فصلنامه علوم خبری
سال دوازدهم، شماره ۴۷ پاییز ۱۴۰۲
صفحات ۳۰-۱۱

La revue science de I'information
année 12 / No 47 Automne2023
pages: 11-30

سازوکارهای تقنینی کشورها در قبال جرائم رایانه ای در اسناد بین المللی

علی زلقی(نویسنده مسئول)

گروه حقوق جزا و جرم شناسی،واحد تهران مرکزی،دانشگاه آزاد اسلامی،تهران،ایران
رایانامه: juristic.1986@gmail.com

اطلاعات مقاله

نوع مقاله: مقاله پژوهشی

تاریخ دریافت:
تاریخ بازنگری:
تاریخ پذیرش:
تاریخ انتشار:

کلیدواژه‌ها:
فضای سایبری
جرایم رایانه ای
هک
فیشینگ
سایبراستالکینگ

چکیده

بیشتر کشورهای دنیا جرایم اینترنتی بعنوان یک معضل حاد و بسیار مهم تلقی می گردد و دولت‌ها در صدد پیدا نمودن راه حل های مختلفی در جهت جلوگیری از وقوع آن می باشند.جرایم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای به عنوان جرایمی که حریم خصوصی اشخاص را مورد تعرض قرار داده و سبب از بین رفتن محرمانگی داده‌ها و سامانه‌های رایانه‌ای می‌گردند، به موازات طرح در حقوق داخلی در قلمرو اسناد بین‌المللی نیز قابل بررسی می‌باشند.فضای سایبر، امکان ارتکاب جرایم مدرنی که در قوانین قبل جرم‌انگاری نشده بود را، برای مجرمان در اقصا نقاط جهان فارغ از مرزهای جغرافیایی بوجود آورد؛ لذا این موضوع توجه قانونگذاران در سطح ملی و بین‌المللی را به خود جلب کرد و حتی قانونگذاران دریافتند که محدود نمودن قلمرو جرایم رایانه‌ای به موارد مدون در اسناد و قوانین ملی یارای مقاومت در برابر این جرایم را ندارد. حال سوال این است که کشورهای مختلف در قبال جرائم رایانه ای در فضای سایبری چه سازوکارهای قانونی را بکار گرفته اند؟ یافته ها بیانگر این نکته است که در بیشتر کشورها جرایم رایانه ای بعنوان یک موضوع جدی مطرح است و کشورها با تصویب قوانینی متناسب با نوع جرایم در پیشگیری از آن تدابیر لازم را اندیشیده اند.

کلیدواژه‌ها: فضای سایبری، جرایم رایانه ای،هک، فیشینگ، سایبراستالکینگ

استناد: نام خانوادگی، نام؛ نام خانوادگی، نام؛ و نام خانوادگی، نام (۱۴۰۱). عنوان مقاله. *علوم خبری*، ۱۱ (۳)، ۲۰-۱.
DOI: http//doi.org/0000000000000000000000000

مقدمه

جرائم رایانه‌ای (سایبر کرایم) یکی از پیش‌رونده‌ترین جرائمی است که با سرعت زیاد در حال گسترش و بلای جان بشر امروز شده است. جهان امروز جهان علم و فناوری است و بی‌شک پیشرفت را نمی‌توان از آن جدا کرد. این در حالی است که همگام با پیشرفت‌های علمی به‌ویژه در زمینه رایانه و اینترنت، عده‌ای برخلاف خدمتگزاران بشریت که به فکر استفاده‌های مثبت از فناوری‌ها هستند به فکر سوءاستفاده‌اند. جرائم رایانه‌ای جرائمی سازمان‌یافته می‌باشند که از طریق اشخاص حرفه‌ای و باسواد انجام می شوند و همیشه و مجازات‌ها قوانین رایانه ای امروزه برای مجازات مجرمین کافی اما کامل نمی باشد چون هر روز جرائم جدیدی به وجود می آید که برای مجازات آن‌ها نیاز به قوانین جدید داریم همان‌گونه که جرائم اینترنتی همیشه در حال روز شدن هستند بایستی تلاش کرد تا بتوان با نو شدن جرائم هرساله قوانینی را که در زمینه جرائم جدید قابل اعمال باشد ارائه کرد چون رایانه و اینترنت همیشه و همیشه شکل های مختلفی به خود می گیرند(شیرزاد،۳۸:۱۳۸۸). با گسترش علم و فناوری اطلاعات و استفاده از رایانه در زندگی شخصی و اجتماعی و روابط اداری، بزهکاری و تخلف در استفاده از رایانه نیز تبدیل به امری اجتناب‌ناپذیر شده است. آنچه امروز تحت عنوان جرائم رایانه‌ای شناخته می‌شود، مجموعه‌ای از همین تخلفات و بزهکاری‌هاست که از طریق رایانه و یا مؤثر بر رایانه اتفاق می‌افتد. همچنین می‌توان گفت جرائم رایانه‌ای، جرائم سنتی هستند که با فناوری اطلاعات از طریق رایانه صورت می‌گیرد، لذا برای رسیدگی به آن و اِعمال مجازات، ناگزیر از وضع اعمال و مقرراتی هستیم که متفاوت از شکل سنتی آن است. نوین ممتاز بودن جرائم رایانه‌ای و خصوصیات منحصربه‌فرد آن، همچون عدم لزوم حضور مرتکب در محل جرم در کنار شیوهٔ ارتکاب این‌گونه جرائم و گاها داشتن جنبه بین‌المللی آن، نحوهٔ رسیدگی و تعقیب را از جهت مسائل آیین دادرسی با چالش‌هایی رو به کرده است. در کشور، آیین‌دادرسی کیفری در خصوص جرائم رایانه‌ای در خردادماه ۸۸ به تصویب مجلس شورای اسلامی رسید که در بخش دوم آن از ماده‌ی ۲۸ تا ۵۱ آیین‌دادرسی جرائم رایانه‌ای بیان شده است. کشف جرم، تعقیب مجرم، جمع‌آوری ادله، حفظ و نگهداری آن‌ها، قابلیت استناد، استنادپذیری ادله از مهم‌ترین مباحث در آیین‌دادرسی این‌گونه جرائم محسوب می‌شود(عمیدی،۶۷:۱۳۸۷).

با توجه به اینکه فضای مجازی روز به‌روز گسترده‌تر می‌شود و در عین حال شیوه‌های ارتکاب جرم نیز با پیشرفت تکنولوژی، رنگ و بوی دیگری می‌گیرد شناخت ابعاد حقوقی جرائم رایانه‌ای و شیوه دادرسی آن با توجه به اینکه کشور ایران نیز مبتلا به این پدیده است امری ضروری است. تلاش در راستای شناخت *نحوه* دادرسی جرائم رایانه‌ای و مراحل آن و کشف و تحلیل نواقص موجود در قانون جرائم رایانه‌ای در راستای رسیدگی هرچه سریع‌تر و بهتر به این جرم و همچنین پیشگیری از آن اموری هستند که کشور بیش از پیش به آن نیاز دارد.

۱. جرایم سایبری و انواع جرم های سایبری

جرائم سایبری یا رایانه ای عبارت است از هرگونه تخلف از قانون کیفری که دانش فناوری رایانه‌ای را در ارتکاب، تحقیق و پیگرد شامل می‌شود. جرائم رایانه ای به چند دسته تقسیم می شوند(پاکزاد،۳۵:۱۳۸۰). دستهٔ اول: جرائمی هستند که در آن‌ها رایانه و تجهیزات جانبی آن موضوع جرم واقع می‌شوند مانند سرقت، تخریب و غیره. دستهٔ دوم: جرائمی هستند که در آن‌ها کامپیوتر به‌عنوان ابزار یا وسیله توسط مجرم برای ارتکاب جرم بکار گرفته می شود. دستهٔ سوم: جرائمی هستند که می‌توان آن‌ها را جرائم کامپیوتری محض نامید. این نوع از جرائم کاملاً با جرائم کلاسیک تفاوت دارند و در دنیای مجازی به وقوع می پیوندند؛ اما آثار آن‌ها در دنیای واقعی ظاهر می‌شود، مانند دسترسی غیرمجاز به سیستم‌های کامپیوتری، سازمان همکاری و توسعه اقتصادی جرم رایانه ای را چنین تعریف می کند «سوءاستفاده از کامپیوتر شامل هر رفتار غیر قانونی غیراخلاقی یا غیرمجاز مربوط به پردازش اتوماتیک و انتقال داده-هاست» (شیرزاد،۵۵:۱۳۸۸).

۱-۱. **هک کردن:** عبارت است از نفوذ به یک سیستم کامپیوتری بدون داشتن مجوز، مالکیت یا صلاحیت لازم. هک کردن یعنی غلبه کردن بر سیستم‌های امنیتی یک سیستم کامپیوتری برای دسترسی غیر قانونی به اطلاعات ذخیره شده در این سیستم کامپیوتری. لو رفتن رمز عبور به‌قصد دسترسی به اطلاعات خصوصی افراد یک سازمان یکی از رایج‌ترین تخلفات رایانه‌ای است. یکی از خطرناک‌ترین خلاف کاری‌های رایانه‌ای عبارت

است از هک کردن آدرس IP تا بدین‌وسیله خلافکار خود را به‌جای کس دیگر جا بزند و افکار شوم یا جنایات مورد نظر خود را اجرا کند(عالی پور،۱۳۹۰:۳۰).

۱-۲.**فیشینگ**: عبارت است از تلاش برای به دست آوردن اطلاعاتی مانند رمز عبور، شناسه عبور و جزئیات کارت اعتباری با جا زدن خود به‌عنوان یک منبع قابل‌اعتماد. فیشینگ از طریق سرویس‌های ایمیل یا با وعده‌های دروغ انجام می‌گیرد یا با ایجاد برخی جذابیت¬ها کاربران اینترنتی را ترغیب می کنند اطلاعات خود را در سایت‌هایی که توسط کلاه‌برداران ساخته شده است وارد کنند. این خلاف‌کاران معمولاً وب‌سایت‌هایی طراحی می کنند که در کاربر احساس اعتماد و وارد شدن در یکسایت امن را می‌دهد و معمولاً هم موفق می‌شوند یعنی کاربر در دام آن‌ها افتاده و اطلاعات خود را وارد می کند(عمیدی،۱۳۸۷:۳۱). فیشینگ نوع بسیار خاصی از جرائم رایانه‌ای است که برای فریب دادن شما در زمینه افشای جزئیات مالی و شخصی شما، طراحی شده است. مجرمان رایانه‌ای، یک وب‌سایت جعلی ایجاد می‌کنند که بسیار شبیه به وب‌سایت بانک (یا هر وب‌سایت دیگری که تراکنش‌های مالی در آن انجام می‌شود مانند $(eBay)$ است. سپس تلاش می‌کنند تا شما را به‌منظور بازدید از این سایت و تایپ کردن اطلاعات محرمانه خود نظیر اطلاعات ورود به سایت، کلمه عبور و PIN فریب دهند. نوعاً مجرمان رایانه‌ای تعداد زیادی نامه‌های الکترونیکی ارسال می‌کنند که حاوی یک فراپیوند به سایت جعلی است. حمله فیشینگ نوعی ویژه از جرم سایبری است که در آن، مجرم یک کپی تقریباً ۱۰۰ درصد شبیه یک وب‌سایت بنگاه تجاری، ایجاد می¬کند. سپس تلاش میکند تا کاربران را برای افشای جزئیات شخصی خود نام کاربری، کلمه عبور، PIN و غیره از طریق یک فرم در سایتی جعلی فریب دهد که این اجازه را به مجرم می‌دهد با استفاده از این اطلاعات پول به دست آورد.

فیشرها یا مجرمان فیشینگ از تکنیک‌های متعددی برای فریب دادن کاربران به‌منظور دسترسی به سایت جعلی استفاده می‌کنند. مثلاً، ارسال ایمیل‌هایی که به نظر می‌آید از یک بانک باشد. این ایمیل‌ها اغلب از لوگوهای قانونی و یک سبک تجاری خوب استفاده می‌کنند و سربرگ نامه را به‌گونه‌ای طراحی می‌کنند که شبیه این به نظر برسد که به بانکی قانونی تعلق دارند. به‌طور کلی، این نامه‌ها به دریافت‌کنندگان اطلاع می‌دهند که بانک، زیرساخت IT خود را تغییر داده و از تمامی مشتریان می‌خواهد که اطلاعات

کاربری خود را مجدداً تصدیق کنند هنگامی‌که دریافت‌کننده، روی لینک موجود در ایمیل کلیک می¬کند، به سایتی جعلی هدایت می‌شود که از او می‌خواهد اطلاعات شخصی خود را وارد کند(فضلی،۱۳۸۹:۳۹).

۱-۳.**گروه ویروس‌های کامپیوتری**: دسته ویروس های کامپیوتری (شامل ویروس‌ها، کرم‌ها، نرم‌افزارهای جاسوسی و...) در حقیقت نرم‌افزارهایی هستند که خود را تکثیر و منتشر می کنند و کامپیوترهای موجود در یک شبکه را بدون اطلاع کاربران آلوده کرده و به آن‌ها صدمه می‌زند. ویروس‌ها از طریق پَروَنجاهای سیستم یک شبکه کامپیوتری، اینترنت یا هر وسیله نقل انتقال اطلاعات مانند حافظه فلش، CD و ...وارد کامپیوترهای دیگر می‌شوند. ویروس‌های کامپیوتری کدهایی هستند که با هدف ضربه زدن به یک سیستم رایانه‌ای یا از بین بردن اطلاعات نوشته شده‌اند. نوشتن ویروس کامپیوتری در همه جای دنیا یک جرم است به‌گونه‌ای که نویسنده ویروس در برابر تمام خسارت‌های وارده به همه کامپیوترهای آلوده شده مسئول است (پاکزاد،۱۳۸۰:۴۱).

۱-۴. **سیبراستالکینگ**[1] : عبارت است از استفاده از فناوری ارتباطات به‌خصوص اینترنت برای آزار و اذیت افراد. تهمت، ارسال نرم‌افزارهای مخرب و تخریب اطلاعات و تجهیزات کامپیوتری در این گروه قرار می‌گیرند. این خلاف‌کاران اغلب کاربران را از طریق چت روم‌ها، تالارهای تبادل‌نظر و اجتماعات اینترنتی شکار می‌کنند سپس اطلاعات آن‌ها را به دست می‌آورند (مثلاً شماره تلفن و آدرس، محل کار و ...) و با استفاده از این اطلاعات قربانیان خود را مورد اذیت و آزار قرار می‌دهند. ایمیل‌های تهدیدآمیز، مزاحمت تلفنی و مانند این‌ها انجام می‌دهند و این مورد یکی از جرم‌های رایانه‌ای خطرناک است که در سراسر دنیا مجازات سنگینی برایش قرار می‌گیرد(عالی پور،۱۳۹۰:۲۹).

۱-۵. هویت جعلی: هویت جعلی یا خود را به‌جای کس دیگر جا زدن یکی از جدیدترین کلاه‌برداری‌هایی است که به کمک آن پول‌های زیادی ربوده شده و سودهای کلانی نصیب کلاه‌برداران می‌شود. در این شیوه کلاه‌بردار خود را به‌جای مالک چیزی جا می‌زند. یا از هویت شخص دیگری برای به دست آوردن کالا یا خدمات مورد نیاز خود

[1] Cyber stalking

استفاده می‌کنند. مهاجرت غیر قانونی، تروریسم و ایمیل‌های سیاه در زمره این جرائم قرار می‌گیرد(زندی،۱۳۸۹:۴۰).

انواع مختلف جرائم رایانه‌ای همه در یک چیز مشترک‌اند و آن هم بهره‌برداری غیر قانونی از فناوری جدید رایانه‌ای و ارتباطات برای فعالیت‌های خلاف‌کارانه است. همان‌طور که فناوری جدید راهی برای مقابله ارائه می‌دهد از آن‌سو هم جنایتکاران از آخرین فناوری‌ها سود می‌برند. همیشه یک قدم از سیستم‌های امنیتی جلوتر هستند؛ و هیچ راهی امن‌تر از احتیاط نیست پس مراقب ایمیل‌های ناشناس، چت روم‌ها، حافظه‌های فلش، وب‌سایت‌های مشکوک و... باشید و سعی کنید اطلاعات بیشتری درباره امنیت در اینترنت پیدا کنید.

۲. تقسیم‌بندی جرائم سایبری

۲-۱.جرائم کلاسیک با توصیف سایبری: جرائمی در این دسته قرار می‌گیرند که جرائم سنتی تلقی می‌شوند؛ اما در حال حاضر به علت پیشرفت فناوری، با وسایل نوینی انجام می‌شوند. ازجمله این جرائم می‌توان به کلاهبرداری سایبری، جعل سایبری، تخریب سایبری، جاسوسی سایبری و ... اشاره نمود(راجی،۱۳۸۵:۳۰).

۲-۲.جرائم علیه محرمانه بودن داده‌ها و سیستم ها: هر نمادی از موضوع‌ها، مفاهیم یا دستورالعمل‌ها ازجمله متن، صوت یا تصویر را که برای برقراری ارتباط میان سیستم‌های رایانه‌ای با پردازش توسط شخص یا سیستم رایانه‌ای به کار گرفته شده و به‌وسیله سیستم رایانه‌ای ایجاد می‌گردد، داده محتوا گویند. ازجمله جرائمی که در این دسته جای می گیرند می‌توان به شنود غیرمجاز داده‌های مخابراتی در یک ارتباط خصوصی یا داده‌های سری که واجد ارزش برای امنیت داخلی و خارجی کشور می‌باشند، اشاره کرد(پرویزی،۱۳۸۴:۲۱).

۲-۳. جرائم علیه صحت و تمامیت داده‌ها و سیستم ها: تغییر، ایجاد، محو یا متوقف کردن رایانه‌ای و مخابراتی به‌قصد تقلب، غیر قابل‌استفاده کردن، تخریب یا اختلال در داده‌ها یا امواج الکترومغناطیسی، ممانعت از دستیابی اشخاص مجاز به داده‌ها با تغییر رمز ورود و یا رمزنگاری ازجمله جرائمی هستند که در این دسته قرار می‌گیرند.

۲-۴. جرائم مرتبط با محتوا: این دسته جرائمی را تحت شمول خود قرار می‌دهد که در آن‌ها، رایانه به‌عنوان ابزار و وسیله توسط مجرم برای ارتکاب جرم به کار گرفته می‌شود و صرفاً فناوری اطلاعات، زمینه ارتکاب آن‌ها را فراهم می‌سازد. برای مثال انتشار محتویات مستهجن از قبیل نمایش اندام جنسی زن و مرد یا نمایش آمیزش جنسی انسان، تبلیغ یا تحریک یا تشویق به انحرافات جنسی یا خودکشی از طریق سیستم رایانه‌ای یا مخابراتی در این دسته قرار می‌گیرند.

۳. ویژگی های جرایم رایانه ای

۳-۱. تنوع مرتکبان و گستردگی حجم خسارات حاصله: امروزه فضای مجازی و اینترنت به‌عنوان یک فضای کسب‌وکار و تجارت تبدیل شده است؛ و بیشتر در معرض عموم قرار گرفته است؛ بنابراین جرائم زیادی در این فضا به وقوع می‌پیوندد. تا چندی پیش به لحاظ محدودیت دسترسی افراد جامعه جهانی به اینترنت، مرتکبان محدود و از طیف خاصی بودند؛ مثل کارمندان ناراضی شرکت های تجاری و امثال آن‌ها که به امکانات رایانه‌ای دسترسی داشتند؛ اما امروزه افراد از طیف‌های مختلف حرفه‌ای یا غیرحرفه‌ای، سازمان یافته یا غیر سازمان یافته و نوجوان یا پیر به ارتکاب این جرائم دست می یازند. به‌عنوان مثال در کشورمان در غالب مغازه‌های فروش نرم‌افزار، ابزار ارتکاب جرائم رایانه‌ای مانند برنامه‌های رایانه‌ای مخصوص نفوذگری با آموزش فارسی در بسته‌بندی‌های رنگی و از طرف شرکت های رسمی ارائه می‌شوند و یک نفر با کمترین اطلاعات رایانه‌ای می‌تواند یک پایگاه اینترنتی را هک کند (زندی،۱۳۸۹:۳۵).

از آنجا که محدودیت های دنیای مادی در مورد این جرائم وجود ندارد و داده‌هایی که ارزش اقتصادی فراوانی دارند در یک حجم کم نگهداری می‌شوند، لذا میزان خسارت آن‌ها نسبت به جرائم کلاسیک بسیار گسترده‌تر است. برای دستبرد زدن الکترونیکی به یک بانک نه سلاح لازم است و نه یک گروه سازمان یافته؛ بلکه یک نفر می‌تواند با نفوذ به سیستم یک بانک میلیاردها دلار پول الکترونیکی را به‌حساب خود یا دیگری انتقال دهد. این عدم محدودیت مادی در کنار گسترش نقش رایانه ها به‌عنوان جزء لاینفک فعالیت روزانه شرکت‌ها و بنگاه های تجاری، سبب می گردد که با وقوع برخی جرائم حتی شرکت های بزرگ به ورطه نابودی و ورشکستگی سقوط کنند(فضلی،۱۳۸۹:۶۴).

در جرائم محیط سایبر، اولاً تعداد بزه دیدگان معمولاً بسیار بالاست و شاید از مرز هزاران و میلیونها نفر هم فراتر رود، ثانیاً معمولاً نمی‌توان آمار دقیقی از تعداد بزه دیدگان داشت، چه، جرائم سایبری در شبکه شیوع می‌یابند و حالت اشاعه جرم ارتکابی که در بسیاری موارد به‌صورت خودکار صورت می گیرد، بسیاری از سیستم های رایانه‌ای و اطلاعات را درگیر خود می‌سازد و این امر قابل شمارش نیست. در واقع، این طبیعت فضای تکنولوژیک فضای سایبری است که موجد پیدایش جرائمی خودکار شده است که مرتکب فقط در قدم اول تحقق جرم نقش دارد و نه در استمرار آن؛ به عبارت دیگر در ارتکاب این جرائم مرتکب آغازگر است، اما شاید هیچ‌گاه ادامه‌دهنده نباشد و این امر جرائم مستمری را آفریده است که فاعل آن در استمرارش نقشی ندارد؛ بنابراین نرخ ارتکاب جرم هم بالاست و در یک لحظه از زمان به میزان بسیار زیادی ممکن است واقع شود. برای نمونه ممکن است بتوان هزاران سند و اطلاعات رایانه ای را در لحظه‌ای از زمان جعل کرد یا به‌صورت غیرمجاز کپی و تکثیر کرد. ازاین‌رو ارتکاب جرائم جمعی در محیط سایبر یک ویژگی نسبتاً معمول است(زندی،۱۳۸۹:۴۰).

۳-۲. سرعت بالای ارتکاب جرم و قابلیت تکرار فراوان: ارتکاب جرم در محیط سایبر کاری بسیار راحت است؛ هر کس با داشتن یک رایانه که امکان اتصال به اینترنت را دارد و اندک آشنایی به سواد رایانه ای می‌تواند مجرمی بالقوه خطرناک باشد؛ صد البته میزان آشنایی بیشتر به علوم رایانه‌ای مرتکب جرم را حرفه‌ای‌تر می‌نماید و بر درجات شدت ارتکاب جرم می‌افزاید. علاوه بر موارد بالا، محدودیت در ارتکاب جرائم در محیط واقعی به‌مراتب بیشتر از محدودیت در محیط سایبر است(دزبانی،۱۳۸۶:۳۰).

۳-۳.شکل ارتکاب جرائم ناشی از فن‌آوری مدرن: حقوق شکلی را باید اصلی‌ترین قربانی جرائم سایبری دانست، چراکه به‌واسطه این جرائم به‌شدت تحت تأثیر قرار گرفته و به بن‌بست رسیده است (دزبانی،۱۳۸۶:۲۲). تحقیق، تعقیب و کشف جرائم رایانه ای در محیط سایبر بسیار دشوار است. روش های تکنولوژیک و فناوری های نوین این امکان را به مجرمین میدهند که آثار جرائم خود را استتار کنند، به‌طوری‌که راهکارهای جدیدی برای نهان‌سازی جرائم رایانه‌ای در این فضا ایجاد شده‌اند که این امکان را به مجرمین می دهند تا از طریق روشهایی چون رمزنگاری در ظاهری قانونی مرتکب جرم شوند. ارتکاب جرم در فضای سایبر راحت‌تر است و امکان دستگیری مجرمین نیز کمتر است. مشکلات

شکلی مرحله تحقیقات مقدماتی در کشف جرائم رایانه‌ای به همین بسنده نمی‌شود؛ در بسیاری از موارد حتی پس از کشف جرم، مجرم کیلومترها دور از دسترس مقامات اجرای قانون و مقامات قضایی است و امکان تعقیب و تحقیق از او وجود ندارد. هنوز همکاری‌های بین‌المللی نیز بدان سطح نرسیده است که برای مبارزه با این جرائم راهکاری قوی و هماهنگ ایجاد شود. حتی سندی بین‌المللی نیز وجود ندارد که به این جرائم جنبه جهانی بخشیده باشد به‌طوری‌که مجرم در هر نقطه ای از جهان که یافت شد بر اساس قوانین بین‌المللی مورد رسیدگی و مجازات قرار گیرد(فضلی،۱۳۸۹:۷۱).

۳-۴. زمان و مکان ارتکاب جرم: یکی از مباحث مهم در حقوق جزای کیفیات مشدده و مخففه می‌باشد که در تعیین مجازات نقش بسزایی دارند. ازجمله عوامل مؤثر در این کیفیات زمان و مکان ارتکاب جرم است که گاهی همانند سال قحطی، در جرم سرقت مستوجب حد، سبب تخفیف شده و گاهی همانند سرقت در شب، سبب تشدید مجازات می‌شوند بنابراین زمان و مکان ارتکاب جرم از مسائل اساسی حقوق جزای است. جرائم سنتی همواره در بعد مکان و زمان قرار دارند؛ یعنی بزهکار باید جرم خود را در زمان مشخص و مکان مشخص مرتکب شود. به همین دلیل، ارتکاب جرائم سنتی عموماً با کندی پیش می‌رود. در مقابل، ساختار جرائم سایبری به نحوی است که در آن‌ها بعد مکان و زمان چندان جایگاهی ندارد. فضای سایبری به نحو شگرفی موجب صرفه‌جویی در هزینه‌های زمانی ارتکاب جرائم سایبر شده است. برای نقض حریم خصوصی افراد در دنیای واقعی، یک مجرم کار بسیار سختی را پیش روی دارد اما در محیط مجازی، کار بسیار آسان است. درگذشته که فناوری اطلاعات و ارتباطات پیشرفت زیادی نکرده بود جرم در زمان و مکان خاصی اتفاق می‌افتاد؛ اما امروز باوجود فضای سایبری مکان و زمان در ارتکاب جرم بسیار پیچیده شده است. از یک‌جهت دستیابی به زمان و مکان ارتکاب جرم آسان شده است از طرفی دیگر به دلیل افزایش مرتکبین جرم دستیابی و پیگیری آنان دشوار شده است(دزبانی،۱۳۸۶:۳۹).

۳-۵. سهولت از بین بردن آثار وقوع جرم و بالا بودن رقم سیاه: در حال حاضر به دلیل پیشرفت‌هایی که در زمینه فناوری اطلاعات و ارتباطات اتفاق افتاده است. میزان وقوع جرم در این نوع فضا هم افزایش یافته است؛ و به رقم سیاهی رسیده است. کسانی که در این حوزه‌ها مرتکب جرم میشوند؛ دارای تخصص بالاتری بوده و از دانش کافی

برخوردارند؛ لذا هنگام ارتکاب اعمال مجرمانه کوشش و اقدام به حذف رد پاهای خود در محیط سایبری می‌کنند(حسینی،۱۳۸۶:۳۹). هرچند با تکیه بر بعضی فناوری‌های جدید می‌توان اطلاعات را دوباره به دست آورد اما همین مهارت آن‌ها باعث وقفه در عملیات‌های بازرسی و پیگیری تیم‌های متخصص میگردد. نکتهٔ دیگری که در این جرائم از اهمیت بالایی برخوردار می‌باشد، حیثیت و وجهه‌ای می‌باشد که افراد یا شرکت‌های معتبر و بانک‌ها با آن روبرو هستند که در اکثر جرائم به دلیل حفظ جایگاه و جلوگیری از تشویش اذهان مشتریان خود، اقدام به گزارش این گونه جرائم نمی‌کنند که همین دلیل منجر به بالا رفتن رقم سیاه جرائم و عدم وجود آمارهای جنایی دقیق و در نهایت عدم برخورد مناسب از لحاظ قضایی با این گونه از بزهکاران هستیم.

۴. نحوه تعقیب و رسیدگی به جرائم رایانه‌ای در فضای سایبری

حجم گسترده اطلاعات مبادله شده در فضای سایبری، متخصصین علم حقوق را بر آن داشته تا نسبت به تدوین وتهیه حقوق فضای مجازی اقدام نمایند. درگذشته ای نه چندان دور رسیدگی به جرائم فضای مجازی با قانون سنتی صورت می گرفت اما با تدوین قانون جرائم رایانه‌ای که درانتهای قانون مجازات اسلامی جدید افزوده شده است. رسیدگی به حقوق فضای مجازی وجرایم سایبری وارد فاز جدید خود شد و به‌عنوان یکی از قوانین تخصصی مورد توجه قرارگرفت. استفاده کننده از فضای مجازی به‌عنوان کاربر وعضو این جامعه که به سان فضای واقعی در زندگی مردم تاثیر زیادی دارد، از حقوقی برخوردار است که این حقوق در همه کشورها مورد حمایت قانون قرارگرفت. قانون جرائم رایانه‌ای، قانون مجازات اشخاصی که فعالیت غیرمجاز سمعی بصری می نمایند، قانون حمایت از پدیدآورندگان نرم‌افزارهای رایانه‌ای، قانون مالکیت معنوی، قانون تجارت الکترونیکی، قانون انتخابات مجلس شورای اسلامی، آیین نامه اجرایی قانون انتخابات مجلس خبرگان رهبری، قانون انتخابات ریاست جمهوری، قانون مجازات اسلامی، قانون مطبوعات وقانون جامع مبارزه با مواد مخدر، ازجمله قوانین مرتبط با حقوق فضای مجازی و جرائم سایبری می‌باشد که در دادسرای جرائم رایانه‌ای تعقیب می‌شود. تقریبا تمامی جرائمی که در فضای حقیقی قابل تحقق و ارتکاب هستند به‌عنوان جرائم سایبری در فضای مجازی هم قابل تحقق هستند؛ اما مسوولیت جبران خسارت زیان‌دیده در فضای

مجازی یکی از مهم‌ترین مباحث حقوق فضای مجازی است که شاید بتوان آن را در صلاحیت اولیه دادسرای جرائم رایانه‌ای قرارداد(حسن بیگی،۱۳۸۹:۳۲). جرائمی که در فضای رایانه های تحقق می‌یابد از قبیل کلاهبرداری رایانه‌ای، تهدید و مزاحمت، انتشار تصاویر و فیلم‌های مستهجن و پورن در فضای مجازی، تشویق و ترغیب به فساد و فحشا، استفاده ابزاری از اندام یا تصاویر زنان جهت فروش کالا یا خدمات، راه اندازی مراکز همسریابی یا صیغه و ازدواج موقت بدون اخذ مجوز از وزارت ورزش و جوانان، توهین به مقدسات مذهبی و مقامات دولتی، ترویج بی‌دینی و تبلیغ ادیان ضاله، تحریک مردم به شورش، تهدید به بمب‌گذاری یا انجام عملیات تروریستی، دسترسی غیرمجاز به داده‌ها، تخریب داده‌ها یا به‌اصطلاح هک داده‌ها، تشکیل باندهای قماربازی تهیه و توزیع مشروبات الکلی و به‌طور کلی همه جرائم که در کارگروه تعیین مصادیق مجرمانه شورای عالی فضای مجازی، بر اساس قانون‌های ذکر شده در بالا به‌عنوان جرائم سایبری و جرائم رایانه ای تعیین شده است، ازجمله مصادیق جرائم سایبری هستند که رسیدگی به آن‌ها در صلاحیت دادسرای جرائم رایانه ای قرار دارد. بعضی از انواع جرائم سایبری و جرایم رایانه‌ای، طبق حقوق فضای مجازی و قانون آیین دادرسی بدون طرح شکایت از سوی شاکی خصوصی قابل‌رسیدگی نیستند؛ و نیاز به اعلام شکایت شاکی خصوصی دارد ولی بعضی از جرائم که جنبه عمومی داشته و به نحوی از انحا کشف شود قابل‌رسیدگی در دادسرای جرائم رایانه‌ای بنا به ارجاع دادستان می‌باشد و نیاز به اعلام شکایت شاکی خصوصی ندارد. هرگونه جرمی که در فضای مجازی به وقوع بپیوندد در صلاحیت دادسرای تخصصی جرائم رایانه‌ای قابل‌پیگیری است.

۵. واکنش تقنینی کشورها در خصوص جرائم رایانه‌ای

پیشرفت فناوری های ارتباطی و اطلاعاتی و به‌تبع آن توسعه فضای مجازی باوجود دستاوردها و کارکردهای فوق‌العاده در زمینه‌های اجتماعی، فرهنگی، اقتصادی و سیاسی به آسیب‌ها و مشکلاتی نیز دامن زده است. سوءاستفاده از این فضا برای جرم و بزهکاری، از آن جمله است. در مواجهه با این نوع از جرائم سایبری که گاه جنبه فراملی و بین‌المللی نیز به خود می‌گیرد، دولت‌ها و سازمان‌های بین‌المللی از دهه ۷۰ به بعد با تدوین و قوانین و قواعد حقوقی جدید به مبارزه برخواسته‌اند. تا دهه ی ۱۹۷۰ میلادی

کشورهای مختلف در چارچوب قوانین سنتی با جرائم سایبر برخورد می‌کردند؛ اما پیشرفت فناوری اطلاعات، تنوع و کثرت سوءاستفاده‌هایی که از این فناوری به عمل آمد، حقوق جزای سنتی کشورها را به چالش کشید.

یکی از علل به چالش کشیده شدن حقوق جزای سنتی این بود که قوانین کیفری کشورها تا قبل از شیوع جرائم سایبری غالباً به حمایت از اهداف و موضوعات ملموس می پرداختند. با رشد فناوری رایانه، اطلاعات و داده‌های رایانه‌ای به‌عنوان یک موضوع غیرملموس، غیر قابل‌رؤیت و باارزش، موضوع جرم سایبری قرار گرفت. حقوق جزای ماهوی که حمایت از ارزش¬ها را بر عهده دارد در برابر تجاوز و تعدی به این ارزش ها با نگرشی جدید واکنش نشان داد. این نگرش طی مراحلی موجب اصلاح سیستم‌های قضایی شد. پروفسور زیبر آلمانی (پدر حقوق کیفری اطلاعات) به پنج مرحله از این مراحل به ترتیب زیر اشاره کرده است: اولین مرحله، اصلاح سیستم‌های قضایی غرب بود که در حمایت از محرمانگی (حقوق خصوصی و فردی) در دهه‌های ۱۹۷۰ و ۱۹۸۰ ظاهر شد. این تقنین، واکنشی در برابر چالش‌های جدید مربوط به حقوق خصوصی و فردی بود که به‌واسطه‌ی امکانات جمع‌آوری، ذخیره‌سازی و انتقال داده‌ها از طریق تکنولوژی جدید با مسائل جدید مواجه شده بود. لذا قوانینِ جدیدِ حمایت از داده‌ها، در حمایت از حقوق خصوصی و فردی شهروندان از جنبه‌ی اداری، مدنی و کیفری در کشورهای مختلف تصویب شد. قوانین کانادا و استرالیا در سال ۱۹۷۲، سوئد ۱۹۷۳، آمریکا ۱۹۷۴، آلمان ۱۹۷۷، فرانسه، نروژ، اتریش و دانمارک ۱۹۸۸، ایسلند ۱۹۸۱، بریتانیا ۱۹۸۴، ایرلند، ژاپن و هلند ۱۹۸۸ تصویب شده‌اند و بعضاً این قوانین جدید مورد اصلاح قرار گرفته‌اند(شیرزاد،۱۳۸۸:۴۴).

مرحله ی دوم از موج قوانین اصلاحی ناظر بر جرائم اقتصادی مرتبط با رایانه در اواخر دهه‌ی ۱۹۷۰ و دهه ی ۱۹۸۰ است. آمریکا درسال ۱۹۷۶ (در سطح ایالات)، ایتالیا ۱۹۷۸، استرالیا ۱۹۷۹، بریتانیا ۱۹۸۱، آمریکا ۱۹۸۴ (در سطح فدرال)، دانمارک وکانادا ۱۹۸۵، آلمان ۱۹۸۶، سوئد و شیلی ۱۹۸۷، اتریش، ژاپن و نروژ ۱۹۸۷، فرانسه و یونان ۱۹۸۸، فنلاند و بریتانیا ۱۹۹۰ قوانینی در خصوص جرائم رایانه‌ای اقتصادی وضع کرده‌اند که بعضی از این قوانین چند بار اصلاح شده‌اند.

مرحله‌ی سوم قوانین اصلاحی در دهه‌ی ۱۹۸۰ ناظر بر جرائم مالکیت معنوی مرتبط با رایانه است. بعد از اینکه برنامه‌های رایانه‌ای در دهه‌ی ۱۹۷۰ تحت حمایت حق اختراع قرار گرفت، قوانین اصلاحی برنامه‌های رایانه‌ای را مشمول کپی‌رایت (مالکیت معنوی) قرار دادند. کشور آمریکا در سال ۱۹۸۰، مجارستان ۱۹۸۳، استرالیا، هند و مکزیک ۱۹۸۴، شیلی، آلمان، فرانسه، ژاپن و انگلستان در ۱۹۸۵، برزیل، کانادا و اسپانیا در ۱۹۸۸، دانمارک، کلمبیا و سوئد ۱۹۹۰ و نروژ در ۱۹۹۱ قوانین مربوط به مالکیت معنوی (کپی رایت) خود را اصلاح کرده‌اند و پیشرفت‌های کلی در زمینه‌ی حمایت جزایی از مالکیت معنوی نیز حاصل شده است.

مرحله ی چهارم اصلاحات بین‌المللی قوانین، در مورد قوانین آئین‌دادرسی است. بسیاری از کشورها مانند آمریکا، کانادا، آلمان و دیگر کشورهای اروپایی قوانینی را در خصوص تفتیش و توقیف داده‌های رایانه‌ای وضع کرده‌اند. در این خصوص می‌توان به تدوین قوانین انگلیس در سال ۱۹۸۴، دانمارک ۱۹۸۵، آمریکا ۱۹۸۶ و هلند ۱۹۹۴ اشاره نمود.

مرحله ی پنجم اصلاح قوانین، در مورد جرائم مربوط به محتواست. به‌عنوان مثال بسیاری از کشورها قوانینی وضع کردند که تهیه، توزیع، عرضه و نگهداری پورنوگرافی (هرزه‌نگاری) کودکان از طریق سیستم‌ها و شبکه‌های رایانه‌ای را جرم تلقی کرده است(پرویزی،۱۳۸۴:۶۰).

در سال ۲۰۰۰ موسسه ی بین‌المللی مک کانل مطالعه‌ای در مورد وضعیت قوانین وضع شده در ارتباط با جرائم سایبری در چهار گوشه‌ی جهان به عمل آورده است. این موسسه از کشورها خواسته است که چنانچه قوانین و یا پیش‌نویس قوانینی در این خصوص دارند ارسال کنند، در غیر این صورت اعلام نمایند که هیچ اقدام مثبتی انجام نداده‌اند. سی و سه کشور (از بین بیش از ۵۰ کشور) مورد بررسی تا آن تاریخ نسبت به‌روز آمد کردن قوانین خود به‌منظور برخورد با انواع جرائم رایانه‌ای هیچ اقدامی انجام نداده بودند ولی اکثراً در حال تهیه‌ی پیش‌نویس قوانین بودند. این کشورها عبارت‌اند از: ایران، آلبانی، بلغارستان، بورندی، کوبا، دومینیکن، مصر، اتیوپی، فیجی، گامبیا، مجارستان، اردن، نیکاراگوئه، قزاقستان، لیتوانی، لبنان، لسوتر، مالت، مولداوی، مراکش، زلاندنو، نیجریه، رومانی، آفریقای جنوبی، ویتنام، یوگسلاوی، زامبیا، زیمبابوه. ده کشور از

کشورهای مورد بررسی برای برخورد با حداکثر پنج نوع از جرائم سایبری، قانون وضع کرده‌اند که عبارت‌اند از: برزیل، کانادا، شیلی، چین، چک، دانمارک، مالزی، لهستان، اسپانیا و فرانسه. نه کشور نیز برای برخورد با بیش از شش نوع از انواع جرم سایبری، قانون وضع کرده‌اند که عبارت‌اند از: آمریکا، انگلیس، ترکیه، پرو، ژاپن، موریس، استونی، استرالیا و هند. کشور فیلیپین برای اکثر جرائم سایبری قانون وضع کرده است.

از نیمه‌ی دوم دهه‌ی ۱۳۷۰ شمسی و بالأخص از ابتدای دهه‌ی ۱۳۸۰ که استفاده از رایانه‌های شخصی توسط سازمان-های اداری، مؤسسات خصوصی و افراد حقیقی در ایران گسترش یافته و دسترسی به خدمات متعدد اینترنت امکان‌پذیر شده، ارتکاب جرائم سایبری در کشورمان نیز از رشد نسبتاً سریعی برخوردار بوده است. اشاعه‌ی فحشا و منکرات، انتشار عکس‌ها، تصاویر و مطالب خلاف عفت عمومی، ایجاد اختلاف بین اقشار جامعه از طریق طرح مسائل قومی و نژادی، انتشار مطالب نژاد پرستانه، انتشار اسناد و مسائل محرمانه، اهانت به مقدسات مذهبی و دینی، اهانت و افترا نسبت به مقامات دولتی، اشخاص حقیقی و حقوقی، سرقت ادبی و غیره ازجمله جرائمی هستند که بعد از فراهم شدن امکان استفاده از خدمات اینترنت از طریق وب‌سایت ها و وبلاگ ها، پست الکترونیک، گروه‌های خبری، چت (گپ زدن) و سایر سرویس های اینترنت به وقوع پیوسته اند. قانون‌گذار در سال ۱۳۷۹ در برابر برخی از جرائم سایبری واکنش نشان داده و با الحاق تبصره ی ۳ به ماده‌ی ۱ قانون مطبوعات مقرر داشته کلیه‌ی نشریات الکترونیکی مشمول مواد این قانون است.

اولین واکنش قانونی ایران در برابر بعضی از جرائم سایبری، قانون اصلاح قانون مطبوعات مصوب ۱۳۷۹/۱/۳۰ مجلس شورای اسلامی می‌باشد که در تاریخ ۱۳۷۹/۲/۷ مورد تائید شورای نگهبان قرار گرفته است. دومین واکنش قانونی کشور ما در مقابل این نوع جرائم، از طریق وضع «قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای» به عمل آمد. این قانون در تاریخ ۱۳۷۹/۱۰/۴ به تصویب مجلس شورای اسلامی رسید. ماده ی ۱۳ قانون مذکور نقض حقوق پدیدآورندگان آن دسته از نرم‌افزارهای رایانه‌ای را که مورد حمایت این قانون قرار گرفته‌اند، جرم تلقی و برای آن مجازاتی معادل ۹۱ روز تا شش ماه حبس و جزای نقدی تعیین کرده است. سومین عکس‌العمل قانون‌گذار ایران در مقابل جرائم سایبری در سال ۱۳۸۲ از طریق تصویب قانون مجازات جرائم نیروهای

مسلح مصوب ۱۳۸۲/۱۰/۹ مجلس شورای اسلامی به عمل آمد. به‌موجب ماده ی ۱۳۱ این قانون، جعل اطلاعات و داده‌های رایانه‌ای، تسلیم و افشاء غیرمجاز اطلاعات و داده‌ها به افرادی که صلاحیت دسترسی به آن را ندارند، سرقت و یا تخریب حامل‌های داده و سوءاستفاده‌ی مالی از طریق رایانه (کلاهبرداری و اختلاس) توسط نظامیان، جرم تلقی و مرتکب حسب مورد به مجازات جرم ارتکابی محکوم می‌شود (جلالی فراهانی،۴۴:۱۳۸۹).

چهارمین واکنش قانونی مرتبط با جرائم سایبری از طریق تصویب قانون تجارت الکترونیکی مصوب ۱۳۸۲/۱۰/۱۷ مجلس شورای اسلامی به عمل آمده است. به‌موجب مواد ۷۷، ۷۶، ۷۵، ۷۴، ۶۶،۶۷،۶۸،۶۹ این قانون، کلاهبرداری، جعل، دستیابی و افشاء غیرمجاز اسرار تجاری، نقض حقوق مربوط به مالکیت معنوی (کپی‌رایت) و غیره که از طریق رایانه و در بستر تجارت الکترونیکی انجام شود، جرم تلقی و برای آن مجازات تعیین گردیده است. هر یک از چهار قانون فوق‌الذکر در بستر خاص خود قابلیت اعمال دارند. مثلاً قانون مطبوعات صرفاً نسبت به جرائم سایبری ارتکابی در قالب نشریات الکترونیکی، قانون مجازات نیروهای مسلح صرفاً در مورد بعضی از جرائم سایبری نظامیان و قانون تجارت الکترونیکی فقط در مورد برخی از جرائم سایبری ارتکابی در بستر تجارت الکترونیکی قابل اجرا هستند.

برای مقابله با سایر سوءاستفاده‌های سایبری مانند سوءاستفاده از محیط سایبر به‌منظور نفوذ به حریم خصوصی افراد، تخریب، سرقت، توقف و تغییر داده‌هایی که فاقد شرایط مقرر در قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای هستند، سوءاستفاده‌های مالی رایانه‌ای خارج از بستر تجارت الکترونیک و سایر سوءاستفاده‌های رایانه‌ای، نیاز به یک قانون جرائم رایانه‌ای پیشرفته و جامع‌الاطراف است.

شورای عالی توسعه‌ی قضایی قوه‌ی قضائیه، پیش‌نویس قانون جرائم رایانه‌ای و آئین دادرسی آن را در سال ۱۳۸۲ تهیه و طی جلسات متعددی با حضور حقوقدانان و متخصصان امور رایانه مورد بررسی قرار داد تا پس از تصویب رئیس قوه قضائیه به‌عنوان لایحه‌ی جرائم رایانه‌ای از طریق هیئت دولت به مجلس شورای اسلامی تقدیم گردد. با این حال، سرعت تصویب و لازم‌الاجرا شدن قوانین حمایتی رایانه‌ای به‌هیچ‌وجه با توسعه ی کمی و کیفی این فناوری در کشورمان تناسب نداشته است و گام‌های نخستین قانون‌گذاری نیز شامل حوزه‌های محدودی نظیر حمایت از مالکیت فکری رایانه‌ای می

شده که البته آن‌ها نیز تمامی جنبه‌های حمایتی را در برنمی‌گیرند. در همین راستا و با هدف تدوین یک قانون کیفری نسبتاً جامع برای مقابله با سوءاستفاده‌های سایبری، شورای عالی توسعه‌ی قضایی قوه‌ی قضاییه در ابتدای سال ۱۳۸۱ با همکاری شورای عالی اطلاع‌رسانی وقت، طرح تدوین لایحه‌ی مبارزه با جرائم رایانه‌ای را آغاز کرد. پس از آن، پیش‌نویس مذکور تقدیم رئیس وقت قوه‌ی قضاییه شد که در شورای عالی مسئولان قضایی مورد بررسی قرار گرفت و پس از تائید آن از سوی ایشان، تقدیم دولت شد که دولت نیز آن را به مجلس شورای اسلامی تقدیم کرد. در سال ۱۳۸۴، کمیته‌ی تخصصی تشکیل شده در کمیسیون حقوقی و قضایی مجلس شورای اسلامی، متشکل از تعدادی از نمایندگان کمیسیون، لایحه را بررسی و تصویب کردند، لیکن نوبت به طرح لایحه در کمیسیون نرسید و عملاً بررسی آن به دوره‌ی هشتم مجلس شورای اسلامی موکول شد. در شهریورماه ۱۳۸۷ کمیسیون حقوقی و قضایی مجلس به‌طورجدی لایحه را بررسی و تصویب کرد و جهت تصویب نهایی به صحن علنی مجلس ارجاع داد که تا پایان آن سال ادامه یافت و پس از یک‌بار ارجاع به شورای نگهبان و رفع ایرادهای مبتنی بر شرع و قانون اساسی وارده از سوی آن شورا، نهایتاً در تیرماه سال ۱۳۸۸ جهت دولت از سوی مجلس شورای اسلامی ابلاغ شد. این قانون مصوب، مشتمل بر ۳ بخش اصلی می‌باشد که به ترتیب به جرائم و مجازات‌ها، آئین دادرسی و سایر مقررات، اختصاص یافته است(فضلی،۱۳۸۹:۲۸).

۶. فعالیت‌های سازمان‌های منطقه‌ای و بین‌المللی در خصوص جرائم رایانه‌ای

به لحاظ خصیصه‌ی فراملی جرائم سایبری، اقدامات بین‌المللی فراوانی برای دستیابی به سیاست جنایی بین‌المللی ناظر بر این جرائم انجام شده است. فعالیت‌های بین‌المللی برای مبارزه با جرائم سایبری از دهه ی ۱۹۸۰ شروع شد. سازمان‌هایی مانند سازمان همکاری و توسعه‌ی اقتصادی، انجمن بین‌المللی حقوق جزا، سازمان ملل متحد، اینترپل، شورای اروپا و مجمع کشورهای شرکت‌کننده در کنفرانس بین‌المللی مبارزه با جرائم سایبر (۲۰۰۱) بوداپست، اقدامات ارزنده‌ای را در این خصوص انجام داده‌اند (فضلی،۱۳۸۹:۲۲).

۶-۱. اصلاحات قانون در جرائم سایبری: دستاورد این پیمان این است که تغییراتی عملی یا بهتر بگوییم انقلابی در قانون‌گذاری جرائم اینترنتی ایجاد کرده است. شورای اروپا در حدود سال ۲۰۰۶، پروژه‌ای جهانی در مورد جرائم اینترنتی راه اندازی کرد که به‌منظور تقویت ثبات داخلی بر اساس پیمان بوداپست طراحی شده بود. انقلاب قانونی و نهادی در مورد جرائم اینترنتی به حدود ۱۲۰ کشور مختلف توصیه شد. تحت تأثیر این فرایند، مجمع عمومی سازمان ملل متحد، پیمان بوداپست را به‌عنوان پایه‌ای برای توسعه قانون و نهادی برای تحقیق و تعقیب جرائم اینترنتی ذکر کرده است و الحاق به آن را به تمام کشورهای جهان پیشنهاد کرد. سازمان ملل متحد نقش پیشگام در استانداردسازی پیمان بوداپست و مدیریت بهبود آن را بر عهده داشته است(زندی،۱۳۸۹:۲۸).

۶-۲. تشکیل سیستم همکاری مؤثر برای کشورهای منفرد: اگرچه پیمان بوداپست توافقی انجام شده توسط شورای اروپا است، اما امروزه، ۵۵ کشور جهان به آن ملحق شده‌اند. با توجه به اینکه ۱۴ کشور اروپایی هنوز به این پیمان نپیوسته‌اند این معاهده به‌جای یک معاهده منطقه‌ای در اروپا، دارای پتانسیلی است که به یک پیمان جهانی توسعه‌یافته تبدیل شود. مزیت دیگر آن این است که کشورها می‌توانند با الحاق به این معاهده از جرائم اینترنتی پیشگیری کنند. علاوه بر این، دستاورد آن، در ترویج فن‌آوری های کلی در مورد جرائم اینترنتی بین‌المللی به‌طور گسترده‌ای به کشورهای جهان کمک خواهد کرد.

۶-۳. کمک زمینه‌های عمومی در افزایش توانایی واکنش به جرائم سایبری: انقلاب حقوقی و نهادی و همچنین همکاری مؤثر کشورها با یکدیگر باعث تجمیع و انباشته شدن تکنیک‌های قانونی و نهادی در مقابله با جرائم اینترنتی شده است بنابراین، این‌طور به نظر می‌رسد که باید یک تأثیر مثبتی برای آن قائل شد از جهت این چشم‌انداز که می توانند به کشورهای غیر عضو کمک کنند بدین معنی که جلسه‌هایی را بر اساس پیمان بوداپست باهم تشکیل دهند. داشتن نشست‌هایی مانند نشستی که به بوداپست انجامید شبیه یک کاتالیزور تسریع‌کننده برای توسعه فناوری در مدیریت جرائم اینترنتی عمل می کند. همچنین، می‌توان در ماده ۱۵ پیمان بوداپست این اصل را مشاهده کرد و از آن به‌عنوان کتابچه راهنما جهت جلوگیری از جرائم اینترنتی و استفاده مناسب از کامپیوتر

استفاده کرد؛ بنابراین، مشارکت در این پیمان نه‌تنها از حریم خصوصی بلکه از حقوق شخصی نیز حمایت می‌کند(زندی،۱۳۸۹:۲۵).

۶-۴. دیگر دستاوردها: پیمان بوداپست به‌عنوان یک اساسنامه برای افزایش اثربخشی معاهدات موجود در هر کشور عمل می‌کند (به‌ویژه، پیمان همکاری حقوقی متقابل، استرداد برای اجرای مجازات در پیمان و غیره). کمک قضایی برای تحقیق، دستگیری و محاکمه جرائم اینترنتی بر اساس پیمان بوداپست، اثر دیگر معاهدات مشابه را نیز افزایش می‌دهد.

نتیجه گیری

با پیشرفت فناوری اطلاعات و ارتباطات علی رغم تحول و دگرگونی که در زندگی بشر ایجاد می کند باعث بروز آسیب ها و صدماتی را به همراه دارد. اعمال و رفتارهایی که در محیط رایانه ای و مجازی واقع می شود حاصل پیشرفت فناوری اطلاعات و ارتباطات و جایگزین محیط سنتی و فیزیکی است. در این محیط هم مانند محیط سنتی تمامی رفتارهای انسانی سالم نیستند بلکه چه بسا تخطی از هنجارهای اخلاقی و یا تعریف شده از آن وجود دارد.و لذا موجبات قربانی شدن و عبارتی بزه دیده شدن اشخاص در محیط رایانه ای را فراهم می کند. محیط رایانه ای هم مانند محیط سنتی می تواند با توجه به ماهیت آن بزه دیدگان خاص خودش را داشته باشد که لازم است همانند محیط سنتی مورد حمایت قوانین ویژه ای قرار گیرد. جرم رایانه ای عبارت از جرایمی است که در فضای مجازی (اینترنتی) رخ میدهد. و در تعریف گسترده هر فعل یا ترک فعلی که در و یا از طریق یا به کمک رایانه یا از طریق اتصال به اینترنت، چه به طور مستقیم یا غیرمستقیم رخ می دهد و توسط قانون ممنوع گردیده و برای آن مجازات در نظر گرفته شده است. در بیشتر کشورها جرایم رایانه ای بعنوان یک موضوع جدی مطرح است و کشورها با تصویب قوانینی متناسب با نوع جرایم در پیشگیری از آن تدابیر لازم را اندیشیده اند. برسی قوانین کیفری ایران پیرامون جرایم رایانه ای متأسفانه در ایران موضوع تخلفات و جرایم کامپیوتری دیرتر از کشورهای دیگر نمودار گردیده و شاید علت آن ناشناخته بودن فن آوری اطلاغات در ایران بوده است.

منابع :

- پاکزاد، بتول،(۱۳۸۰)،*جرایم رایانه*، پایان‌نامه کارشناسی ارشد، دانشگاه شهید بهشتی.
- پرویزی، رضا؛(۱۳۸۴)، *پی‌جویی جرایم رایانه‌ای* ، تهران، انتشارات جهان جام جم، (شماره ۴۶)،چاپ اول.
- جلالی فراهانی، امیر حسین،(۱۳۸۹)،*درآمدی بر آیین دادرسی کیفری جرایم سایبری* ، تهران،انتشارات خرسندی.
- حسینی، بیژن،(۱۳۸۶)،*جرائم اینترنتی علیه اطفال و زمینه‌های جرم‌شناسی آن*، پایان‌نامه مقطع کارشناسی ارشد، دانشگاه آزاد اسلامی، واحد علوم تحقیقات.
- حسن بیگی، ابراهیم،(۱۳۸۹)، *آسیب‌شناسی شبکه جهانی اطلاع‌رسانی اینترنت و ارائه راهبردهای مناسب جهت مقابله با تهدیدها از دیدگاه امنیت ملی با تاکید بر جنبه‌های حقوقی و فنی*، پایان‌نامه دکتری، دانشگاه عالی دفاع ملی
- دزبانی، محمد حسن،(۱۳۸۶)،*جرائم کامپیوتری* ، تهران، دبیرخانه شورای عالی انفورماتیک ، جلد اول.
- دیویدچی، آیکاو ،(۱۳۹۰)،*«راهکارهای پیشگیری و مقابله با جرایم رایانهای»*، ترجمه: اکبر استرکی و دیگران، تهران،انتشارات دانشگاه علوم انتظامی ناجا، چاپ اول.
- راجی، سید محمد هادی؛(۱۳۸۵)، *نگاهی به قانون تجارت الکترونیک*، فصلنامه نشریه حقوقی گواه،(شماره ۶و۷) بهار و تابستان.
- زندی، محمدرضا،(۱۳۸۹)،*تحقیقات مقدماتی در جرائم سایبری*، تهران،انتشارات جنگل، چاپ اول.
- شیرزاد، کامران،(۱۳۸۸)،*جرایم رایانه‌ای از دیدگاه حقوق جزای ایران و بین‌الملل*، تهران ، نشر بهینه فراگیر ، چاپ اول.
- فضلی، مهدی،(۱۳۸۹)،*مسئولیت کیفری در فضای سایبر*، تهران،انتشارات خرسندی، چاپ اول،
- عالی پور، حسن،(۱۳۹۰)،*حقوق کیفری فناوری اطلاعات (جرایم رایانه‌ای)*، تهران،انتشارات خرسندی، چاپ اول.
- عمیدی، مهدی،(۱۳۸۷)،*مطالعه تطبیقی جرایم رایانه‌ای از دیدگاه فقه و حقوق کیفری ایران*، پایان‌نامه کارشناسی ارشد حقوق جزا و جرم‌شناسی، دانشگاه آزاد اسلامی واحد تهران مرکز.

- معظمی، شهلا،(۱۳۸۹)،*«جرم سازمان یافته و راهکارهـای جهـانی مقابلـه بـا آن»*، تهران، نشر دادگستر چـاپ سوم.
- معتمد نژاد، کاظم،(۱۳۸۳)،*وسایل ارتباط‌جمعی*،جلد نخست، تهران، انتشارات دانشگاه علامه طباطبایی.
- نجفی ابرندآبادی، علی حسین،(۱۳۸۲)،*تقریرات درس جرم‌شناسی (پیشگیری)*، دوره کارشناسی ارشد حقوق کیفری و جرم‌شناسی، تنظیم مهدی سید زاده، نیمسال دوم تحصیلی.