بررسی جرایم رایانه ای در حقوق ایران و بین الملل

احسان پهلوانی فرد[1]، علی امیری پورقصاب[2]

تاریخ دریافت: ۱۳۹۱/۰۲/۰۵

تاریخ پذیرش: ۱۳۹۱/۰٤/۱۰

چکیده

با ظهور رایانه و به تبع آن شبکه های اطلاعاتی و ارتباطی جهانی، یکی از تاثیر گذارترین عناصر بشر بوده است. در کنار این فناوری نوین در میان جوامع سوء استفاده هایی رخ داده که منجر به آسیب های اجتماعی شده است. لذا با توجه به ویژگی فضای جدید، محدودیت هایی همچون مرز، ملیت، مسافت، زمان، مکان و ... معنا ندارد. وقتی در خصوص فناوری بحث می‌شود، نمی‌توان رایانه را نادیده گرفت. رایانه، خود بزرگ ترین فناوری عصر حاضر است و سایر فناوری‌های نوین یا به وسیله آن و یا بر بستر آن شکل می‌گیرند. امروزه همه عرصه های نوین جامعه از تأثیر و مداخله رایانه مصون نیست در جهان حاضر، هر کسی کار با رایانه را آموزش ندیده باشد یک بی سواد نوین است. البته فناوری‌ها در کنار مزایای خود می‌توانند بسترساز سوء استفاده‌هایی نیز باشند. و دامنه خطرهای آن افزایش می‌یابد. این نوشتار در صدد است با توجه به این که حجم مقاله محدود می باشد، به بررسی تطبیقی اجمالی به جرم رایانه ای[3] در حقوق ایران و حقوق بین الملل پرداخته و در پایان، به بیان راه کارهای مناسب در پیشگیری از جرم بپردازد.

واژگان کلیدی: *جرایم رایانه ای، فناوری اطلاعات، قانون جرایم رایانه ای، فضای سایبری.*

---

[1] دانشجوی کارشناسی ارشد حقوق بین الملل واحد دامغان.

[2] فوق دکتری حقوق بین الملل، استادیار دانشگاه آزاد دامغان.

[3] Computer crime

مقدمه

انسان های اولیه برای برقرار کردن ارتباط و انتقال اطلاعات خویش از اشارات و علائمی مثل دود استفاده می کردند و بعدها با اختراع خط، از چوب و پوست حیوانات به ثبت و نگهداری اطلاعات استفاده کردند. به مرور زمان بعد از انقلاب صنعتی، به وجود آمدن انقلاب اطلاعات موجب دگرگونی تمام جنبه های زندگی انسان ها شد در کنار این تحول عظیم ارتباطات، با سوء استفاده های افراد و سازمان های سود جو باعث به وجود آمدن جرایمی در این حوزه گردید. جرایمی که با عنوان جرایم رایانه ای در کشور های مختلف برای حفظ اسرار و اطلاعات شکل گرفت. با پیشرفت تکنولوژی، راه های ارتکاب جرایم علیه تمامیت جسمانی چون قتل و سایر صدمات بدنی و صدمات معنوی مانند افترا و نشر اکاذیب و جرایم بر ضد اموال و مالکیت مانند تخریب وکلاهبرداری و سرقت و جرایم بر ضدّ امنیت و آسایش عمومی از قبیل تروریسم و جعل، بسیار فنی‌تر وظریف‌تر شده و پیشگیری از بروز آنها یا کشف جرم و تعقیب و محاکمه و اعمال حکم محکومیت، به تدریج با دشواری‌های بیشتری مواجه گردیده است. در صورتی که تحصیل مال غیر با استفاده از روش متقلبانه توسط کامپیوتر انجام شود به حکم قانون می‌تواند از جرایم در حکم کلاهبردرای تلقّی شود، زیرا زیاندیده اصولاً، اموال خود را به کلاهبردار تسلیم نمی‌کند بلکه در بیشتر موارد از حساب او سوءاستفاده به عمل آمده و بدهکار می‌شود و یا از حساب مربوط به نحو متقلبانه و برخلاف رضایت و اطلاع ذینفع برداشت می‌شود.

از این دست جرایم متقلبانه به وسیله رایانه که با تکنولوژی برتر همراه است نیازمند شناخت بیشتر این دستاورد می باشد و همچنین آگاهی از نحوه ی کاربرد و عملکرد آن و شیوه های اجرایی و آگاهی روز دنیا می طلبد بتوان با این جرم که بسیار هوشمندانه و پیچیده است مقابله نمود. حقوق کیفری نوین، امروزه با جرایم و مجرمان رایانه‌ای طرف است. ماهیت و ویژگی این

دسته از جرایم به نحوی اساسی با جرایم سنتی تفاوت دارد. امروزه، مجرمان رایانه‌ای در مکان‌هایی به غیر از نقاطی‌که آثار و نتایج اعمال آنها ظاهر می‌شود، قرار دارند. در صورتی‌که کارایی قوانین جزایی موجود و متداول، منحصر به قلمرو خاصی است و به دلیل آنکه اجزای عنصر مادی کاملاً یا بعضاً تغییر یافته و برخی عناوین مجرمانه ی تازه هم به وجود آمده، نمی‌توان مجرمان را با قوانین قبلی محاکمه کرد[1]. پیشرفت تکنولوژی و علم و دست یابی بشر به فناوری اطلاعات و استفاده از رایانه و پیدایش دنیای مجازی دارای پیامدهای مثبت و منفی فراوانی برای بشر بوده است. از جمله پیامدهای منفی آن، پیدایش جرایم رایانه ای بوده است. در مورد جرایم رایانه ای تعاریف متعددی ذکر شده است.

[1] www.imj.ir/index.php?option=com_content&view=article&id=1381:1389-03-01-20-13-38&catid=57:1388-08-19-07-45-26

بیان مساله

سازمان ملل در شماره ۴۳ و ۴۴ نشریه بین المللی سیاست جنایی با یادآوری این نکته که در زمینه جرایم کامپیوتری تعریف مورد توافقی وجود ندارد، جرایم کامپیوتری را از یک طرف شامل فعالیت مجرمانه با اهمیت سنتی مثل سرقت و جعل دانسته که به طور معمول این جرایم در تمام کشورها دارای ضمانت اجرای کیفری هستند و از سوی دیگر، شامل فعالیت های مجرمانه جدیدی دانسته که پیش از این ممکن نبوده، بلکه کامپیوتر امکان این گونه سوء استفاده ها را مهیا ساخته است.

در واقع سازمان ملل به نوعی از طبقه بندی جرایم کامپیوتری اشاره دارد، نه به تعریف جرم کامپیوتری. پروفسور شیک یکی از حقوقدانان اطریشی در تعریف جرم رایانه ای بیان می کند: جرم رایانه ای به هر عمل مجرمانه ای گفته می شود که در آن رایانه، وسیله یا هدف ارتکاب جرم باشد.[۱] در ایالات متحده آمریکا تعریف وسیعی از جرم رایانه‌ای به عمل آمده مبنی بر آنکه: هر اقدام غیرقانونی که با یک رایانه یا به کارگیری آن مرتبط باشد جرم رایانه‌ای می‌گویند. یا هر اقدامی‌که به هر ترتیب با رایانه مرتبط بوده و موجب ایجاد خسارت به بزه دیده شود و مرتکب از این طریق منافعی را تحصیل کند، جرم محسوب می‌شود.[۲]

روش تحقیق

روش تحقیق به صورت نظری و کتابخانه ای بوده و برای تطبیق مطالب از کتب مختلف و تحقیقات بنیادین گذشتگان و ترجمه متون و کتاب های مرتبط استفاده شده است.

---

[۱] شیرزاد، کامران، جرایم رایانه ای از دیدگاه حقوق جزای ایران و بین الملل، نشر بهینه فراگیر، چاپ اول، تهران ۱۳۸۸ ص۳۵

[۲] عمیدی، مهدی، مطالعه تطبیقی جرایم رایانه‌ای از دیدگاه فقه و حقوق کیفری ایران، پایان نامه کارشناسی ارشد حقوق جزا و جرم شناسی، دانشگاه آزاد اسلامی واحد تهران مرکز ، ۱۳۸۷ ص۲۰

- مفهوم جرم رایانه ای در کانادا

در کانادا نیز جرایم رایانه ای این چنین تعریف شده : «جرم رایانه ای شامل هر فعالیت مجرمانه ای است که در برگیرنده کپی، استفاده، جابه جایی، مداخله، دسترسی یا سوء استفاده از سیستم های رایانه ای، عملکرد رایانه، داده ها یا برنامه های رایانه است.»[۱]

- مفهوم جرم رایانه ای در فدرال آلمان

پلیس جنایی فدرال آلمان در تعریفی از جرایم رایانه ای این چنین اعلام داشته : «جرم رایانه ای در برگیرنده همه اوضاع و احوال و کیفیاتی است که در آن شکل های پردازش الکترونیک داده‌ها، وسیله ارتکاب و یا هدف یک جرم قرار گرفته و مبنایی برای نشان دادن این ظن است که جرمی ارتکاب یافته است.[۲]

- مفهوم جرم رایانه ای در شورای اروپا

دومین سازمانی که تلاش کرد تعریفی از این جرم ارائه کند شورای اروپا بود و بیان داشته هر فعل مثبت غیر قانونی که رایانه، ابزار یا موضوع جرم است . به عبارت دیگر باز هم این سازمان بین المللی نتوانسته تعریفی ارائه کند بلکه بیشتر به مصادیقی از جرم رایانه ای پرداخته تا به معیار دقیقی برای جرم رایانه ای ارائه دهد.[۳]

---

[۱] شریفی، مرسده، جرایم رایانه ای در حقوق جزای بین المللی، پایان نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد تهران، ۱۳۷۹ ص ۸۰.

[۲] دزیانی، محمد حسن، ابعاد جزایی کاربرد کامپیوتر و جرایم کامپیوتری، خبرنامه انفورماتیک، شورای عالی انفورماتیک کشور، شماره ۵۸، دی و اسفند ۱۳۷۳ صص ۱۵۷- ۱۵۸.

[۳] پور قهرمانی، بابک؛ بای، حسینعلی؛ آقا بابایی، اسماعیل؛ بررسی فقهی حقوقی جرایم رایانه، نشر: پژوهشگاه علوم و فرهنگ اسلامی، چاپ اول، ۱۳۹۰ص ۱۵.

کمیته اروپایی مسائل جنایی در شورای اروپا: در سال ۱۹۸۹ گزارش کاری بیان کرد که در آن یکی از متخصصان چنین تعریفی ارائه کرده است: هر فعل مثبت غیر قانونی که رایانه، ابزار یا موضوع جرم باشد. یعنی به عبارت دیگر هر جرمی که ابزار یا هدف آن تاثیر گذاری بر عملکرد رایانه باشد.[۱]

یافته ها

ارائه تعریف دقیق به نحو جامع و مانع، مشکل به نظر می‌رسد و دلیل آن جدید بودن ابعاد جرایم رایانه‌ای است. از این رو، مراجع قانونگذاری کشورهای مختلف هر یک به فراخور نیازها و تهدیدات پیش‌رو، تعریف متفاوتی از این جرایم ارائه کرده‌اند. برای مثال در ایالات متحده امریکا تعریف وسیعی از جرم رایانه‌ای به عمل آمده مبنی بر آنکه هر اقدام غیرقانونی که با یک رایانه یا به کارگیری آن مرتبط باشد، جرم رایانه‌ای می‌گویند. یا هر اقدامی‌که به هر ترتیب با رایانه مرتبط بوده و موجب ایجاد خسارت به بزه دیده شود و مرتکب از این طریق منافعی را تحصیل کند، جرم محسوب می‌شود. در ایران، نه در قانون تجارت الکترونیک و نه در قانون جدید مصوب جرایم رایانه‌ای هیچ تعریفی از این مفهوم ارائه نشده است. شاید دلیل آن اختلافات مبنایی است که میان حقوقدانان از تعریف جرایم رایانه‌ای وجود دارد. ارائه یک تعریف جامع از تعریف جرم رایانه ای به جهات ذیل حایز اهمیت می باشد: به لحاظ فراملی بودن جرم رایانه ای تعریف معین از این جرم می تواند در انجام معاضدت قضایی و همکاری بین المللی برای مبارزه با جرم رایانه ای موثر باشد. مقامات تعقیب و تحقیق و قضات دادگاه در انجام وظیفه ی محوله دچار مشکل نمی شوند.

---

[۱] دزیانی، محمد حسن، ابعاد جزایی کاربرد کامپیوتر و جرایم کامپیوتری، صص ۱۵۷- ۱۵۸.

با وجود تعریف جامع از این جرم در گردآوری آثار جرم به مشکلی بر نمی خوریم.[۱]

بند اول - مفهوم فضای مجازی در حقوق ایران: تعریف جامعی ارائه نکرده فقط بر وفق ماده (۱) قانون جرایم رایانه ای[۲] «هر کس به طور غیر مجاز به داده ها یا سامانه های رایانه ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد ...» فقط بخشی از جرم را پوشش داده و به مصادیق اشاره کرده به عبارت دیگر جرم رایانه ای در بر دارنده هر رفتار غیر قانونی است که رایانه یا شبکه به عنوان منبع، ابزار، هدف و مکان جرم مطرح می گردد[۳]. در حقوق ایران، نه در قانون تجارت الکترونیک و نه در قانون جرایم رایانه‌ای مصوب ۱۳۸۸/۱۱/۱۱ هیچ تعریفی از این مفهوم ارائه نشده است. شاید دلیل آن اختلافات مبنایی است که میان حقوقدانان از تعریف جرایم رایانه‌ای وجود دارد. اما می‌توان به عنوان نمونه تعریف زیر را ارائه کرد: «آن دسته از جرایمی‌که با سوءاستفاده از یک سیستم رایا،نه‌ای برخلاف قانون ارتکاب می‌یابد جرایم رایانه‌ای نام دارد». البته این دسته از جرایم را می‌توان شامل جرایم سنتی که به واسطه رایانه صورت می‌گیرد از قبیل کلاهبرداری و سرقت و نیز جرایم نو ظهوری که با تولد رایانه پا به عرصه حیات گذاشته اند دانست، مانند جرایم علیه صحت و تمامیت داده‌ها. در واقع در حقوق ایران تعریف جرایم رایانه ای به سکوت واگذار شده و در بیشتر موارد تقریباً همان تعریف ارائه شده از طرف سازمان همکاری و توسعه اقتصادی را پذیرفته اند.

[۱] پور قهرمانی، بابک؛ بای، حسینعلی؛ آقا بابایی، اسماعی؛ بررسی فقهی حقوقی جرایم رایانه، نشر: پژوهشگاه علوم و فرهنگ اسلامی، چاپ اول، ۱۳۹۰ص ۱۴.

[۲] منتشره در روزنامه رسمی مصوب ۱۳۸۸/۳/۵ شماره ۱۸۷۴۲ مورخ ۱۳۸۸/۴/۱۷

[3] http://en.wikipedia.org/wiki/computer-crime

ایرادات تعریف: در این که چه عناصر و عواملی جرم رایانه ای را تشکیل می دهد بین صاحب نظران اختلاف نظر است. هنوز تعریف جامعی که در سطح بین المللی مورد توجه باشد ارائه نشده، این امر هم ناشی از عوامل مختلفی از جمله نظام حقوق کیفری کشورهای مختلف است.[۱]

بند اول - ایرادات شکلی: با توجه به تعاریف ارائه شده ناقص، ایرادات را از دو بعد کلی شکلی و ماهوی بیان می کنیم:

۱- فراملی بودن جرم [۲]

با توجه به بعد فراملی بودن جرم رایانه ای، این جرم بدون توجه به مرزها و حاکمیت دولتها می تواند به وقوع پیوندد. حال به فرض اینکه بتوانیم مجرمین را شناسایی کنیم، کدام مرجع به صلاحیت جرم رسیدگی می کند؟ کدام دادگاه بین المللی صالح به آن رسیدگی است؟ مجرمین بدون نیاز به مکانی خاص می توانند به اهداف اصلی خود برسند. از طرف دیگر مجرمان سایبری به دنبال فرار از کشورهایی هستند که قانون جرایم سایبری سخت تری دارند. مجرمان می توانند با اتصال به اینترنت از هر نقطه ای مرتکب جرم شوند، با پیگیری جرم و سر نخ ها ممکن است چندین کشور و سازمان دیگر درگیر یک پرونده شوند.

۲-اثرات نامرئی[۳]

با توجه به جرم سنتی جعل، که در اسناد ظاهر می گردید در جعل رایانه ای از خود آثاری به وضوح نمی گذارد و متخصصین خاص خود را می خواهد، همچنین مدارک و اسناد موجود، به

---

[1] http://www.rooznamehrasmi.ir/Detail.as?
[2] oftransnational crime
[3] Invisible effects

اصطلاح دیجیتالی می باشد و مثل اسناد عادی در قوامین ملی کشورها نیست و نیازمند تعریف جامعی می باشد که این اثرات را نیز مورد عنایت قرار دهد.[۱]

بند دوم - ایرادات ماهوی: این تعاریف در بعد ماهوی نیز دچار اشکالاتی می باشد که به بررسی مختصری از آن می پردازیم:

۱- مطابقت نداشتن با قوانین ملی کشورها

بعضی از مصادیق اصلا جرم انگاری نشده مثلاً مبحث افترا، خیانت در امانت، دزدی، کلاهبرداری در بازی آنلاین و همچنین بعضی از مصادیق جرم انگاری شده ولی بر اساس قانون داخلی بعضی از کشورها جرم است و در بعضی دیگر جرم نیست مثلاً توهین به ساحت پیامبر اکرم در بعضی از کشورها به شدت برخورد می شود ولی بعضی دیگر آزادتر می باشند.[۲]

۲- به روز نبودن قوانین

این جرم با توجه به وسیله ارتکاب آن به سرعت در حال پیشرفته شدن و پیچیدگی خاص خود شده ولی در مقابل، قانونگذار یک پله از مجرم عقب تر است هنوز تعریف جامعی ارائه نکرده که بتوانیم مجرم را شناسایی کنیم.[۳] از طرف دیگر هم باید از شتاب زدگی نسبت به وضع قوانین اجتناب کرد. مهم ترین چالش در این عرصه، تاخیر بین شناخت پتانسیل سوء استفاده از فناوریهای جدید و اصلاحیه های ضروری برای قانون کیفری ملی می باشد.

[۱] زیبر، اولریش؛ جرایم رایانه ای، ترجمه محمد علی نوری، رضا نخجوانی، مصطفی بختیاروند و احمد رحیمی مقدم، کتابخانه گنج دانش، چاپ اول،۱۳۸۳، ص ۲۳۲.

[2] http://www.secondlife.com

[۳] گرگی، مارکو؛ جرایم سایبری راهنمایی برای کشورهای در حال توسعه، ترجمه مرتضی اکبری، نشر: پلیس امنیت فضای تولید و تبادل اطلاعات ناجا، چاپ اول ۱۳۸۹ ، ص۱۷۳.

۳- تعارض قوانین

با توجه به این که مرجع تصویب قوانین در هر کشوری متفاوت است و مطابق با عقاید و آداب و رسوم خود این قوانین را وضع می کنند بنابراین نگارش قوانین جرایم سایبری به طور جداگانه ممکن است منجر به تعارض قوانین و هدر رفتن منابع و وقت گردد. بنابراین یک کشور بعضی مصادیق را جرم تلقی می نماید و ممکن است کشور دیگر همان مصادیق را جرم نشناسد.[۱]

- ویژگی های جرم:

جرم رایانه ای، نوعی از جرایم اینترنتی می باشد. طبیعت این جرم در دنیای مجازی هیچ گاه در دنیای حقیقی واقع نمی شود. امنیت پایین این محیط مجازی و در مقابل وجود ابزار های تکنولوژی بالای در دسترس افراد شرور باعث سوء استفاده های فراوانی شده است. مهم ترین خصیصه ی این جرم بالا بودن انتشار سریع اطلاعات است. بدین نحو که اطلاعات به سرعت در فضای مجازی منتشر شده و فرد متخلف با کمترین امکانات و صرف کمترین وقت به اهدافی که خواسته سریع تر دست می یابد.

بند اول - ارتکاب جرم بدون علائم:

در فضای واقعی وقتی سرقتی اتفاق می افتد سارق رد پایی از خود به جای می گذارد صندوق پول یا صندوق جواهرات خالی شده در حالی که در فضای مجازی کمتر پیش می آید رد پایی باقی بماند. سارق در فضای مجازی می تواند یک کپی دیجیتال کامل از نرم افزار مسروقه بگیرد

[۱] گرگی، مارکو ؛ پیشین، ص ۱۷۴.

و نرم افزار اصلی را همان طور که دقیقا بوده باقی بگذارد. همچنین توسط رایانه ممکن است حسابی خالی شود ولی بدون هیچ علامتی باشد.[۱]

- عدم نیاز به مکان

به دلیل خصیصه ی فراملی بودن این جرم، نیاز به مکان خاصی برای تحقق ندارد، سازمان یا فردی ممکن است در کشور دیگری باشد و با اتصال به اینترنت وارد سازمان کشور مقابل شود، بدون نیاز به سفرهای هوایی یا زمینی به این سازمان، می تواند به اهداف مخصوصه خود برسد و اطلاعات مورد نیاز را برداشته یا در سیستم خرابکاری ایجاد کند. در این جرم، مرز معنایی ندارد.[۲]

- فراملی بودن

جرم سایبری اغلب دارای بعد بین المللی است. این جرم بدون توجه به ملیت، رنگ، زبان و... به وقوع می پیوندد. با ارسال پست های الکترونیکی غیر قانونی به کشورهای دیگر یا با ورود به سیستم کشورها و دست یابی به اطلاعات خرابکاری می کنند. با توجه به این که جرم به دلیل استفاده از تکنولوژی برتر و از مرزی به مرز دیگر به کشورها نفوذ می کند نیازمند یک همکاری بین المللی در این عرصه می باشد.

[۱] زیبر، اولریش، پیشین ص ۲۳۱.
[۲] گرگی، مارکو ، پیشین ص ۱۵۳.

- مجرمین رایانه ای

به دلیل آسان بودن ارتکاب این جرم و آسان بودن تهیه وسایل ارتکاب جرم، مرتکبین به مراتب بیشتر و تعقیب و دستگیری آن ها سخت تر می باشد. به طور کلی مجرمین را به دو دسته کلی تقسیم می کنند[1]:

۱- مرتکبینی که به دنبال حس کنجکاوی، رسیدن به یک نتیجه علمی و یا برای سرگرمی و غیره دست به ارتکاب می زنند (هکرها).

۲- مجرمینی که به دنبال منافع خود هستند (کراکرها).

- هکرها[2]

در دهه ۱۹۷۰ واژه هکر به شخصی اطلاق می شد که در برنامه نویسی ماهر بود، در دهه ۱۹۸۰ به شخصی اطلاق شد که در نفوذ سیستم ها به صورت ناشناس تبحر داشته باشد، امروزه به شخص یا سازمانی اطلاق می شود که با استفاده از تکنولوژی و با کمک فناوری موجود وارد سیستم مورد نظر شود. در واقع هکرها به دنبال کنجکاوی اطلاعات می باشند ممکن است در نهایت باعث خساراتی هم بشوند. در واقع بیشتر به دنبال یافتن اطلاعات هستند نه انتقام گیری و صدمه زدن.[3]

- کراکرها

دسته دوم از مجرمین کراکرها هستند که به دنبال رخنه انداختن در سیستم ها می باشند تا خرابکاری کنند و با هدف انتقام گیری دست به این کار می زنند. ویروس و کرم های رایانه ای را منتشر می کنند. در واقع هکرها دوستدار مطالبی هستند که دسترسی به آنها ممنوع شده و

[1] Arkin,s.s. Prevention and Prosecution of computer and hiy Technology crime ,1989
[2] Hacker
[3] en.wikipedia.org/wiki/Hacker

توسط سازمان مخصوصه فیلتر شده و به دنبال کنجکاوی هستند تا صدمه زدن، در مقابل هدف اصلی کراکرها صدمه زدن است.[۱] از جهت دیگر هم می توان گفت، مرتکبین جرایم مورد بحث، افراد و کاربران مجاز یا غیر مجاز می باشند. به طور مثال کارمندان یک بانک یا یک شرکت حق استفاده و کار کردن با رایانه این موسسات را دارند پس این افراد در دسته کاربران مجازند، در حالی که یک مشتری حق دسترسی به این سیستم ها را ندارد و چنانچه افراد غیر مجاز به این سیستم ها دسترسی پیدا کنند می توان تحت عنوان کلاهبرداری و استفاده غیر مجاز آنها را تحت تعقیب قرار داد. در مقابل کاربران بانک یا شرکت چنانچه قصد کلاهبرداری داشته باشند به راحتی می توانند به هدف خود برسند هر چند آنها هم در صورت ارتکاب تحت تعقیب قرار می گیرند ولی ارتکاب جرم برای کارمند بانک نسبت به مشتری آسان تر است.[۲]

- صلاحیت رسیدگی به این جرم

در همه کشورهای صنعتی تاکنون مباحثات قضایی مربوط به جرایم رایانه ای تنها به حقوق ماهوی متمرکز شده و در رابطه با مسائل آیین دادرسی کیفری مربوط به این جرایم کوتاهی شده است. جنبه های دادرسی مختص رایانه نه تنها از جهت تعقیب جرایم رایانه ای اهمیت دارد، بلکه از حیث تحقیقات جنایی که لازمه آن مراجعه به محیط های رایانه می باشد با لحاظ بکار گیری رایانه در اکثر یا همه جنبه های زندگی اجتماعی و اقتصادی اهمیت بیشتری داشته و خواهد یافت. لذا با توجه به خصیصه های یاد شده در این جرم و با توجه به فراملی بودن جرم

[۱] ایازی، رضا؛ قوانین و جرایم رایانه ای، فصل نامه مطالعات بین المللی پلیس، سال اول، شماره ۳، پاییز ۱۳۸۹.
[۲] شیرزاد، کامران، جرایم رایانه ای از دیدگاه حقوق جزای ایران و حقوق بین الملل، نشر بهینه فراگیر، چاپ اول، ۱۳۸۸ ص ۸۹.

رایانه ای کشورها و سازمان های مختلفی درگیر این موضوع هستند. بنابراین در دو بعد داخلی و بین المللی مورد بحث قرار می دهیم.[۱]

بند اول - صلاحیت بین المللی[۲]

محل وقوع جرم نیز در برخی از جرایم رایانه ای، مساله ای قابل تامل و مهم است، مخصوصاً وقتی جرم جنبه برون مرزی پیدا کند. هنگامی که سارق توسط یک خط تلفن با رایانه ای ارتباط برقرار می کند و اطلاعاتش را به دست می آورد و از نقطه ای به نقطه دیگر دنیا انتقال می دهد یا از بین می برد، محل وقوع جرم کجاست؟[۳] در حوزه بین الملل با توجه به اصول بین المللی موجود، رسیدگی به این جرم سخت شده است. با عنایت به اصل عدم مداخله در امور کشورها در صورت بروز این جرم ممکن است کشور محل وقوع جرم با سازمان های بین المللی با توجه به این اصل، همکاری لازم را نکند. در حال حاضر در حوزه بین الملل کشورها با قرار دادهای دو جانبه یا چند جانبه که با هم منعقد می کنند توافق به همکاری می کنند و متعهد می شوند همکاری لازم در جهت استرداد مجرمین انجام دهند. در مقابل ممکن است کشوری موافقت دو یا چند جانبه منعقد نکند که در این صورت اینترپل (پلیس بین الملل) با در اختیار داشتن کارشناسان و متخصصین کشورهای عضو و تشکیل کار گروه های مورد نیاز در حوزه بین الملل به این جرم رسیدگی می کند. پلیس بین الملل در کنار ایجاد پایگاه های داده های بزرگ مفصل که حاوی اطلاعات بسیار سودمند از مجرمان است به انتشار راهنماها، منابع آموزشی و فنی برای پلیس و مراجع ذی ربط اقدام کرده است.

---

[۱] شیرزاد، کامران، پیشین ص ۱۳۲.

[2] competent international

[3] http://www.afp.gov.au/media-centre/publications/platypus/previous editions/2000/june-2000/compcri.aspx

- صلاحیت ملی (داخلی)[1]

هر کشور نسبت مقررات داخلی خود می تواند با توجه به اینکه جرم در حوزه وی واقع شده به این موضوع رسیدگی نماید. اداره تحقیقات فدرال FBA یک کار گروه ویژه برای رسیدگی و تعقیب این جرم ایجاد کرده، بعضی کشورهای دیگر هم کارگروه هایی ایجاد کرده اند.[2] اداره تحقیقات فدرال دارایکنیروی ویژه به نام یگان ملی جرایم رایانه ای (NCCS) است که مسئول رسیدگی به تخلفات از قانون فدرال از جمله سوءاستفاده وکلاهبرداری رایانه ای در سال ۱۹۸۶ می باشد. در این قانون، افرادی که با استفاده از خطوط بین ایالتی یا بین المللی دست به اقداماتی نظیر ورود غیر مجاز به رایانه های فدرال یا ایالتی می زنند و در نتیجه به اطلاعات مالی یا پزشکی آنها دسترسی پیدا می کنند، متخلف شناخته می شوند. همچنین NCCS هر گونه ورود غیر مجاز به سیستم شرکت های تلفن یا شبکه رایانه ای بزرگ دیگر، با هدف، جاسوسی صنعتی، کلاهبرداری بانکی، ارتکاب جرایم سازماندهی شده و سرقت نرم افزار را مورد بررسی قرار می دهد. در ایران در حال حاضر پلیس فتا مطابق قانون جرایم رایانه ای پیگیری و تعقیب این جرم را بر عهده دارد. از آنجا که جرم را دادگاه عمومی رسیدگی می کند، باید قضات با تجربه و آگاه در این خصوص داشته باشند. و باید جرم در دادگاه های ویژه ای مورد بررسی قرار گیرد.

[1] National competency

[2] شیرزاد ، کامران، پیشین ص ۱۳۵.

نتیجه گیری و پیشنهادها

جرایم رایانه ای ممکن است در هر جایی اتفاق افتد و غالباً قابل رد یابی نیستند. این جرایم را جرم شناسان در زمره جرایم (یقه سفیدان[1]) مورد بررسی قرار می دهند. جرایم یقه سفید معمولاً از سطح دانش و آگاهی بالایی برخودار هستند. بنابر این بیشتر ادارات پلیس، فاقد پرسنل ماهر یا بودجه لازم برای مبارزه با جرایم رایانه ای هستند به ویژه به این دلیل که پرونده ها ممکن است در آن واحد به حوزه های قضایی متعددی مربوط شوند و همچنین قربانیان این جرم اغلب کم اتفاق افتاده شکایات و گزارشات خود را به مراجع قضایی ارائه دهند. بنابراین گزارش مطمئنی از این جرم در دست نداریم، باید با استفاده از تکنولوژی، اطلاعات دقیق تری به دست آوریم تا بتوانیم آسانتر و بهتر به پیشگیری و مقابله با این جرم بپردازیم.

راهکارهای پیشگیری از وقوع جرم در ابعاد داخلی:

۱- تدوین قانون جامع در رابطه با جرم رایانه ای که همه ابعاد جرم را مد نظر قرار بدهد .

۲- تقویت سیاست های اجرایی، انتظامی، امنیتی و نظارتی پیشگیرانه

۳- آموزش های لازم از طریق پلیس فتا به بخش های مختلف اداری، اقتصادی و ...

۴- اتخاذ تدابیر مناسب قضایی، امنیتی، انتظامی در جهت مبارزه قاطع و موثر با جرم

۵- با استفاده از فناوری پیشرفته برای پیشگیری و مبارزه با آن

۶- افزایش سطح سواد و علم گرایی

۷-کنترل اینترنت از طریق فناوری مدرن مثل فیلتر کردن و ...

۸- تخصصی کردن دادگاه ها و آشنایی قضات از علوم رایانه ای

---

[1] White Collar

در ابعاد بین المللی:

۱- تقویت همکاری بین المللی و منطقه ای به منظور اجرای برنامه های پیشگیری از وقوع جرم

۲- به کارگیری قانون واحد بین المللی در حوزه جرایم رایانه

۳- اعطای فناوری نوین از کشورهای توسعه یافته به کشورهای در حال توسعه

۴- برای مهار این جرم در صحنه ی جهانی نیاز به همکاری بین المللی می طلبد

۵- یک سازمان بین المللی در این عرصه به کنترل داده ها و اطلاعات بپردازد و در صورت مشاهده جرم به مراجع صالح اطلاع دهد

۶- ضمانت اجرای قوی وضع گردد و قاطعانه برخورد شود

فهرست منابع

- عالی پور، حسن (۱۳۹۰). حقوق کیفری فناوری اطلاعات، انتشارات خردسندی، چاپ اول.

- زیبر، اولریش (۱۳۸۳). جرایم رایانه ای، ترجمه: محمد علی نوری؛ رضا نخجوانی؛ مصطفی بختیاروند و احمد رحیمی مقدم، کتابخانه گنج دانش، چاپ اول.

- گرگی، مارکو (۱۳۸۹). جرایم سایبری راهنمایی برای کشورهای در حال توسعه، ترجمه: اکبری، مرتضی، تاثیر پلیس امنیت فضای تولید و تبادل اطلاعات ناجا، چاپ اول.

- پور قهرمانی، بابک؛ بای، حسینعلی؛ آقا بابایی، اسماعیل (۱۳۹۰). بررسی فقهی حقوقی جرایم رایانه، نشر: پژوهشگاه علوم و فرهنگ اسلامی، چاپ اول.

- شیرزاد، کامران (۱۳۸۸). جرایم رایانه ای از دیدگاه حقوق جزای ایران و حقوق بین الملل، نشر بهینه فراگیر، چاپ اول.

- قانون جرایم رایانه ای مصوب ۱۳۸۸/۳/۲۰ مجلس شورای اسلامی ایران.

- طارمی، محمد حسین (۱۳۸۷). گذری بر جرایم رایانه‌ای.

- ایازی، رضا (۱۳۸۹). قوانین و جرایم رایانه ای، فصل نامه مطالعات بین المللی پلیس سال اول شماره ۳.

- دزیانی، محمد حسن (۱۳۷۳). ابعاد جزایی کاربرد کامپیوتر و جرایم کامپیوتری، خبرنامه انفورماتیک، شورای عالی انفورماتیک کشور، شماره ۵۸.

- شریفی، مرسده (۱۳۷۹). جرایم رایانه ای در حقوق جزای بین المللی، پایان نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد تهران.

- عمیدی، مهدی (۱۳۸۷). مطالعه تطبیقی جرایم رایانه‌ای از دیدگاه فقه و حقوق کیفری ایران، پایان نامه کارشناسی ارشد حقوق جزا و جرم شناسی، دانشگاه آزاد اسلامی واحد تهران مرکزی.
- پاکزاد، بتول (۱۳۸۰). جرایم رایانه، پایان نامه کارشناسی ارشد، دانشگاه شهید بهشتی.
- Arkin,s.s. Prevention and Prosecution of computer and hiy Technology crime, 1989
- http://en.wikipedia.org/wiki/computer crime
- http://en.wikipedia.org/wiki/Hacker
- http://www.rooznamehrasmi.ir/Detail.as?
- http://www.secondlife.com
- http://www.vekalat.org/public.php?cat=2&newsnum=2312170#
- http://www.imj.ir/index.php?option=com
- http://www.afp.gov.au/media-centre/publications/platypus/previous-editions/2000/june-2000/compcri.aspx