱.
- Sieber, Ulrich, The International Handbook on Computer Crime: Computer-Related Economic Crime and the Infringements of Privacy, Michigan, Wiley, 1986.