چالش‌های حقوقی جرایم سایبری
در نظام حقوق بین الملل و نظام حقوقی ایران

تاریخ دریافت: ۹۳/۱۲/۲۰ تاریخ پذیرش: ۹۴/۵/۱۲

از صفحهٔ ۱۱۷ تا ۱۳۸

رضا صبح خیز[۱]

چکیده

فناوری اطلاعات روز به روز در حال تکامل و پیشرفت بوده و تا لایه های پایین و جزئی جوامع بشری نفوذ پیدا کرده است. فضای سایبری زائیدهٔ این فناوری است. فضایی که با دارا بودن ویژگی‌های منحصر به فرد، می‌تواند بسترساز جرایم خاص و پیچیده ای همانند جرایم علیه تمامیت و صحت داده ها باشد. لذا باتوجه به ساختارهای پیچیدهٔ این نوع جرایم، اغلب حقوق دانان و نهادهای مبارزه کننده با جرم، درصدد بررسی وضعیت شکلی و ماهوی این جرایم بوده تا براساس معیارهای به دست آمده، اقدامات سازنده ای را در سیستم جرم انگاری این نوع جرایم داشته باشند. تحقیق حاضر با هدف بررسی چالش‌های حقوقی جرایم سایبری در نظام حقوق بین‌الملل و ایران انجام شده است. این پژوهش به روش علمی - مروری انجام شده و با گردآوری اطلاعات مورد نیاز، ضمن تشریح مبانی نظری پیرامون فضا و جرایم سایبری؛ اقدامات حقوقی ماهوی و شکلی انجام شده در خصوص جرایم سایبری در نظام حقوق بین‌الملل و ایران مورد تحلیل قرار داده و در ادامه، در یافته‌های خود بر این امر صحه می گذارد که با چالش‌های فراگیر و عمیقی همچون تعارض قوانین و دادگاه‌ها مواجه است که در نتیجه با لحاظ کردن شرایط همگون حقوقی با سایر کشورها و همکاری بین المللی می‌توان این چالش‌ها را به صورت نسبی مرتفع کرد.

کلید واژه ها

فضای سایبری، جرم سایبری، چالش‌های حقوقی، نظام حقوق بین الملل، نظام حقوقی ایران

۱ - مربی حقوق جزا و جرم شناسی دانشگاه علوم انتظامی امین، Reza123onlymorning@gmail.com

مقدمه

تحول و پیشرفت عظیم و شگرفی که امروز در دنیـای علـم و دانـش فنـاوری شـاهد هستیم؛ از چنان سرعتی برخوردار است که به صورت مستمر زیرساخت هـای مهـم جامعه را تحت تأثیر قرار داده و تغییرات عمده ای را در آن ایجاد مـی‌کنـد. امـروزه از این تحول و پیشرفت به نام فناوری اطلاعات[1] نام بـرده مـی‌شـود. فنـاوری اطلاعـات همان‌گونه که رویکرد نو و فضایی دوست داشتنی را برای ما به ارمغان آورده است، بـه تبع آن تهدیدهای این فضا نیز برای افراد و جامعه، جای تأمل دارد. رایانه بـه عنـوان ابزاری از فناوری اطلاعات با توجه به قابلیت‌های بسیار زیاد همچون دقت بالا، سرعت زیاد، ذخیره سازی حجم زیاد، اطلاعات، خستگی ناپـذیری، تبـادل سـریع اطلاعـات، دسترسی آسان و محاسن بی شمار دیگر، امکانات زیادی را برای بشر به ارمغان آورده است، اما از منظر دیگر سبب بروز جرایم جدیدی شده است که قابل مقایسه بـا هـیچ یک از جرایم کلاسیک موجود نبوده و چه بسا که خطرناک‌تر باشد. جرایم نسل جدید فناوری اطلاعاتی که رایانه بستر آن و شبکه جهانی اینترنت از مهم‌ترین ابزار آن است، به معنای واقعی، جرایم فراملی بوده و حد و مرزی نمی‌شناسد. به خصوص که جـرایم نسل سوم رایانه در محیط مجازی[2] به وقوع می پیوندد و اغلب این محـیط در فضـای شبکه های بین‌المللی موجود در جهان از جمله اینترنت وجود داشته و هر گونه فعـل و انفعالی در داده ها و اطلاعات می تواند نوید وقوع یک جرم را بدهد که در مـواردی قابل تطبیق با جرایم کلاسیک و سنتی نبوده و به جهاتی جرایم بی سابقه و نوظهـور هستند و در هر صورت، کمتر می‌توان عناصر سه گانه وقوع جـرم را از لحـاظ حقـوق کیفری در این گونه جرایم پیدا کرد و از طرفی ابعاد بین‌المللی این نوع جرایم موجب شده تا افراد مختلف از جمله جرم شناسان، حقوق دانان و متخصصان رایانه به مطالعه و بررسی همه جانبهٔ این پدیده روی آوردند؛ چرا که تدوین قوانین و اجرای مجازات با توجه به فراملی بودن ماهیت جـرایم سـایبری بـه مسـئله ای پیچیـده تبـدیل شـده است(باستانی،۱۳۸۶: ۱۴). اما اقـدامات حقـوقی نـه چنـدانی در بسـترهای شـکلی و

1 - Information Technology
2- Cyber space

ماهوی و در سطوح داخلی و بین المللی توسط دولت‌ها و نهادها در حوزهٔ جرایم سایبری صورت پذیرفته است که این تحقیق سعی دارد به طور اجمال، ضمن تجزیه و تحلیل جرایم سایبری به صورت ماهوی و شکلی در سطح بین‌الملل و حقوق ایران و با اشاره و مقایسهٔ تطبیقی قوانین و مقررات بین‌المللی و داخلی، چالش‌های موجود در این زمینه را احصاء و مورد نقد و بررسی قرار داده و در نهایت راهکارهایی در این خصوص ارایه دهد. به طور کلی مهم‌ترین سؤال‌های مطروحه دربارهٔ حقوق بین‌الملل[۱] و حقوق ایران در زمینهٔ سایبری عبارت اند از: مابین حقوق بین الملل و حقوق ایران در مورد جرایم سایبری، چالش‌هایی وجود دارد یا خیر؟ چگونه می‌توان این چالش ها را مرتفع کرد؟ سیاست کیفری ایران در برخورد با جرایم سایبری نسبت به مقررات بین‌المللی چگونه است؟ و رفتارهای حقوقی بین المللی به چه سمتی سوق داده شده است؟

مبانی نظری تحقیق

سایبر پیشوندی است برای توصیف یک شخص، یک شیء، یک ایده یا یک فضا که مربوط به دنیای رایانه و اطلاعات است. در طی توسعهٔ اینترنت، واژه‌های ترکیبی بسیاری از کلمهٔ سایبر به‌وجود آمده است؛ از جمله: فضای سایبر[۲]، شهروند سایبر[۳]، پول سایبر[۴]، فرهنگ سایبر[۵]، راهنمایی فضای سایبر[۶]، تجارت سایبر[۷]، کانال سایبر[۸]و ... . در اصطلاح علم فناوری اطلاعات، فضای سایبر به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق رایانه و وسایل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می شود[۹]. یک سیستم آنلاین[برخط] نمونه‌ای از فضای سایبر است که کاربران آن می‌توانند از طریق ایمیل با یکدیگر ارتباط برقرار کنند. بر خلاف فضای واقعی، در

1- International law
2- Cyberspace
3- Cybercitizen
4- Cybercash
5- Cyberculture
6- Cybercoach
7- Cyberbussiness
8- Cyberchannel
9 - http://www.sis-eg.com/services/article_a/11216.

فضای سایبر نیاز به جابجایی‌های فیزیکی نیست و کلیهٔ اعمال، فقط از طریق فشردن کلیدها یا حرکات ماوس صورت می‌گیرد. می‌توان فضای سایبر را چنین تعریف کرد: محیطی است مجازی و غیرملموس در فضای شبکه‌های بین‌المللی (این شبکه‌ها از طریق شاهراه‌های اطلاعاتی مثل اینترنت به‌هم وصل هستند) که تمام اطلاعات راجع به روابط افراد، فرهنگ‌ها، ملت‌ها، کشورها و به‌طور کلی، هر آنچه در کرهٔ خاکی به‌صورت فیزیکی و ملموس وجود دارد؛ به‌صورت نوشته، تصویر، صوت و اسناد، می‌تواند دقیقاً در یک فضای مجازی و به شکل دیجیتالی وجود داشته و قابل استفاده و دسترس استفاده کنندگان و کاربران باشند و از طریق رایانه، اجزای آن و شبکه‌های بین‌المللی به هم مرتبط است(باستانی، ۱۳۸۶: ۶۴).

جرایم سایبری[1]: در اواسط دههٔ ۱۹۹۰ میلادی، نسل جدیدی از فناوری رایانه (که در واقع باید آن را ماحصل فناوری ارتباطی و اطلاعاتی نامید) تجلی پیدا کرد. رایانه ها در یک روند تکاملی بسیار سریع، به سیستم‌های رایانه‌ای متشکل از چندین وسیلهٔ رایانه ای که قابلیت ارتباط بین سیستم‌ها و شبکه‌های بین‌المللی را داشتند، تبدیل شدند. رایانه ها به وسیلهٔ شبکه‌ها، روز به روز ارتباط گسترده تری پیدا کرده و از طریق مخابرات و ماهواره، هرگونه دریافت، انتقال، صدور علایم، تصاویر، صداها، نوشته‌ها و نشانه ها را مقدور ساخته اند. لذا با توجه به این قابلیت شگرف فناوری ارتباطی، تحول عظیم در دنیای ارتباطات و عصر فناوری اطلاعات به وجود آمد که از مشخصه‌های این فناوری جدید، شکل‌گیری ارتباط بین افراد ملل دنیا در یک فضای مجازی و در محیط شبکه‌های بین‌المللی است که به نوبهٔ خود، سهم بسزایی در تغییر شکل و کارکرد روابط اجتماعی دارد و به همان نسبت در تغییر الگوی ماهیت جرایم کلاسیک نیز تحول ایجاد کرده است(زرگر، ۱۳۸۵: ۲۰۶). از خصوصیات متمایز کنندهٔ این نوع جرایم با جرایم پیشین، عدم وابستگی ارتکاب جرم به حضور فیزیکی مجرم در محل بروز نتایج جرم، زمان ارتکاب، مکان ارتکاب، بزه‌دیده و شکل ارتکاب است. به این نوع جرایم که در این نوع فضا (مجازی) وقوع پیدا می‌کند؛ جرایم سایبری گفته می‌شود.

1- Cybercrime

در فضای سایبر برای جستجو و کشف جرایم، مشکلات پیچیده‌تر می شود. در دنیای واقعی، سرقت از بانک کاملاً مشخص است؛ زیرا بعد از سرقت در خزانهٔ بانک، پولی موجود نیست. ولی در فناوری رایانه ای، خزانه می‌تواند بدون هیچ علامتی خالی شود. برای مثال سارق می‌تواند یک کپی دیجیتال کامل از نرم افزار بگیرد و نرم‌افزار اصلی را همان طور که بوده، باقی بگذارد. در فضای سایبر، کپی، عین اصل است. با کمی کار روی سیستم، سارق می‌تواند امکان هرگونه تعقیب و بررسی را مثل پاک کردن اثر انگشت تغییر دهد. نگران کننده‌ترین جنبه‌های فضای سایبر، انتشار سریع اطلاعات در یک لحظه است. مثلاً در لحظه‌های کوتاهی قسمتی از اطلاعاتی که می‌تواند به طور بالقوه مورد سوء استفاده قرار گیرد، کشف می‌شود(بیوند[1]، ۱۹۹۷: ۲۸ به نقل از باستانی، ۱۳۸۳). بسیاری از هکرها (سارقان رایانه ای کلاه خاکستری) معتقد نیستند که کار آنها نادرست است. آنها معتقدند که هک کردن (سرقت داده‌ها و یا ورود غیرمجاز به سامانه) صرفاً به دلیل ارضای حس کنجکاوی آنهاست. خیلی از هکرها در محدودهٔ قانون باقی می‌مانند و حتی اقلیت هکرهایی که در سرقت سیستم های رایانه‌ای دست دارند و در فعالیت‌های خود معتقد به نگرش «ببین! اما دست نزن» هستند. درحال حاضر، نگهداری و تبادل اطلاعات در مورد چگونگی ورود به سیستم‌های رایانه ای و تعدی به آنها، در بیشتر کشورها مخالف قانون نیست. هر چند به کار بردن و استفاده از این اطلاعات، خلاف قانون است. اما خطر زمانی بروز می‌کند که این اطلاعات در دست افراد شروری بیفتد که اهداف مجرمانه دارند. جرایم سایبری نیز به دلایل اجتماعی و روان شناختی همه گیر شده است؛ به دلیل طبیعت مجازی فضای سایبر، بعضی از هکرها آن را به دیدهٔ یک بازی می‌نگرند و در تمایز فضای سایبر از دنیای مجازی مشکل دارند. برای آنها هک کردن فقط یک ماجراجویی است که آنها در دنیای رایانه تجربه می کنند. متأسفانه این بازی‌ها برای آنها، همان مجازات و شرایط دنیای واقعی را دارد. ورود غیر مجاز به سیستم برای بعضی از نوجوانان، علت‌های اجتماعی دیگری نیز دارد. آنها سایت‌ها را «هک» می‌کنند که به اطرافیان خود لیاقت خود را نشان می‌دهند و ارزش و احترام کسب

1- Beyond

کنند. هکرها اغلب روش‌های تکمیلی را بین خود رد و بدل می‌کنند(به نقل از صبح‌خیز، ۱۳۹۱: ۲۷).

تعاریف متعددی از جرم سایبری بیان شده است. یک تعریف عمومی، جرم سایبری را به عنوان هرگونه فعالیتی که در آن رایانه ها یا شبکه ها، ابزار، هدف یا مکانی برای فعالیت تبهکاری هستند، توصیف می‌کند. پیش نویس کنوانسیون بین‌المللی به تقویت حفاظت در برابر جرایم سایبری و تروریسم اشاره دارد. جرایم سایبری اعمالی در رابطه با سیستم های سایبری است. برخی تعریف‌ها، در تلاش برای در نظر گرفتن اهداف و نیت‌ها هستند و جرایم سایبری را دقیق‌تر تعریف می‌کنند. اما باید توجه داشت که در ابعاد بین الملل و داخلی، تعریف دقیق و شفافی از جرم سایبری صورت نگرفته است. بنابراین براساس داشته های موجود و تعریف جرم در نگاه حقوقی جمهوری اسلامی ایران که اذعان می‌دارد: جرم، هرفعل یا ترک فعلی است که در قانون برای آن مجازات تعیین شده باشد، بنابراین جرم سایبری را می‌توان تلویحاً چنین تعریف کرد که: هر فعل یا ترک فعلی است که در فضای سایبر به وقوع می‌پیوندد و برابر قانون برای آن مجازات تعیین شده باشد(صبح خیز، ۱۳۹۱:۲۷).

روش‌شناسی تحقیق

روش انجام تحقیق در این مبحث، علمی- مروری است و گردآوری داده ها و اطلاعات مورد نیاز این پژوهش به روش کتابخانه‌ای و اسنادی، از طریق مطالعهٔ وبگاه‌های معتبر اینترنتی و مصوبات نهادهای حقوقی و بین المللی و مصاحبه با اساتید و صاحب نظران و همچنین مطالعهٔ کتب مربوط به فضا و جرایم سایبری و رایانه‌ای و اسناد حقوقی کنوانسیون‌های مختلف و دیگر قوانین و مقررات بین‌المللی انجام شده است.

یافته‌های تحقیق

الف) ماهیت جرایم سایبری: با توجه به مباحث پیشین اشاره شد که جرم سایبری تکامل یافته جرایم رایانه ای کلاسیک است. باید توجه داشت که جرایم رایانه ای محض با جرایم سایبری متفاوت است و هر جرم رایانه ای الزاماً جرم سایبری نیست. اما باید به این نکته اشاره کرد که در حال حاضر عبارت‌هایی از قبیل جرایم رایانه ای،

قوانین جرایم رایانه ای و ... که در عموم مطرح است، همان جرایم و قوانین سایبری است؛ زیرا، در صورت نبود شبکهٔ اجتماعی نمی‌توان به این نتیجه دست یافت.

جدول ۱: بررسی تطبیقی عنصر مادی و معنوی نسل اول تا سوم جرایم تحت رایانه

ردیف	عنصر مادی	عنصر معنوی
نسل اول	استفاده از رایانه تنها به عنوان ابزار	انگیزه مجرم ارتکاب جرم سنتی
نسل دوم	استفاده از رایانه به عنوان موضوع، هدف و ابزار	انگیزه مجرم سرقت، تغییر و تخریب اطلاعات
نسل سوم	استفاده از رایانه و فضای سایبر به عنوان موضوع، هدف و ابزار	انگیزه مجرم ارتکاب جرایم سنتی و جرایم محض سایبر از طریق فضای سایبر

ب) اقدامات حقوقی در نظام حقوقی بین‌الملل و نظام حقوقی ایران: جرم سایبری اغلب دارای بعد بین المللی است. پست‌های الکترونیکی با محتوای غیرقانونی، اغلب از میان تعدادی کشور حین انتقال از فرستنده به گیرنده عبور می‌کنند، یا محتوای غیر قانونی خارج از کشور ذخیره می شود. در پیگرد جرایم سایبری همکاری نزدیک بین کشورهای درگیر بسیار مهم است. توافقات قانونی دوطرفه موجود بر پایه فرآیندهای رسمی، پیچیده و اغلب زمان بر است. انجام توافقات برای پاسخ سریع به رویدادها، همچنین درخواست‌ها برای همکاری بین‌المللی ضروری است. تعدادی از کشورها، نحوهٔ همکاری قانونی دوطرفه‌اشان را براساس اصل مجرمیت دوگانه قرار می دهند. پیگردها در سطح جهانی در کل، محدود به جرایمی هستند که در همهٔ کشورهای شرکت کننده جرم شمرده می شوند. اگر چه تخلفاتی وجود دارد که در هرجایی از دنیا می توانند مورد پیگرد قانونی قرار گیرند با این وجود تفاوت‌های منطقه ای، نقش مهمی را در این امر بازی می کنند.

جرم‌انگاری محتوای غیرقانونی در کشورهای مختلف، متفاوت است. موضوعاتی که از لحاظ قانونی می توانند در کشوری منتشر شوند، ممکن است در کشور دیگری غیرقانونی باشند. فناوری رایانهٔ مورد استفاده، به طور عمده در دنیا یکسان است. جدا از مقوله های زبانی و نوع قدرت، تفاوت‌های خیلی اندکی بین سیستم‌های رایانه ای و تلفن‌های همراه فروخته شده در آسیا و آنهایی که در اروپا فروخته شده اند، وجود دارد. موقعیتی مشابه در رابطه با اینترنت وجود دارد. به خاطر استاندارد سازی، پروتکل های استفاده شده در کشورهای قارهٔ آفریقا با آنهایی که در ایالت متحده

آمریکا استفاده شده یکسان است. استاندارد سازی، امکان دسترسی کاربران سرتاسر دنیا را به خدمات یکسان اینترنتی فراهم می سازد(شیرزاد، ۴۲:۱۳۸۸). بنابراین در این خصوص به اقدامات جامعهٔ بین المللی و طبقه بندی برخی از نهادهای جهانی از جرایم سایبری و رایانه ای داشتند را بررسی می‌کنیم:

۱- **اقدامات حقوقی در نظام بین‌الملل:** در جامعهٔ اطلاعاتی به دلیل جهانی شدن ارتباطات و گستردگی محیط فعالیت، دیگر سازوکار های گذشته کارکردهای مطلوبی در مقابله با عوامل مجازی نفوذ کننده، هکرها، ویروس ها و غیره ندارند. لذا شرایط جدید، قوانین و ابزارهای نوین را می طلبد تا بتوانند امنیت کافی را برای حفاظت از آثار و اطلاعات موجود در شبکه ها و رایانه ها تأمین کند. برخی کشورها، در زمینهٔ تدوین قوانین نوین پیشگام بوده و اقدامات چشمگیری را در این رابطه انجام داده اند، ولی در کشورهایی که هنوز با موضوعات نوین جامعهٔ اطلاعاتی از جمله شناسایی محیط جدید سایبری و تدوین قوانین لازم برای هدایت، کنترل و مقابله با جرایم سایبری، اقداماتی انجام نداده اند، لزوم تهیه و تدوین قوانین مورد نیاز ضروری است. برای مثال، می توان به موافقت‌نامهٔ جرایم سایبری شورای اروپا در تقسیم بندی، تعریف و شناسایی این جرایم در سال ۲۰۰۱ اشاره کرد. انجمن بین المللی حقوق کیفری نیز طی یک گردهمایی در سال ۱۹۹۲ در ورستبورک، بر کشورها توصیه کرد تا هنگام اصلاح قوانین موجود یا تدوین قوانین نوین به مواردی همچون دقت و وضوح مقررات، عدم تورم کیفری به‌خصوص با تجدید مسئولیت کیفری به جرایم عمدی و مطابقت این قوانین با نسل حقوقی و فرهنگی کشور خود توجه لازم را مبذول دارند (سازمان ملل، ۱۳۷۶: ۴۹ و ۵۰).

در کشورهای پیشرفته، قانون‌گذاران با توجه به نیاز جامعه، انواع مختلفی از اعمال مجرمانهٔ رایانه ای را شناسایی و در قالب قوانین کیفری خود گنجانده اند و همزمان با این اقدامات پراکنده کشورها، مراجع بین‌الملل نیز فعالیت خود را در این زمینه آغاز و با دسته بندی جرایم شناخته شده، لیست هایی از این گونه جرایم را به عنوان الگوی واحد و راهنما برای تدوین قوانین ملی کشورها ارائه کردند. از جمله سازمان‌های

بین‌المللی و منطقه ای پیشرو در این زمینه، می توان به سازمان همکاری و توسعه اقتصادی[1]، شورای اروپا، انجمن بین المللی حقوق جزا، سازمان ملل، طبقه بندی اینترپل (سازمان پلیس جنایی بین المللی)، طبقه بندی کنوانسیون بوداپست[2]، اقدام گروه هشت در سال ۱۹۹۹، اقدام موسسهٔ مک کانل اشاره کرد (بای و پورقهرمانی، ۷۹:۱۳۸۸).

کشورهای مختلف نیز در همین ارتباط، بنابر ارزش های اخلاقی خود سعی کرده‌اند ترکیبی از عوامل تکنیکی و حقوقی را مدنظر قرار دهند. آخرین و مهم‌ترین گردهمایی و مصوبهٔ راجع به جرایم سایبر، به کنفرانس بوداپست در اواخر سال ۲۰۰۱ میلادی بر می‌گردد که در آن بیشتر کشورهای اروپایی همراه کانادا، ژاپن و آفریقای جنوبی و آمریکا مصوبه ای به نام «کنوانسیون جرایم سایبر» امضاء کردند. در مجموع، بیش از ۳۲ کشور به مصوبات کنفرانس بوداپست صحه گذاشتند و اما روسیه، اسلواکی، ترکیه، لیتوانی، لوکزامبورگ، چک، دانمارک و بوسنی هنوز به آن نپیوسته اند. راهکارهایی نظیر توسعهٔ امنیت سیستم ها و مشارکت امضا کنندگان برای دسترسی به این هدف در زمینه های نرم افزاری و سخت افزاری نیز مورد تأکید قرار گرفته است که قرار شده امضا کنندگان در زمینهٔ استرداد مجرمان سایبر با یکدیگر همکاری مستقیم داشته باشند. کنفرانس بوداپست به عنوان اولین همایش فراملی دربارهٔ جرایم سایبر درکانون توجه حقوقدانان اینترنتی قرارگرفت و پس از آن، همچنان درحال توسعه و گسترش است(باستانی، ۱۳۸۶: ۷۲).

۲- اقدامات حقوقی ایران: همهٔ کشورهای جهان به نسبت میزان برخورداری و بهره مندی‌اشان از فناوری اطلاعات، در معرض خطرات و تهدیدات ناشی از این فناوری می باشند. قطعاً کشورهای توسعه یافته، در حال حاضر به لحاظ استفادهٔ بیشتر از این فناوری، در معرض خطر بیشتری هستند. مثلاً دولت آمریکا چهار مرحله از پنج مرحلهٔ تشکیل دولت الکترونیک را پشت سر گذاشته است. در آن کشور و اکثر کشورهای اروپایی بسیاری از خدمات دولتی به صورت الکترونیکی ارائه می‌شود.

1- Organization for Economic Cooperation & Development

2- Budapest Convention

فروشگاه‌های بزرگ که مراکز فروش الکترونیک نامیده می‌شود کالاهای خود را از طریق شبکه‌های رایانه‌ای و به صورت مبادلهٔ الکترونیک به فروش می‌رسانند. کشورهای در حال توسعه نیز ناگزیرند که برای پیشرفت و توسعهٔ کشورخود، مجهز به فناوری اطلاعات شوند و طی کردن این مسیر اجتناب ناپذیر است و بدون بهره‌گیری از پیشرفته ترین فناوری نمی‌توان به توسعه و پیشرفت دست یافت. کسی که می‌خواهد در عصر فراصنعتی و در جامعهٔ اطلاعاتی زندگی کند، باید خود را مجهز به پیشرفته ترین لوازم آن نماید. ترس از جرم، نباید مانع از پیشرفت ما باشد. به نقل از یکی از استاتید حقوق دانشگاه میشیگان: «ما نمی‌توانیم با جنگیدن، جلو پیشرفت فناوری اطلاعات را بگیریم و حتی نمی توانیم از آن فرار کنیم؛ چرا که هیچ جایی برای فرار نخواهیم یافت که از این فناوری تأثیر نگرفته باشد. پس تعلل و اتلاف وقت برای چیست؟»(افق یک، ۱۳۸۱: ۲).

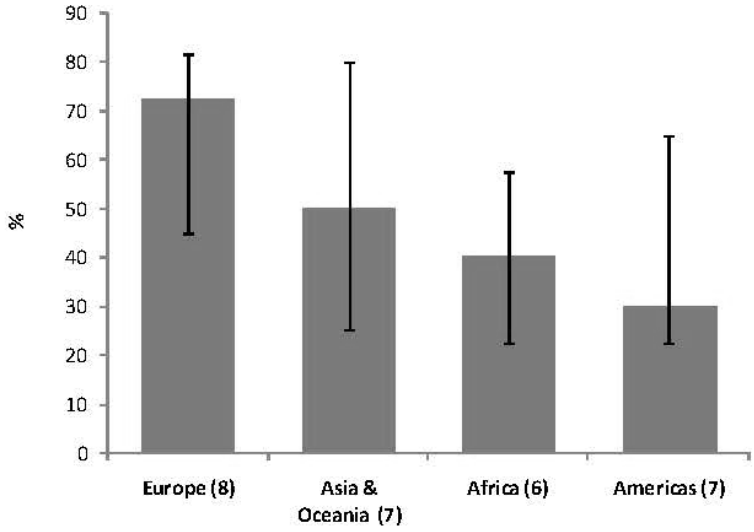
اولین واکنش قانونی جمهوری اسلامی ایران در برابر بعضی از جرایم رایانه‌ای، قانون اصلاح مطبوعات مصوب ۷۹/۱/۳۰ بوده که مورد تأیید شورای نگهبان قرار گرفته است. دومین واکنش جمهوری اسلامی ایران از طریق وضع «قانون حمایت از حقوق پدیدآورندگان نرم افزارهای رایانه ای» به عمل آمد. مادهٔ ۱۳ قانون مذکور، نقض حقوق پدید آورندگان آن دسته از نرم افزارهای رایانه ای را که مورد حمایت این قانون قرار گرفته اند، جرم تلقی و برای آن مجازاتی معادل ۹۱ روز تا ۶ ماه حبس و جزای نقدی تعیین کرده است. البته اشکالاتی بر این قانون وارد است که در این نوشته نمی‌گنجد. سومین عکس العمل قانون گذار ایران در مقابل جرایم ر ایانه ای در سال ۱۳۸۲ از طریق تصویب قانون مجازات جرایم نیروهای مسلح مصوب ۸۲/۱۰/۹ مجلس شورای اسلامی به عمل آمد به موجب مادهٔ ۱۳۱ این قانون، جعل اطلاعات و داده‌های رایانه‌ای، تسلیم و افشای غیر مجاز اطلاعات و داده‌ها و سوء استفادهٔ مالی از طریق رایانه (کلاهبرداری و اختلاس) توسط نظامیان جرم تلقی و مرتکب، حسب مورد به مجازات جرم ارتکابی محکوم می‌شود. چهارمین واکنش قانونی از طریق تصویب قانون تجارت الکترونیکی مصوب ۸۲/۱۰/۱۷ مجلس شورای اسلامی به عمل آمده است. به موجب مواد ۷۷، ۶۶، ۶۷، ۶۸، ۶۹، ۷۴، ۷۵ و ۷۶ این قانون، کلاهبرداری، جعل و دستیابی و افشای غیر مجاز اسرار تجاری، نقض حقوق مربوط به مالکیت معنوی

(کپی رایت) و غیره که از طریق رایانه و در بستر تجارت الکترونیکی انجام شود، جرم تلقی و برای آن مجازات تعیین شده است و پنجمین واکنش، بالاخره تصویب قانون جرایم رایانه ای بود که در سال ۱۳۸۸ به تصویب رسید(شیرزاد، ۸۵:۱۳۸۸).

ج) بررسی چالش‌های جرایم سایبری

۱- چالش‌های حقوق بین‌الملل عمومی: حقوق بین الملل عمومی، مجموعه قواعد و مقررات حاکم بر روابط دولت‌ها را مورد مطالعه قرار می‌دهد. بدین صورت که دولت‌ها در جهت منافع ملی خود، درصدد آن هستند که با رعایت چارچوب‌های قانونی و حقوقی اتخاذ شدهٔ دو یا چند جانبه، اقدامات خود را سازماندهی کنند. حال این منافع ملی می‌تواند منافع اقتصادی، نظامی، امنیتی، اجتماعی، سیاسی و ... را شامل شود. پایه و اساس حقوق بین‌الملل عمومی، بر وجود چالش‌های فراگیر در زمینه‌های بالا، دولت‌ها با سایر دولت‌ها در منطقه، فرامنطقه یا جهان استوار است. برای مثال، زمانی که کشورها در خصوص برداشت منافع و منابع ملی با سایر کشورها به چالشی برخورد می‌کنند، تنها می‌تواند این چالش را با رجوع به مفاد معاهدات منعقده یا مورد قبول آنان مرتفع کرد. بنابراین، نقطهٔ تکامل و پیشرفت حقوق بین الملل عمومی، وجود چالش‌های مشترک فی مابین کشورها و تلاش درجهت رفع حداقلی آنهاست؛ اما یکی از چالش‌هایی که امروزه دولت ها با آن روبه‌رو هستند، ظهور پدیدهٔ فراملی فضای سایبری و به تبع آن جرایم سایبری است. برابر آمارهای کسب شده در سال ۲۰۱۲ توسط دفتر مقابله با جرم و مواد مخدر سازمان ملل[1](۱۳۹۱)، بیش از نیمی از کشورها گزارش داده اند که بین ۵۰ تا ۱۰۰ درصد از جرایم سایبری که توسط پلیس به آنها برخورده شده است، ابعاد فراملی داشته است(ص ۴۱). شکل شمارهٔ ۱ نشان می‌دهد که کشورهای اروپایی، بالاترین نسبت جرایم سایبری را دارا هستند.

1- UNODC



Source: Study cybercrime questionnaire. Q83. (n=28)

نمودار ۱ : درصد اعمال مجرمانهٔ سایبری[۱]

- **حق حاکمیت و استقلال دولت‌ها:** برابری حق حاکمیت کشورها توسط قوانین متعارف حقوق بین‌الملل عمومی تعریف شده است. این قوانین شامل تعهداتی برای کشورهاست تا به هیچ شکلی و به هیچ دلیلی به منافع کشور دیگر در داخل یا خارج از کشور تجاوز نکنند. بر این اساس، موضوعات اعمال قوانین و قضاوت به طور سنتی به مرزهای جغرافیایی پیوند خورده است. بنابراین کشورها باید از فشار آوردن جهت تأثیرگذاری بر سایر کشورها در خصوص رفتار نهادهای قضایی همانند قوهٔ قضائیه خودداری کنند. بر این اساس، داخل مرزهای یک کشور دیگر نمی توان اشخاص را دستگیر کرد، نمی‌توان احضاریه برای اشخاص صادر کرد یا تحقیقات پلیسی یا مالیاتی را به اجرا گذاشت، مگر تحت شرایط یک معاهده یا موافقت‌نامهٔ مشترک که این خود از موارد توسعهٔ تدریجی حقوق بین المللی به‌شمار می آید.

در جرایم سنتی که یکی از عناصر متشکلهٔ جرم همانند محل وقوع جرم، محل اقامت متهم یا ملیت شاکی و متهم، موجبات تدوین و تنظیم تفاهم نامه های

۱- اعمال مجرمانهٔ سایبری که در بر دارندهٔ یک بعد فراملّی بوده‌اند، میزان آن برای کشورهای اروپایی بالای ۷۰ درصد است.

همکاری را میسر می ساخت، متأسفانه در جرایم سایبری وضع به همین منوال نیست. برای مثال احتمال دارد یک مجرم تبعهٔ یک کشور افریقایی از یک کافی نت در یک از شهرهای آمریکا و با استفاده از پهنای باند اختصاصی چندین کشور اروپایی، وارد یک حساب کاربری در یک بانک ایرانی شده و حساب یک شخص را به حساب دیگری در بانکی واقع در هنگ کنگ خالی کند. همان‌طور که ملاحظه می‌شود چندین کشور با عناصر متشکلهٔ شکلی یک جرم درگیر هستند و وضعیت انعقاد تفاهم‌نامه بر معیارهای تعیین شدهٔ سنتی بسیار متفاوت است.

- **همکاری‌های بین المللی:** در اغلب جرایم سنتی، تنها دو یا سه کشور محدود شمار با پدیدهٔ جرم سنتی مواجه هستند. برای مثال، در مبحث قاچاق مواد مخدر، محل ترانزیت مواد مخدر از کشور مبدأ تا مقصد مشخص است، یا کسی که یک جرمی را در یک کشور انجام داده و در حال حاضر به یک کشور دیگر فرار کرده است نیز روند شفافی را دنبال می کند و بر این اساس، دولتمردان با انعقاد تفاهم‌نامه های همکاری دو یا چند جانبه، در مباحث معاضدت قضایی یا استرداد مجرمان، سعی در رفع حداقلی این چالش هستند. اما در جرایم سایبری با توجه به موارد اشاره شده در بخش حق مالکیت و استقلال، باید سطح همکاری‌های بین المللی در سطح وسیع‌تر مورد مطالعه قرار گیرد.

۲- چالش‌های حقوق بین‌الملل خصوصی: از ویژگی‌های مهم جرایم رایانه‌ای و جرایم اینترنتی، ماهیت فراملی بودن این‌گونه جرایم است که به دلیل قابلیت‌های فنی رایانه‌ها و اجزای مرتبط با آن، امکان ذخیره سازی، حرکت، استفاده از داده‌ها از طریق شبکه‌ها و ایجاد ارتباط و انتقال سریع درسطح وسیع بین سیستم‌های رایانه ای افزایش یافته است، به طوری که دامنهٔ گسترش سیستم‌های رایانه ای از محیط رایانه و شبکهٔ داخلی به سطح بین‌المللی، گسترش پیدا کرده و موجب خلق نسل جدید جرایم رایانه ای یعنی جرایم در محیط سایبری شده است که ماهیت و خاصیت کاملاً فراملی و بین المللی دارند. به هر حال، امروزه جرایم رایانه ای تبدیل به یک پدیدهٔ مجرمانهٔ کاملاً بین‌المللی شده است. در مسائل بین المللی، اولین اثر جرایم رایانه ای، بحث صلاحیت است. علی‌الخصوص در قواعد حاکم بر صلاحیت سرزمینی و مکان ارتکاب، مقام صالح دچار مشکل می‌شود. زیرا جرایم رایانه‌ای، فراملی بوده که موجب

تعدد محل ارتکاب و تعدد صلاحیت‌ها می‌شوند. در بحث صلاحیت‌ها، علاوه بر موضوعاتی از قبیل تابعیت مجرم، تابعیت بزه دیده، نوع جرم ارتکابی (جاسوسی رایانه‌ای، تخریب داده رایانه ای [1] و ...) بحث صلاحیت شخصی و واقعی نیز مطرح می‌شود.

- **تعارض دادگاه‌ها:** ماهیت جرایم سایبری به این صورت است که چالش‌های عمیق موجود در نظام حقوق بین‌الملل همانند تعارض دادگاه‌ها و تعارض قوانین را شدت می‌دهد. زیرا، در جرایم سایبری محل وقوع جرم مشخص نیست تا دادگاه صالح به رسیدگی بر آن جرم را مشخص کند. از این رو، بسیاری از کشورها، مکان ارتکاب را بر مبنای دکترین (حضور درهر جا) [2] تعیین می‌کنند. طبق این دکترین، جرم چنانچه، مقدار یا فقط بخشی از آن در یک مکان ارتکاب یافته باشد، تماماً ارتکاب یافته در آن محل فرض می‌شود، بدین ترتیب که طبیعی است که چند دولت خود را صالح به رسیدگی بدانند(شورای اروپایی جرایم سایبری [3]، ۱۹۹۰: ۱۵۳).

اصل صلاحیت شخصی براساس تابعیت مجرم استوار است که به‌کارگیری آن عموماً به جرایم مهم محدود می‌شود تا از بروز صلاحیت‌های موازی اجتناب شود. اصل صلاحیت شخصی منفعل که به تابعیت بزه دیده بستگی دارد، به‌دلیل انتقادهایی که از آن به عمل آمده است به ندرت اعمال می‌شود. اصل صلاحیت براساس حمایت از منابع حیاتی و ملی یک کشور استوار است و طبق این اصل، یک کشور می‌تواند در موارد جرایم ارتکابی در خارج از کشور که امنیت ملی را به خطر می اندازند، صلاحیت خود را اعمال کند(عبقری، ۹۳:۱۳۷۷).

حال باتوجه به موارد فوق، نتیجهٔ مطالعات صورت گرفته از طرف دفتر مقابله با جرم و مواد مخدر سازمان ملل در دو حوزهٔ استفاده از حاکمیت قضایی و استفاده از رسیدگی قضایی مبتنی بر ملّیت به شرح زیر مورد تجزیه قرار می‌گیرد:

- استفاده از حاکمیت قضایی

الف)اسناد بین‌المللی و منطقه‌ای: تمامی اسناد بین‌المللی و منطقه ای جرایم سایبری

---

1 sabotage
2- Ubiquity
3- Council of Europe - Cybercrime

که در بر دارندۀ یک ماده قانون قضایی هستند، اصل حاکمیت مرزی را محترم می‌شمارند، یعنی از کشورها می‌خواهند که قضاوت‌ها را در مورد هر عملی که مطابق با آن سند، جرم تعیین شده است و در داخل مرزهای هر کشور ارتکاب شده است، استعمال کنند. همچنین فعالیت‌های مجرمانه در کشتی و هواپیما نیز توسط یک‌سری از اسناد الزام‌آور و غیرالزام‌آور پوشش داده شده‌اند. مطابق اصل حاکمیت مرزی واقعی، بسیاری از اسناد بین‌المللی و منطقه‌ای تعیین می‌کنند که برای به‌کار بردن حاکمیت قضایی مرزی، لازم نیست تمامی عناصر جرم در داخل مرز یک کشور رخ داده باشند. برای مثال، گزارش تشریحی معاهدۀ جرایم سایبری شورای اروپا تصریح می‌کند که تحت اصول حاکمیت مرزی، هریک از اعضاء می‌تواند هم درصورتی که شخص حمله کننده به یک سیستم رایانه ای و سیستم قربانی هردو در داخل مرزهای آن کشور قرار داشته باشند، هم در صورتی که سیستم رایانه ای مورد تهاجم در داخل مرزهای کشور قرار داشته باشد؛ حتی اگر مهاجم در خارج از مرزها واقع شده باشد، از حاکمیت قضایی خود بر علیه آن مجرم استفاده کند. (دفتر مقابله با جرم و مواد مخدر سازمان ملل، ۲۹۸:۱۳۹۱).

ب)رویکردهای ملّی: تأثیر رویکردهای حاکمیتی در اسناد بین‌المللی و منطقه ای در سطح ملّی در همه حال آشکار است. کشورها، گستره‌ای از مقررات را گزارش کرده‌اند که انعکاس دهندۀ این ایده است که لازم نیست کل جرم برای اینکه قضاوت حاکمیتی به اجرا گذاشته شود، در داخل کشور رخ داده باشد. اما مکانیزم‌ها برای شناسایی ارتباطات حاکمیتی فرق داشتند (دفتر مقابله با جرم و مواد مخدر سازمان ملل، ۱۸۹:۱۳۹۱).

- استفاده از رسیدگی قضایی مبتنی بر ملّیت

الف)اسناد بین‌المللی و منطقه ای: درجایی که اسناد بین‌المللی و منطقه‌ای جرایم سایبری، اصول حاکمیت داخلی را تشخیص بدهند، این اسناد، اصل ملیت فعال را نیز شامل خواهند شد. این مستلزم آن است که یک کشور از رسیدگی قضایی در هنگامی که جرم توسط یکی از اتباعش، اگرچه در خارج از مرزهای آن کشور ارتکاب شده باشد، اطمینان حاصل کند. تنها تعداد محدودی از اسناد برای قضاوت برمبنای اصل ملیت غیرفعال، مقرر شده‌اند. مانند آنهایی که به حقوق کودکان مربوط می‌شوند.

دستورالعمل اتحادیهٔ اروپا در زمینهٔ بهره‌کشی از کودکان سازمان ملل متحد از کشورها می‌خواهد که برروی جرایمی که در خارج از مرزها بر علیه یکی از اتباع آنها یا شخصی که یک شهروند دائمی محسوب می شود، ارتکاب می‌یابد، عملیات قضایی را به مورد اجرا بگذارند. معاهدهٔ محافظت از کودکان شورای اروپا، مقرر می‌دارد که کشورهای طرف قرار داد باید برای به اجرا گذاشتن چنین قضاوت‌هایی کوشش کنند. این گونه مقررات، اختیارات قضایی را برای تضمین محافظت از کودکان این کشورها در سرتاسر دنیا به آنها عرضه می‌دارد.

ب)رویکردهای ملّی: تعدادی از کشورها به استفاده از اصل ملّیت فعال برای به اجرا گذاردن قضاوت‌ها در زمینهٔ جرایمی که توسط اتباع آنها انجام گرفته‌اند، در هر جایی که ارتکاب یافته باشند، اشاره کرده‌اند. اگرچه این یک الزام رایج نمی‌باشد، ولی معدودی از کشورها متذکر شده‌اند که الزامی برای برخی اَعمال وجود دارد که در کشوری که در آن ارتکاب شده اند به عنوان یک جرم شناخته شوند. تعداد کمی از کشورها، همچنین به اصل ملّیت غیرفعال برای قضاوت درمورد جرایم تأثیرگذار بر روی اتباع آنها، در هرکجا که روی دهند، اشاره کرده‌اند. برای مثال، یک کشور اروپایی گزارش داد که بسیاری از موارد جرایم سایبری که با آنها مواجه شده است دارای عناصر فرامرزی بوده‌اند و اینکه در برخی از موارد قربانیان ملی در خارج از کشور حضور داشته‌اند که باعث پیچیدگی‌های قضایی شده است. کشور اروپایی دیگری گزارش داده که قانون کیفری جدیدی را اتخاذ کرده است که مشتمل بر اصل ملیت غیرفعال به ویژه برای کاستن از مشکلات قضایی در پرونده‌هایی که در آن ارتکاب کننده یک خارجی بوده و جرمی را در خارج از کشور مرتکب شده است که بر روی یک تبعهٔ کشور در خارج از مرز تأثیر گذاشته است می‌باشد(دفتر مقابله با جرم و مواد مخدر سازمان ملل، ۱۳۹۱:۱۳۳).

- استفاده از سایر نهادهای رسیدگی کنندهٔ قضایی

الف) اسناد بین‌المللی و منطقه ای: دو سند، معاهدهٔ انجمن کشورهای عرب و قانون مدل، خصوصاً برای اصل محافظت کننده تدارک دیده‌اند. برای مثال، معاهده مشخص می‌کند که کشورهای طرف قرارداد باید صلاحیت جرایم تأثیرگذار برروی یک سرمایهٔ برجسته از کشور را گسترش دهند. سندهای اروپایی، نظیر قرار اتحادیهٔ اروپا در زمینهٔ

حملات تأثیرگذار برعلیه سیستم‌های اطلاعاتی، همچنین شامل یک مبنای اضافی از قضاوتی که جرایم ارتکاب شده برای منافع یک شخص حقوقی که دفتر اصلی آن در داخل کشور قرار دارد را پوشش می‌دهد، استوار است. درنهایت، مطابق اصل «استرداد و پیگرد مجرمان»، یک سری از اسناد برای قضاوت در مواردی که یک مجرم منتسب در داخل مرزهای یک کشور حضور داشته و کشور او را صرفاً به دلیل ملیتش، پس از ارائه درخواست استرداد به کشور دیگری مسترد نمی‌کند، مقرر شده اند.

ب) رویکردهای ملّی: تعداد کمی از کشورهای پاسخ دهنده به اصل محافظتی در مضمون شرایط الصاق شده به سایر اشکال قضاوت اشاره کرده‌اند. آنچنان که به سایر نهادهای قضایی نظیر قضاوت جهانی، مربوط می شود، تعدادی از کشورها شرایطی را مورد اشاره قرار دادند که در آن یک ارتکاب کنندهٔ خارجی یک جرم، کاملاً فرامرزی در داخل مرز حضور دارد، ولی درخواستی برای استرداد او وجود ندارد. برخی از کشورها، متذکر شدند که قضاوت جهانی به جرایم بین‌المللی ذاتی محدود شده است و عموماً اعمال مجرمانه سایبری را پوشش نمی‌دهند. اما سایر کشورها، توصیه کردند که برخی از اعمال مجرمانهٔ سایبری سخت نظیر پورنوگرافی کودکان، می‌توانند در یک چنان شکلی از قضاوت قرار گیرند.

- **تعارض قوانین:** ساختارهای حقوقی متفاوتی در سطح دنیا وجود دارد و کشورها از این ساختارها تبعیت می کنند. برای مثال کشور جمهوری اسلامی ایران از ساختار مختلط پیروی می‌کند(حقوق نوشته و حقوق اسلامی). بر این اساس، مجموعه رفتارهای قانونی کشورها نیز در مواجه با جرم سایبری متمایز است و این امر در سطح وسیع تر و در سطح بین المللی، موجب شدت گرفتن تعارض قوانین کشورها در مقابله با جرایم سایبری می‌شود. بسیاری از کشورها در زمینه جرایم سایبری فاقد جرم‌انگاری بوده و هیچ قانونی برای آن ندارند و از طرفی، برخی از کشورها نیز بسیاری از مواردی را که توسط بسیاری از کشورها جرم انگاری شده را جرم‌انگاری نکرده اند. برخی از کشورها همانند کشور جمهوری اسلامی ایران فاقد قانون جامع و کامل در این خصوص است. موارد فوق موجب شده است که چالش پیش‌رو در حوزهٔ تعارض قوانین، بسیار عمیق‌تر از موارد تعارض قوانین سنتی در حقوق بین‌الملل محسوب شود.

۳- چالش‌های حقوق ماهوی و شکلی ایران: در طول قرون متمادی، سیستم‌های قضایی بر موضوعات ملموس و عینی متمرکز شده اند و مقررات جزایی به حمایت از این دسته موضوعات پرداخته است. این در حالی است که امروزه اموال غیر مادی اهمیت بسیار یافته اند. داده ها و اطلاعات تبدیل به نوعی دارایی شده‌اند که می‌توان موضوع ارتکاب جرم واقع شود و رژیم حقوقی مربوط به موضوعات این چنینی، تنها نمی‌توانند بر مبنای قیاس با قواعد موجود و مختص به موضوعات مادی بنا شود؛ زیرا نحوهٔ ارزیابی و حمایت داده ها و اطلاعات با آنچه در خصوص اشیای مادی مقرر است تفاوت قابل ملاحظه ای دارد. بدین سان که اشیای مادی را می‌توان به افراد خاصی نسبت داد، ولی اطلاعات کالایی عمومی است که علی الاصول بنابر قاعدهٔ «دسترسی آزاد به اطلاعات»[1] بایستی به صورت آزادانه در جامعه جریان داشه باشد. بنابراین، همچون اموال مادی مشمول حمایت انحصاری واقع نمی شود. علاوه بر این، در راستای حمایت از اطلاعات، نه تنها باید منافع مالک یا دارندهٔ آن مدنظر قرار گیرد، بلکه منافع کسانی که به نحوی با محتوای اطلاعات سرو کار دارند نیز باید محفوظ بماند. پس ملاحظه می‌شود که نمی‌توانیم به قواعد موجود در زمینهٔ اموال مادی بسنده کنیم و به تغییر در طرح و چهارچوب قضایی جاری نیازمندیم.

حقوق جزایی ماهوی در ارتباط با جرایم رایانه ای، از دو لحاظ با مشکل مواجه است: از یک سو، اوصاف و عناصر متشکله جرایم کلاسیک دستخوش تحولاتی گشته اند؛ تا جایی که نمی‌توان تعاریف مجرمانهٔ موجود در متن قانونی را به جرایم رایانه‌ای مشابه تسری دارد و از سوی دیگر، عناوین مجرمانهٔ نوینی نیاز است تا برخی دیگر از راه‌های سوء استفاده رایانه ای را که به طور جدی جوامع بشری را تهدید می‌کند، به عنوان جرم شناسایی کنیم.

نتیجه‌گیری

به طورکلی پیشرفت علم و گسترش فناوری علاوه بر محاسن و ویژگی‌های مثبت وافر, اصولاً مشکلات و معضلاتی را نیز به دنبال خواهدداشت. همان گونه که فناوری

1- Free Access To Information

رایانه و ارتباطات، سهولت روابط بین افراد و بسیاری از نیازهای جامعه بشری را برآورده کرده و در هر زمینه ای، رفاه و راحتی را به ارمغان آورده است، از طرفی، راه سوء استفاده را برای افراد بزهکار و مجرمان هموار کرده است.

در حقوق کیفری و سیاست جنایی همانند سایر علوم و دیگر شاخه های علم حقوق، مسائل جدیدی در غالب جرایم به وجود آمده است که باید ضمن شناسایی، تعریف و تجزیه و تحلیل این دسته از جرایم نوین، راهکار های پیشگیری و محدود ساختن طرق ارتکاب و مبارزه پیش بینی شود. باتوجه به رشد بسیار سریع فناوری رایانه و گسترش فناوری ارتباطی و تبادل اطلاعاتی به کمک رایانه و اجزای وابسته به آن، در ارتباط و وابستگی تنگاتنگ جامعهٔ امروزی به این فناوری، از بُعد حقوق کیفری، اقدامات خاص قضایی یکسان با جامعهٔ جهانی، چه در زمینهٔ تدوین قوانین جدید و کارآمد و چه در زمینهٔ اقدامات امنیتی در حفاظت از سیستم‌های رایانه ای و شبکه ای و آموزش نیروی متخصص، ضروری و لازم می آید. از جهتی علوم جنایی در مواجهه با جرم سایبری با یافته های جدید روبرو است که در زمینهٔ پیشگیری و بزه دیده شناسی، مسائلی قابل طرح و بحث می‌باشد که در حقوق کلاسیک بی سابقه بوده است. اما در خصوص قوانین موضوعه ایران، باید اذعان کرد که هر یک از قوانین فوق الذکر، در بستر خاص خود قابلیت اِعمال دارند. مثلاً قانون مطبوعات صرفاً نسبت به جرایم رایانه‌ای ارتکابی در قالب نشریه‌های الکترونیکی و قانون مجازات نیرو های مسلح صرفاً در مورد بعضی از جرایم رایانه‌ای نظامیان و قانون تجارت الکترونیکی فقط در مورد برخی از جرایم رایانه‌ای ارتکابی در بستر تجارت الکترونیکی قابل اجرا هستند. اما به نظر می‌رسد که بسترهای فراهم شده از طریق قوانین موضوعهٔ ایران به علت نوپا بودن این قوانین و نیز تکاپوی سریع فناوری در فضای سایبری، جوابگوی نیازهای حقوقی فضای سایبری نبوده و باید به حالت رشد و تعالی درآورد.

در طول قرون متمادی، سیستم‌های قضایی سنتی بر اهداف و موضوعات ملموس و عینی متمرکز شده بودند و در حالی که، امروزه اموال غیر مادی اهمیت بسزایی یافته است. از آنجایی که رِژیم حقوقی برای اموال و موضوعات غیر فیزیکی نمی‌تواند بر مبنای قیاس با قواعد موجود و صرف موضوعات مادی بنا باشد، لذا تحول فناوری، منجر به تغییر در طرح و چارچوبهٔ قضایی کشورها و یک تئوری جدید در وضع حقوق

اطلاعات شده است.

دکترین جدید حقوق کیفری در زمینهٔ فناوری ارتباطی، باید بر مبنای اصول جریان آزاد اطلاعات و تکیه بر موضوعات غیر ملموس و مجازی بنیان شود. به دلیل رشد سریع فناوری رایانه ای، هنوز در تمامی دنیا قوانین تدوین شده در زمینهٔ جرایم رایانه‌ای و شبکه ای، جایگاه و منزلت خود را به طور کامل پیدا نکرده اند. در حال حاضر، کشورهای جهان در این خصوص در سطح یکسانی قرار ندارند و پیشگامان تدوین و اصلاح قوانین را می‌توان غالباً کشورهای اروپایی و آمریکایی دانست.

در خصوص آئین دادرسی جرایم رایانه ای و نحوهٔ دادرسی و جمع آوری ادله و شواهد دیجیتال و مراحل آئین‌دادرسی در ایران، باید اذعان کرد که این موارد با استفاده از قوانین قبلی انجام می‌گیرد. با توجه به مقولات ارائه شده و بررسی انجام گرفته در خصوص ماهیت جرایم سایبری باید نسبت به ارائه و وضع قوانین آئین دادرسی در مواجه با این نوع جرایم اقداماتی صورت پذیرد به این دلیل که:۱- جرایم سایبری جرایمی فرامنطقه ای و فراملی بوده و مجموعه قوانین و مقررات آئین دادرسی کنونی در خصوص صلاحیت دادگاه‌ها، این موضوع را به چالش می‌کشاند و۲- بحث جمع آوری و اثبات ادله و شواهد دیجیتال کاملاً با مباحث جرایم قبلی متفاوت است.

منابع

- افق یک(۱۳۸۱). *اطلاعات فناوری قضا*، تهران: دفتر همکاری‌های فناوری ریاست جمهوری.

- باستانی، برومند(۱۳۸۳). جرایم کامپیوتری و اینترنتی، تهران: انتشارات بهنامی.

- باستانی، برومند(۱۳۸۶). *جرایم کامپیوتری و اینترنتی جلوه ای نوین از بزهکاری*(جلد سوم)، تهران: انتشارات بهنامی.

- بای، حسینعلی و پورقهرمانی، بابک(۱۳۸۸). *بررسی فقهی حقوقی جرایم رایانه ای*، تهران: پژوهشگاه علوم و فرهنگ اسلامی.

- دفتر مقابله با جرم و مواد مخدر سازمان ملل(۱۳۹۱). *مطالعهٔ جامع جرایم سایبری*، ترجمه: حمید صادقی، تهران: انتشارات پلیس فتا.

- زرگر، علیرضا (۱۳۸۵). *امنیت و تهدید در جامعه اطلاعاتی*، تهران: انتشارات قدیم.
- سازمان ملل(۱۳۷۶). *نشریهٔ سیاست جنایی(جلد اول- ش۴۳-۱۹۹۴/۴۴)*، ترجمه: دبیرخانهٔ شورای عالی انفورماتیک سازمان برنامه و بودجه کشور، شمارهٔ ۴۹-۵۰.
- شیرزاد، کامران(۱۳۸۸). *جرایم رایانه ای از دیدگاه حقوق جزای ایران و حقوق بین الملل*، تهران: شرکت نشر بهینه فراگیر.
- صبح‌خیز، رضا(۱۳۹۱). *بررسی تطبیقی جرایم سایبر در نظام حقوق بین الملل و حقوق ایران*(پایان‌نامهٔ کارشناسی ارشد)، دانشگاه آزاد اسلامی واحد مراغه.
- عبقری، آدینه(۱۳۷۷). جرایم کامپیوتری، جلوه ای نوین از بزهکاری(پایان نامهٔ کارشناسی ارشد)، تهران: دانشگاه تهران.
- Council of Europe – cybercrime (1990). Recommendation No. 89, *Strasbourg, the translation of the High Council of Informatics*, Management and Planning Organization of Iran, 1376.