مطالعات علوم سیاسی، حقوق و فقه
دوره ۱۱، شماره ۲، تابستان ۱۴۰۴
صفحات ۳۵۱-۳۳۴

Online ISSN: ۲۴۷۶-۴۴۶۹
Print ISSN: ۲۵۳۸-۲۰۳۹
www.irijournals.com

مطالعه تطبیقی جرایم فضای مجازی در حقوق ایران و فرانسه

عبدالحسین سبحان پور[۱]، احسان عزیزی[۲]

[۱] دانش آموخته ی کارشناسی ارشد گروه حقوق جزا و جرم شناسی، واحد نورآباد ممسنی، دانشگاه آزاد اسلامی، نورآباد ممسنی، ایران.

[۳] هیات علمی گروه حقوق خصوصی، واحد نورآباد ممسنی، دانشگاه آزاد اسلامی، نورآباد ممسنی، ایران.

چکیده

تحول اطلاعات و گسترش روز افزون استفاده از رایانه و اینترنت در تمامی ابعاد زندگی بشر و نیاز شرکت ها، سازمان ها، گروه ها به آن سبب وقوع جرایم مختلفی در فضای مجازی شده است. فضای مجازی با ویژگی های خود مانند فراملی بودن، تعدد بازیگران، مخفی بودن سبب شده افراد وارد این فضا شوند و بدون اینکه به راحتی مورد شناسایی واقع شوند جرایم مختلفی را مرتکب شوند. در این فضای مجازی اما واقعی و حقیقی جرایم مختلفی مانند سرقت، کلاهبرداری، جعل، جاسوسی به وقوع می پیوندد. برخی از این جرایم سبب آسیب و صدمه زدن به جامعه و به عنوان تهدیدی علیه امنیت داده ها محسوب می گردد. برخی دیگر از این جرایم صدمات مالی و اقتصادی وارد می کند و برخی نیز به عنوان تهدید و آسیبی علیه اشخاص می باشد. جرایم فضای مجازی به عنوان یکی از مسائل غیرقابل انکار در حوزه سیاست جنایی کشورها می باشد و به همین دلیل دولت ها درصدد مقابله با اینگونه جرایم برمی آیند. امنیت داده های هر کشوری یکی از نگرانی های دولت ها می باشد که در صدد تأمین امنیت داخلی و خارجی گام برمی دارند. به همین منظور در جهت مقابله با دستیابی غیر مجاز داده ها و جرایمی که بوسیله وسایل الکترونیکی و به شیوه پیشرفته به وقوع می پیوست، توسط قانونگذار آیین نامه ها و قوانینی وضع گردید تا بدینوسیله راه را برافرادسودجو ببندد و موجبات امنیت داده ها فراهم گردد.

واژگان کلیدی: حمایت کیفری، امنیت، امنیت داده ها، جرایم فضای مجازی، فضای مجازی

مقدمه

ورود رایانه به زندگی بشری و استفاده روز افزون از این وسیله شگفت انگیز سبب بوجود آمدن دگرگونی و تحولات گسترده در حیطه اطلاعات گردیده است. رایانه با ویژگی های منحصر به فرد خود مانند حجم بالای اطلاعات، دسترسی سریع و آسان به اطلاعات و ویژگی های متنوع و فراوان دیگری توانسته است، امکانات بی شماری را در اختیار افراد قرار دهد. همین امر سبب بوجود آمدن جرایم متنوع و مختلفی شده است که در مقایسه با جرایم کلاسیک می تواند آسیب های جبران ناپذیر و خطرناکی را به همراه داشته باشد (مقدسی و عیانی: ۱۳۹۲، ۱۲۸).

محیط فضای مجازی به مجرمین این امکان را می دهد که در فضایی به دور از دیدگان مردم به راحتی و در محیطی امن دست به ارتکاب جرم بزنند. امروزه با توجه به افزایش روز افزون استفاده کنندگان از اینترنت میزان جرایم سایبری نیز سیر صعودی به خود گرفته است. از آنجا که این گونه جرایم در سطح ملی و حتی فراملی رخ می دهد پس می توان گفت برای اینگونه جرایم حد و مرزی وجود ندارد. کاربران در این محیط به ایجاد تغییراتی در داده ها و اطلاعات زده که همین امر نشانگر وقوع جرمی می باشد.

مخفی بودن این محیط امکان تعقیب و شناسایی مجرمین را کاهش داده است. پس هر شخص به راحتی در هر نقطه از جهان می تواند در گوشه ای دیگر از جهان جرمی را مرتکب شود. همین امر موجب گردیده است که جهت تأمین امنیت داده ها وسیستم های رایانه ای قوانین و مقرراتی وضع گردد. به دلیل تنوع و گستردگی اینگونه جرایم کشف و مقابله با آنها لازم و ضروری می باشد. به همین دلیل است که تمام حقوق دانان وجرم شناسان به دنبال شناسایی ماهیت اینگونه جرایم بر آمدند. توسعه پدیده جهانی فناوری اطلاعات و ارتباطات، تحولی شگرف در ابعاد مختلف حیات اقتصادی، اجتماعی، فرهنگی سیاسی و امنیتی ایجاد نموده است. انقلاب الکترونیک تبدیل به مهمترین پدیده تعیین کننده معاصر شده است. روزانه ده ها هزار رایانه ورود خود را به دنیای جدید اعلام می کنند. ظهور شبکه ها به معنای تهدید بزرگ حریم اطلاعاتی و رابطه افراد در مقایسه با فنون قبلی ارتباطات است که ناشی از دسته بندی و ادغام پرونده ها و قابلیت ردگیری کارهای روزانه افراد است. این به معنای بوجود آمدن ارزشی ضد ارزش در دسترس بودن در هر مکان و زمان است که به وسیله آن می توان رد افراد را تا عمیق ترین زوایای جامعه گرفت. یکی از نگرانی های اساسی در مورد اینترنت حفظ حریم شخصی افراد و امنیت داده ها است اطلاعات گوناگون که درباره داده ها نگهداری می شود از طریق نفوذ به این سیستم ها امکان سوء استفاده و ایجاد خطر را برای شهروندان به دنبال خواهد داشت. به طور خاص اطلاعاتی که می تواند محرمانه یا شخص تلقی شود و امکان افشای آن از طریق اینترنت هست عبارت اند از: علائم تجاری، روابط جنسی، امور مذهبی و سیاسی، اطلاعات پزشکی و مالی یا امنیتی این اطلاعات که به دلایل مختلف و برای سهولت دسترسی به آنها و یا انتقال به دیگران از سوی شبکه های رایانه ای حفظ می شود به راحتی می تواند در اختیار افراد غیرصالح قرار بگیرد و با افشای آن ضررهای هنگفتی به مال یا آبروی افراد وارد آید. (مقدسی و عیانی، ۱۳۹۲)

امروزه علاوه بر نظارت هایی که به مدد فناوری اطلاعات در مورد امور شخصی مردم اعمال می شود، اطلاعات خصوصی گردآوری شدهٔ آنان یا دربارهٔ آنان نیز می تواند دستخوش تهدید و نقل و انتقال های کینه توزانه و زیان بار شود. اطلاعات راجع به تولد، ازدواج، طلاق، مالکیت اموال، گواهی نامه های رانندگی، مشخصات وسایل نقلیه، سوابق قانون شکنی ها و تخلّفات مؤثر، مشخصات پدری و مادری و نهایتاً وفات آنها ثبت می گردد. در دایره ی وسیعی از ذخیره اطلاعات، مردم با نام، نشانی، شماره تلفن، شمارهٔ کارت اعتباری، شماره تأمین اجتماعی، شماره گذرنامه و مواردی دیگر تعیین هویت می شوند. قانون حمایت از داده یکی از پایه های عصر جدید است که از اصول مهم فضای مجازی به شمار می رود و تقریباً همه کشورها سطح

متعارفی از اصول حمایتی آن را برقرار کرده اند. فقدان قوانین مناسب جهت حمایت از داده ها در زندگی امروزه حتی بر ساده ترین استفاده ها در فضای مجازی اثر می گذارد. انتقال فرامرزی اطلاعات شخصی در قالب فایلهای الکترونیکی به کشورهای دیگر، براساس قانون ملی کشورهایی که در این زمینه دارای قوانین تصویب شده هستند، تنها در صورتی امکانپذیر است که کشور مقصد نیز دارای قوانین مشابه حمایت داده باشد. اگر چه قانونگذار با تصویب قانون جرایم رایانه ای خلأ فقدان این قانون را با توجه به بسط و گسترش استفاده از سیستم های رایانه ای و مخابراتی پر نموده و نسبت به مجرمانه قلمداد نمودن افعال و اعمال در این خصوص اهتمام ورزیده، اما با تطبیق و بررسی این قانون هنوز خلأهایی در این قانون مشاهده می گردد. از طرف دیگر مجازاتی که برای برخی از این جرایم در این قانون پیش بینی شده به مراتب بسیار کمتر از مجازات مذکور در مقررات کیفری عمومی است. با توجه به اهمیت موضوع لازم است که برای تدوین قانون و بررسی جوانب آن از متخصصین کامپیوتر استفاده شود چرا که این رشته به عنوان یک رشته نوین و جدید بوده و بسیاری از نکاتی که در این زمینه می بایست مطرح شود فقط توسط اندشمندان این رشته قابل بحث است که می توانند کمک شایانی به قانونگذار در تدوین قانون جامع و مانع که کلیه جوانب را در نظر گرفته باشد، بکنند. همچنین با توجه به گسترش روزافزون علوم رایانه ای و گسترش استفاده عامه در مناسبات روزمره و ظهور روش های نرم افزاری و سخت افزاری متعدد و به روز خرابکارانه سیستم رایانه ای جهت دسترسی غیر مجاز به داده های شخصی افراد، می طلبد که قانونی پویا جهت پوشش دادن به کلیه موارد موجود در این زمینه تدوین گردد. (باقری اصل، ۱۳۸۹)

تفاوت‌های اصلی در مجازات جرایم فضای مجازی بین ایران و فرانسه عبارتند از:

در ایران، برخی جرایم فضای مجازی مانند سرقت اینترنتی به‌صورت حدی (مجازات‌های مشخص و قطعی) تلقی می‌شوند و مجازات‌هایی مانند حبس یاحتی اعدام برای جرایمی نظیر جاسوسی سایبری وجود دارد.

در فرانسه، مجازات‌ها بیشتر تعزیری و مالی هستند؛ مثلاً جریمه‌های سنگین مالی متناسب با درآمد مرتکب یا شرکت‌های متخلف (مانندجریمه ۱۱۸ میلیون دلاری فیسبوک) اعمال می‌شود و حبس نیز در محدوده‌های مشخص قانونی است که قاضی نمی‌تواند خارج از آن حکم دهد.

فرانسه مجازات‌ها را با توجه به شدت جرم و شرایط تشدیدکننده (مانند باندی بودن جرم یا سوءاستفاده از مقام دولتی) افزایش می‌دهد، در حالی که ایران امکان تعیین مجازات در بازه حداقل و حداکثر را بر اساس اوضاع و احوال مرتکب دارد.

همچنین فرانسه در قوانین خود تأکید بیشتری بر حمایت از حقوق مصرف‌کننده و شفافیت هویت تبلیغ کنندگان آنلاین دارد که تخلف از آن با جریمه‌های مشخص مواجه است، موضوعی که در قوانین ایران کمتر مورد توجه است.

به طور خلاصه، مجازات‌ها در ایران غالباً شدیدتر و مبتنی بر مقررات اسلامی است، در حالی که فرانسه بیشتر به مجازات‌های مالی و چارچوب‌های قانونی مشخص و حمایت از حقوق کاربران فضای مجازی توجه دارد. سوال اصلی که در اینجا مطرح می شود ای است که رویکرد نظام حقوقی ایران و فرانسه در جرائم فضای مجازی چیست و تا چه حد باهم تطابق دارد؟

پیشینه پژوهش و مبانی نظری

سدره نشین در پایان نامه خود با عنوان قانون جرایم رایانه ای ایران از دیدگاه حقوق کیفری و مهندسی نرم افزار در سال ۱۴۰۲ بیان نمود که، قانون جرایم رایانه ای مصوب پنجم خرداد ماه سال ۱۳۸۸ از قوانین جدیدی است که تحولی را در نظام حقوقی ایران به وجود آورده و نمایانگر حمایت کیفری از ارزش های جدیدی در جامعه ایران است که رواج پدیده رایانه و فضای سایبر آن را ایجاب می کند. اما برای تهیه قانونی مناسب که حقوق و تکالیف دست اندرکاران و کاربران این حوزه را

تعیین کند، ایجاد زبان مشترک میان حقوقدانان و متخصصین فن آوری اطلاعات و ارتباطات و نگاه قانونگذار به موضوعات مختلف از زاویه دید مهندسین نرم افزار رایانه و کاربران فضای سایبر، ضرورتی انکار ناپذیر است. به نظر می رسد این حمایت کیفری در وهله نخست، مبتنی بر مصلحت های امنیت کشور و منافع ملی است که در حیثیت عمومی هر جرمی ریشه دارد، ولی در جرایم رایانه ای تا قلمرو «تسامح صفر» پیش رفته است. بدین سان، افزون بر جرم انگاری های گسترده و کیفرگذاری های سنگین در این قانون، نه تنها فصلی مستقل از آن به تشدید کیفرها اختصاص یافته، بلکه در مواردی که در این قانون، برای رفتار ارتکابی مجازات یا مقرراتی مقرر نشده است، برحسب مورد، طبق قوانین جزایی دیگر اقدام خواهد شد. در وهله دوم، حمایت کیفری مورد نظر در قانون جرایم رایانه ای، برای حمایت و پشتیبانی از بزه دیدگان واقعی این جرم ها است که عفت، ناموس، حیثیت، تمامیت وجودی و یا دارایی های مادی و معنوی آنها مورد آسیب و مخاطره قرار می گیرد. با وجود این، جنبه اخیر حمایت کیفری، زیر سایه ویژگی امنیت مدار این قانون قرار گرفته است. به گونه ای که به نظر می رسد متولیان تصویب این قانون، خطر جرایم رایانه ای را تا جایی احساس می کرده اند که حتی مجال ویرایش قانون را نیز نیافته اند.

نیما نادرخانی (۱۴۰۰) در پایان نامه کارشناسی ارشد خود تحت عنوان جرایم علیه تمامیت داده ها و سامانه های رایانه ای بیان نمود که، حفاظت از تمامیت عناصر رایانه ای، یکی از اهداف اساسی در وضع قوانین مربوط به جرایم رایانه ای در هر کشوری است، این ارزش هم پایه و یا حتی بیش از سایر ارزش ها موجود در عرصه الکترونیکی، مورد حمایت قرار گرفته است، چرا که یکی از ابتدایی ترین و با اهمیت ترین حقوق در این عرصه، در امام بودن اشخاص از تعرض به تمامیت داده ها و سامانه های رایانه ای آنهاست. جرایمی که بر ضد تمامیت در فضای الکترونیکی قابل وقوع هستند و در قانون جرایم رایانه ای ایران از آنها به عنوان دو جرم علیه تمامیت در فضای الکترونیکی قابل وقوع هستند و در قانون جرایم رایانه ای ایران از آنها به عنوان دو جرم علیه تمامیت داده ها و سامانه های رایانه ای نام برده شده است، مشتمل بر دو جرم اصلی می باشند، یکی از این دو، جرم تخریب داده های رایانه ای است، که مرتکب آن درصدد ایراد ضرر و آسیب رسانیدن بدون حق به داده رایانه ای است و دیگری، جرم اخلال در سامانه های رایانه ای است، که مرتکب آن به توسط انجام اقداماتی بدون حق بر روی داده های رایانه ای، می خواهد به سامانه رایانه ای آسیب برساند و یا کارکرد آن را مختل سازد. هر دوی این جرایم را می توان تحت عنوان تخریب رایانه ای بررسی نمود و البته نباید این نکته را از نظر دور داشت که جرایمی چون تروریسم و ساپوتاژ رایانه ای نیز علی رغم وجود سابقه ی امنیتی در آنها، ماهیتا از زمره زیر شاخه ها یجرایم علیه تمامیت داده هاو سامانه های رایانه ای محسوب می گردند.

عبدالرضا جوان جعفری (۱۴۰۰) در مقاله خود با عنوان جرایم سایبر و رویکرد افتراقی حقوق کیفری بیان نمود که، فناوری اطلاعات، تمام ابعاد زندگی اجتماعی، اقتصادی، فرهنگی و از جمله حقوق کیفری را عمیقا متاثر ساخته است. این تحول، حقوقدانان و سیاست گذاران حوزه های مربوطه را به تامل وادار نموده است. تفاوت های جرایم سایبر با جرایم سنتی به گونه ای است که رویکرد کیفری متعارف و اصول و مبانی شناخته شده آن برای مقابله با این جرایم پاسخگو نیستند. فرامرزی بودن، سهولت ارتکاب جرم و ناشناختگی مجرمین از جمله خصایص این گونه جرایم اند. ویژگی های مذکور از یک سو و وابستگی های ساختارهای زندگی مدرن به تکنولوژی سایبر از یک سوی دیگر، تبیین یک رویکرد کیفری متفاوت را ضروری ساخته است. اثربخشی و کارآیی قوانینی که برای مقابله با جرایم دیجیتال تصویب می شوند، مستلزم نگاهی متفاوت به مقولاتی مانند تعریف جرم، ارکان جرم، مسئولیت کیفری و امثال آن است.

مهدی رزاقی نژاد در سال ۱۳۹۹ در پایان نامه خود با عنون بررسی سیاست جنایی ایران در قبال جرائم علیه صحت و تمامیت داده ها و سیستم‌های رایانه‌ای و مخابراتی بیان نمود که، حفاظت از صحت و تمامیت داده ها و سیستم های رایانه ای از اهداف

سیاست جنایی کشورها در وضع قوانین و جرم انگاری در حیطه فناوری اطلاعات می باشد زیرا که این دو اصل از اصول اساسی حاکم بر حمایت از داد ها و سیستم ها بوده و از اهمیت فوق العاده ای برخوردار است. جرائمی که ضد صحت و تمامیت در فضای الکترونیکی قابل وقوع هستند شامل چندین جرم می باشند. یکی از اینها جرم جعل رایانه ای ضد صحت داده ها می باشد که در قوانین متعدد چون قانون جرائم رایانه ای، قانون تجارت الکترونیک و قانون جرائم نیروهای مسلح جرم انگاری گردیده و هدف مرتکب ایجاد یا تغییر در داده ها و برنامه های رایانه ای می باشد. قسم دیگر این جرائم عنوان عام خرابکاری رایانه ای می باشد که جرائم ضد تمامیت داده و سامانه ها را در بر می گیرد و چهار عنوان تخریب داده، اخلال در سیستم، ممانعت از دسترسی و تروریسم سایبری را شامل می شود که مرتکب آن با انجام اقداماتی بدون حق به داده های رایانه ای آسیب رسانده و یا کارکرد سیستم را مختل می نماید. آشنایی با مفاهیم اساسی هر یک از این جرائم و بررسی ارکان سه گانه و شناسایی انواع پاسخ های واکنشی و تدابیر کنشی در دو محور پیشگیری اجتماعی و وضعی وتبیین مدل سیاست جنایی کشور ایران در با مقابله با این قسم از جرائم به عنوان اهداف این پژوهش مد نظر قرار گرفته است.

مفهوم و ویژگی های فضای مجازی (سایبری)

امروزه بحث های مربوط به اطلاعات و ارتباطات الکترونیکی وارد عرصه جدیدی بنام فضای مجازی شده است.

واژه فضای سایبر نخستین بار توسط ویلیام گیبسون[1] در سال ۱۹۸۴ به کار برده شد (زندی: ۱۳۸۹، ۳۸).

منظور از فضای مجازی محیط هایی غیر مادی است که در آن کاربران توسط وسایل الکترونیکی همچون اینترنت به یکدیگر متصل می شوند و از نظر خود دنیای مجازی را بوجود می آورند که وجود واقعی ندارد در حالی که این دنیا حقیقتی مجازی است که توسط رایانه بوجود آمده است. هرچند در زبان فارسی واژه سایبر را به مجازی ترجمه کرده اند ولی فضای سایبری فضایی است حقیقی و واقعی که بسیاری از کارهای باور نکردنی که تنها در ذهن ما نمود پیدا می کنند در این فضا و این دنیای مجازی حقیقت پیدا می کند. آن چه به موازات ساده سازی و تنوع بخشیدن به کارکردهای انعطاف پذیر رایانه ها، بهره برداری گسترده تر و متنوع تر از سیستم های رایانه ای شخص[2] را به نحو باور نکردنی توسعه داد و به آن وجه های جهانی بخشید، امکان اتصال آن ها به یکدیگر از طریق ارتباطات الکترونیک است. این امر اشتراک گذاری کارکردها و اطلاعات میان رایانه ها را میسر ساخت و به تدریج شبکه ای جهانی به وجود آمد و فضایی به نام فضای سایبر شکل گرفت به طوری که از دنیای فیزیکی کاملاً متمایز بود و ویژگی هایی داشت که نمونه های آن در داستان های تخیلی آمده بود (باقری اصل: ۱۳۸۹، ۱۱).

در این فضا می توان بسیاری از کارهایی را که تنها در ذهن و خیال می باشد، به راحتی و به دور از چشم دیگران انجام داد و همین امر موجب گردیده است تا درصدد کشف اینگونه جرایم و شناخت مجرمینی که در این محیط دست به ارتکاب جرم می زنند برآمد. با چنین تعبیری از فضای سایبر به دنیای مجازی صرفاً می توان بزهکاران و مجرمینی که دراین محیط پهناور دست به ارتکاب جرم می زنند و همچنین علل ارتکاب جرم را شناخت و با اتخاذ تدابیر مناسب بتوان در پیشگیری اجتماعی و نهادینه سازی هنجارهای اخلاقی سایبری مورد بررسی قرار داد. از محیط سایبر به محیط فناوری اطلاعات یا محیط اطلاعات و ارتباطات نیز یاد شده است. ازاین رو، مشاهده می شود که برای نمونه به جرم های محیط سایبر جرم های علیه فناوری اطلاعات نیز گفته می شود. این عبارت ها نیز نمی توانند به گونه ای جامع متضمن جرم های محیط سایبر باشند، زیرا، برای

[1] .William Gibson
[2] .Personal computer

نمونه، بسیاری از جرمها در محیط سایبر و با استفاده از این محیط ارتکاب می یابند و نه لزوماً علیه محیط سایبر. بنابراین، عبارت جرم های علیه فناوری اطلاعات نیز عبارت درستی نیست. همچنین، باید توجه داشت که فناوری اطلاعات بر ابزار تأکید دارد، حال آنکه سایبر به محیطی اشاره دارد که جرم درآن محیط به وقوع می پیوندد (فضلی: ۱۳۸۳، ۱۶۵).

فضای سایبری و ارتباط شبکه های اطلاع‌رسانی

فضای مجازی با توجه به گستردگی و تنوع کاربران آن، دنیای جدیدی را بوجود آورده است که دارای قابلیت ها و کارکردهای مختلفی است و به نسبت کارکردهای آن چالش های مختلفی نیز بوجود آورده است. با ظهور اینترنت و ارتباطاتی که در سطح جهانی به وجود آمد، ایجاد شبکه جهانی را می توان یکی از مظاهر فن آوری اطلاعات به شمار آورد که با پیدایش رایانه ها و سامانه های ارتباطی و تحول گردش اطلاعات توانست در زندگی انسان ها تأثیر بگذارد. رایانه توانست روش جمع آوری و تولید اطلاعات و پردازش داده ها را متحول سازد. داده ها عبارت از نمادهایی هستند که می توانند قابلیت انجام کارهایی مانند ورود، خروج، پردازش و ذخیره در یک سیستم رایانه ای را داشته باشند. داده ها به اشکال مختلف از جمله متن های صوتی و تصویری، دیسکهای نوری، یا داده های رقمی که دریک تراشه ذخیره شده و برای سیستم رایانه ای دارای مفهوم خاصی است، پردازش می کنند. کامپیوتر یا اینترنت را می توان به عنوان ساختار اصلی جرایم سایبری دانست، در فضای سایبری اینترنت نقش اصلی را ایفا می کند و این فضا چیزی غیر از داده و اطلاعات نیست که گاهی این دو در معنای مشابهی مورد استفاده قرار می گیرند. دراین فضا به راحتی می توان به آنسوی دنیا متصل شد و به تبادل اطلاعات در سطح بین المللی دست یافت. که این تبادل اطلاعات تنها به وسیله سخت افزارهای رایانه ای عمکرد خود را اجرا خواهد کرد (رضوی: ۱۳۸۶، ۱۲۴).

مخفی و پنهان بودن

پنهانی و مخفی بودن فضای مجازی را می توان یکی دیگر از ویژگی های آن دانست. این فضا را همانند ذهن آدمی که بسیاری از قضایا درآن نقش می بندد و به صورت پنهانی است، می توان تشبیه نمود. تا زمانی که افکار خود را در عمل نشان ندهد آن چیز تنها در ذهن خود آن شخص است و به صورت پنهانی است، امّا وقتی آن افکار نمایان شود گاهی سبب نقض قوانین و هنجارهای جامعه خواهد شد. در فضای سایبر نیز اشخاص در محیطی امن از طریق رایانه های خود، هر آنچه را که در ذهن دارند و به صورت پنهانی و پوشیده می باشد نمایان می سازند. به نقل از اندیشمندانی چون «هابز» که ذات انسان را شرور می دانند در چنین فضایی دوباره قوت می گیرد، چرا که حس پوشیده بودن و مخفی ماندن اعمال ارتکابی است که اینترنت را دنیایی آزاد جلوه گر می سازد تا در این پهنه، افراد به شکلی افسار گسیخته و فارغ از کنترل های اجتماعی و اخلاقی میدانی برای تاخت و تاز و عقده گشایی آنچه بدان دست نیافته اند بیابند؛ نمونه این امر را می توان در مورد انتشار تصاویر مستهجن کودکان در فضای سایبر دید که در عین حالی که وسیله سود آوری برای ارائه کنندگان این تصاویر گشته، برای خواستاران ارضای غرایز جنسی نیز دنیایی آزاد فراهم آورده تا هر لحظه که خواستند بتوانند به راحتی وارد این دنیای خیال گونه شوند و تمایلات غریزی خود را فرو بنشانند (فضلی: پیشین، ۱۲۷).

فراملی و غیر قابل کنترل بودن

فراملی بودن و غیر قابل کنترل بودن اینترنت و عدم وجود محدودیت مکانی و زمانی برای آن یکی دیگر از ویژگی های فضای مجازی می باشد. پیدایش میلیاردها سایت اینترنتی در این فضا سبب شده کاربران بسیاری در سطح جهانی و بین المللی

بوسیله رایانه با یکدیگر مرتبط شده و همین امر گاهی مشکلات فراوانی را موجب می گردد، از جمله می توان به خدشه وارد کردن به حاکمیت سرزمینی دولت ها اشاره داشت و همین امر کنترل این دنیای بزرگ را با مشکل رو به روساخته است. در این فضا به وسیلهٔ شبکه جهانی اینترنت می توان با صرف کمترین هزینه ممکن، به آسان ترین شیوه به گنجینه کامل از اطلاعات در هر نقطه از جهان دست یافت. به طور مثال در فضای مجازی یک کاربر در دورترین نقطه اهواز با فشردن یک دکمه با یک سرویس دهنده در خراسان می تواند تماس و ارتباط برقرار کند یا شخصی در دورترین نقطه قاره اروپا با یک کاربر در قاره آسیا بدون اینکه هیچگونه محدودیتی وجود داشته باشد با یکدیگر در ارتباط باشند. اینترنت ابزارهای جدید ارتباطی مانند وبلاگ ها را ایجاد نموده است، که جهت انتقال اطلاعات و افکار کاربران براحتی می توانند خواسته ها و اندیشه های خود را وارد شبکه های مورد نظر خود نمایند تا دیگران از آن استفاده نمایند. همین امر اینترنت را از ارتباطات یکطرفه خارج ساخته و از آن رسانه ای مبتنی بر تعامل می سازد که آزادانه افراد، گروه ها، سازمان هارا به یکدیگر متصل می سازد. تصور اشخاص از این محیط این است که در این فضا به دور از چشم قانون و به دور از نظارت سازمان یا افراد مختلف، هر کس هر آنچه می خواهد انجام می دهد چرا که او را در حین ارتکاب جرم نمی بینند. بنابراین ویژگی دیگر این محیط عدم امکان یک کنترل مؤثر تکنیکی و حقوقی در شرایط حاضر است (بیگی: ۱۳۸۴، ۳۶).

جرایم سایبری و ویژگی آن

باتوجه به نقش وسیع و گسترده سیستمهای رایانه ای در ابعاد مختلف زندگی بشری و افزایش روز افزون جرایم مرتبط با رایانه در اغلب کشورها، بویژه کشورهای پیشرفته و بوجود آمدن تنش و چالش های گوناگون، اغلب دولتمردان در صدد شناخت اینگونه جرایم و وضع قوانین و تدابیری در جهت جلوگیری از جرایم و برخورد با مرتکبین اینگونه جرایم برآمده اند. در این قسمت در قسمت اول از جرایم سایبری و جرایم مرتبط با آن تعاریفی ارائه می گردد و در قسمت دوم به سیر تاریخی جرایم سایبری در ایران و نظام بین الملل خواهیم پرداخت.

امروزه نقش اصلی اینترنت را می توان در انقلاب اطلاعات در عصر صنعت و تکنولوژی و نیازهای جامعه بشری به اینگونه پیشرفت ها و تأثیرات آن بر زندگی انسان ها دانست. از جمله مزایای اینترنت می توان به قابلیت های تراکم اطلاعات و فرآیندها، قابلیت دستیابی به سیستم های کامپیوتری، اینترنت و تجارت الکترونیک، اینترنت گنجینه اطلاعاتی و تبادل فرهنگ ها را نام برد (باستانی: ۱۳۹۰، ۴۱).

درکنار مزایایی که اینترنت به عنوان یک شبکه بین المللی دارد باید، معایب و مشکلاتی را که بوجود آورده است برشمرد. برهمین اساس می توان، بوجود آمدن زمینهٔ مناسب برای ارتکاب جرایم مرتبط با کامپیوتر را نام برد. مانند جرایم اینترنتی، جرایم سایبری، جرایم مالتی مدیا (چند رسانه ای). جرایم اینترنتی می تواند نقض حق مالکیت معنوی، نقض حق اختراع، ربودن اسرار تجاری و غیره باشد. این جرایم، همچنین شامل حمله عمدی به رایانه ها به منظور مختل کردن آن ها و یا کپی از اطلاعات طبقه بندی شده می شود. تحلیل گران هزینه جرایم اینترنتی رابرای صنعت جهانی بیش از هزارمیلیارد دلار در موارد نقض مالکیت فکری واز دست دادن اطلاعات تخمین زده اند. بیشترمجرمان اینترنتی ازمجازات فرارمی کنند. این فعالیت پر سود و اغلب بودن مجازات، در واقع تهدیدی برای امنیت ملی به شمار می آید (خلیلی پور و نورعلی وند: ۱۳۹۱، ۱۷۳).

امروزه با تحول و پیشرفت در زمینه ارتباطات واطلاعات بسیاری از جرایم سنتی نیز به جرایمی تبدیل شده اند که توسط رایانه و در محیطی غیرفیزیکی به وقوع می پیوندند وجرایم سایبری نامیده می شوند. برخلاف جرایم کلاسیک که درآن زمان و مکان وقوع جرم مشهود می باشند. در جرایم سایبری زمان ومکان وقوع جرم به آسانی قابل شناسایی نمی باشد و همین امر سبب

شده است که هکرها به وسیله رایانه ها و ابزارهای الکترونیک به راحتی با زیرپا گذاشتن حریم شخصی افراد اطلاعات شخصی قربانیان را مورد هدف انواع مختلفی از جرایم سایبری قراردهند. جرایم سایبری را می توان یکی از جرایمی دانست که به سرعت رو به رشد است و تعداد مرتکبین این گونه جرایم در حال افزایش می باشد. همانطور که انسان ها در زندگی خود بدنبال پیشرفت علمی در رشته های مختلف می باشند در زمینـهٔ فناوری اطلاعات و ارتباطات نیز هر روز بر تعداد استفاده کنندگان از اینترنت نیز افزوده می شود و بر سطح علمی خود در زمینهٔ نحوهٔ استفاده از این فن آوری جدید ارتباطات می افزایند. هرچه وابستگی انسان ها به استفاده از رایانه بیشتر شود، به همان میزان بر جرایم مرتبط با رایانه نیز افزوده خواهد شد. ازآنجا که جرم سایبری یک مسئله اجتماعی، عاری از خشونت هایی است که ممکن است در جرایم سنتی وجود داشته باشد و دارای ماهیت اقتصادی است، به تعریف و شناخت جرایم سایبری و جرایمی که می تواند به نحوی با آن مرتبط باشد خواهیم پرداخت.سپس ویژگی های اینگونه جرایم را بیان می نماییم.

جرم سایبری و جرایم مرتبط با آن

اینترنت از اتصال چندین رایانه به یکدیگر بوجود آمده است. این عرصه را وسایل بشری نظیر تلفن، تلگراف، خطوط سیمی و ماهواره به یکدیگر متصل کرده است و همین امر سبب تحول دنیای کامپیوتر و ارتباطات شده است. امروزه بر اثر اینگونه تحولات شگرف در زمینه فناوری اطلاعات و ارتباطات، بسیاری از جرایم سنتی به جرایم مدرن تبدیل شده است که در فضای مجازی و به وسیله رایانه انجام می شود و جرایم سایبری نامیده می شود. در کنار اینگونه کاربرد اینترنت باید با قابلیت های دیگر اینترنت در زمینه تجارت الکترونیک، پست الکترونیک، تبادل اطلاعات و غیره نیز اشاره داشت. همین ویژگی اینترنت سبب بوجودآمدن جرایم مختلفی در زمینه های گوناگون آن شده است. ازجمله جرایم تجارت الکترونیک، جرایم مالتی مدیا، جرایم اینترنتی وغیره. مفهوم تجارت الکترونیک به معنای پردازش عملیات های تجاری دو یا چند طرف تجاری از طریق کامپیوترهای شبکه بندی شده (بطور مستقیم متصل به هم یا متصل به اینترنت) است. به عبارت دیگر، تجارت الکترونیک تمام مراحلی را که در یک چرخه تجاری اجرا می شود شامل تبلیغات، تکمیل صورتحساب، پشتیبانی و خدمات مشتریان، در بر می گیرد (باستانی: پیشین، ۴۲).

پس جرایم تجارت الکترونیک را می توان جرایمی نامید که در بستر مبادلات تجاری و مالی انجام می گیرد و بوسیلهٔ وسایل ارتباطی غیر از رایانه مانند تلفن، تلگراف وغیره نیز به وقوع می پیوندد. در حقیقت فناوری اطلاعات تنها در رایانه خلاصه نمی شود. تجهیزات تأمین کننده ارتباط از راه دور مانند مخابرات، ماهواره و غیره نقش عظیمی در گسترش قابلیتهای فناوری اطلاعات دارند، چنانچه مهمترین مظهر فناوری اطلاعات که اینترنت است بدون استفاده از تجهیزات ارتباطی، مخابراتی، قابلیت استفاده نخواهد داشت. بدیهی است که این تجهیزات جدید نیز مانند رایانه مورد سوء استفاده مجرمان واقع می شوند، بنابراین در بهینه فناوری اطلاعات، وقوع جرم لزوماً به معنای وقوع جرم مرتبط با رایانه، جرم رایانه ای نیست. پس برخی محققان به دنبال عبارتی که همه ی جرایم مرتبط با فناوری اطلاعات را پوشش دهد، تعبیر«جرایم فناوری اطلاعات»یا «جرایم فناوری برتر » را برگزیده اند (خرم آبادی: ۱۳۸۴، ۵۵).

بنابراین باید گفت با ورود این پدیده در ابتدای دهه ۹۰ میلادی یک تحول اساسی ایجاد شد و به پدیده ای فوق رایانه، تعبیر شد. زیرا از تلفیق رایانه و مخابرات و ماهواره و امکانات ضبط، صدا و تصویر وغیره این جرایم ایجاد شده بودند و لذا هر چند رایانه نقش مهمی در این بین ایفا می کند، اما دیگر به عنوان تنها عامل مؤثر در این فضا محسوب نمی شود. پس نه تنها

جرایم سایبری بلکه جرایمی که توسط رایانه به وقوع می پیوندد و در بالا به آن اشاره شد را می توان زیر مجموعه جرایم سایبری نامید و آن ها نیز می توانند به عنوان تهدیدی برای امنیت محسوب شوند.

ویژگی های جرایم فضای مجازی

شناخت ویژگی های جرایم سایبری راهی آسان و مطمئن جهت شناخت ماهیت اینگونه جرایم می باشد و می تواند کمک مؤثری برای مقابله با مشکلات ناشی از این جرایم باشد. دراین محیط کاربران می توانند به هرگونه خدمات اطلاعاتی الکترونیکی دستیابی پیدا کنند، بدون در نظر گرفتن اینکه این اطلاعات و خدمات در کدام نقطه دنیا واقع شده است. محیط مجازی زمینه فعالیت های اقتصادی مهم و ابزار ضروری برای انجام کلیه معاملات تجاری در سطح بین المللی و فراملی بدون دخالت مستقیم بشر را فراهم آورده است. با توجه به گستردگی جرایم اینترنتی، در فضای مجازی و مجازی اینترنت همانند فضای واقعی جهان خارجی انواع جرایم و جنایات مانند کلاهبرداری، تخریب و اختلال در داده ها، جعل، جاسوسی وغیره اتفاق می افتد که این جرایم ویژگی های خاص خود را دارد. پس می توان گفت که تقریباً تمامی جرایمی که درجهان فیزیکی رخ می دهد، در جهان مجازی نیز به وقوع می پیوندد ولی وجه تمایز اینگونه جرایم در سرعت و سهولت ارتکاب اینگونه جرایم می باشد. یعنی به دلیل امکانات و فناوری های پیشرفته و تکنولوژیهای ارتباطی جرایم سایبری به آسانی رخ می دهد. از دیگر ویژگی های جرایمی که در محیط مجازی رخ می دهد به بقایای آثار مجرمانه اشاره داشت. در جرایم سایبری برخلاف جرایم سنتی و کلاسیک می باشد. درجرایم کلاسیک مجرم به صورت آنی مرتکب جرم شده یعنی جرمی را در لحظه ای مرتکب می شود ولی آثار و بقایای آن به صورت مستمروجود دارد. بلکه فضای مجازی بدلیل ویژگی خاص خودیعنی فنی بودن و خودکار بودن امکان باقی ماندن جرم برای تقریباً مدت زمان طولانی وجود دارد. از جمله چالشهای پی چوبی فعالیت های مجرمانه در حوزه محاسبات، گستره تحصیل کلیه ادله است. ازجمله عواملی که درایجاد چالش ها نقش دارند عبارتند از:

نخست اینکه ماهیت توزیعی شبکه ها موجب توزیع صحنه های جرم شده مشکلات عملی و صلاحیتی را بوجود آورده است. به عنوان مثال در اکثر موارد امکان جمع آوری ادله از رایانه ای واقع در مکآن های مختلف فراهم نیست، بلکه پیچیدگی اینکار فقط در جرایم مهم قابل اجرا می باشد.

دوم داده های دیجیتال به راحتی قابل حذف و یا تغییرند، لازم است هرچه سریعتر جمع آوری و نگهداری شود.

سومین عامل که دراین فرآیند نقش ایفا می کند حوزه گسترده تخصصی فنی است که در زمان مواجه شبکه ها به افعال مجرمانه به آن نیاز می شود (زندی: ۱۳۸۹، ۶۰).

جرایم سایبری به عنوان نسل سوم از جرایم را شامل می شود که تلاشهایی در جهت شناسایی اینگونه جرایم و ویژگی های خاص آن در سطح بین المللی صورت گرفته است که در نتیجه موجب تدوین قوانین مخصوص دراین رابطه شده است (شیرزاد: ۱۳۸۸، ۱۰۹).

جرایم فضای مجازی و وضع قوانین مربوط به آن

با توجه به استفاده روز افزون از کامپیوتر امروزه با اینکه عمر چندانی از تاریخ ورود رایانه به ایران نمی گذرد ولی چالش های مختلفی را برای حقوق جزا و رشته های آن بوجود آورده است. باتوجه به اینکه از عمر جرایم سایبری بیش از دوهه نمی گذرد این جرایم سبب ایجاد چالش در رشته های مختلف حقوق جزا و در نهایت آیین دادرسی کیفری را دچار تحولاتی ساخته است. استفاده از رایانه سبب رشد سریع جرایم شده است. از نیمه دوم دهه ۱۳۷۰ و بالاخص از ابتدای دهه ۱۳۸۰ که استفاده

از رایانه های شخصی توسط سازمان های اداری و مؤسسات خصوصی و افراد حقیقی گسترش یافته دسترسی به خدمات متعدد اینترنت امکان پذیر شده است. ارتکاب جرایم رایانه ای نیز از رشد نسبتاً سریعی برخوردار بوده است. جرایم مختلفی مانند اهانت و افترا نسبت به اشخاص حقیقی و حقوقی، اشاعه فحشا و منکرات و انتشار عکس ها و تصاویر و مطالب خلاف عفت عمومی از جمله جرایمی هستند که بعد از فراهم شدن امکان استفاده از خدمات اینترنت به وقوع پیوسته اند. قانونگذار باالحاق تبصره ۳ به ماده ۱ قانون مطبوعات در سال ۱۳۷۹ مقرر داشت «کلیه نشریات الکترونیکی مشمول مواد این قانون است » و بالاخره قانونگذار تصمیم به وضع قانون جرایم سایبری در سال ۱۳۸۸ نمود. در کشورهای پیشرفته به دلیل استفاده بسیار بالا از اینترنت در زمینه مختلف سیاسی، اجتماعی، اقتصادی، امنیتی و نفوذ افراد در داده ها و اطلاعات خصوصی و تخریب اطلاعات دولت ها از مدتها قبل درصدد تلاش جدی جهت مقابله با اینگونه جرایم بوده اند و مجازاتهایی را وضع نموده اند (شیرزاد: پیشین، ۱۱۷).

تحقیقات مقدماتی و کشف جرایم فضای مجازی در حقوق ایران و فرانسه

در کنار اوصاف جرایم رایانه ای از جمله سهولت ارتکاب آن، مسئله دشواری کشف این جرایم وجود دارد. در این گفتار از دیدگاه آیین دادرسی کیفری دو نکته اساسی را بررسی و مرور می‌کنیم. یکی دلایل عدم کشف جرایم رایانه ای و دیگری طرقی که می‌توان به وسیله آن کشف جرایم مذکور را افزایش داد.

دلایل دشواری کشف و تعقیب جرایم سایبر در حقوق ایران و فرانسه

موانع و مشکلات موجد در راه کشف و اطلاع از جرایم در زمینه داده پردازی، اجرای صحیح و دقیق قانون و تعقیب جرایم رایانه ای به ویژه توسط مراجع تحقیق و دادگاهها را به موضوعی پیچیده و بغرنج تبدیل کرده است. دلایل متعددی در خصوص دشواری کشف جرم وجود دارد. در ذیل مهم‌ترین آن را بیان می‌کنیم:

۱- بی‌تجربگی مجریان قانون: مأمورین تحقیق در زمینه تکنولوژی غالباً فاقد اطلاعات لازم هستند، و نه از نحوه ارتکاب این جرایم سر در می‌آورند و نه از نحوه ی چگونگی کشف آن. عدم آشنایی بازرسان، مأمورین تحقیق و قضات با رسانه های اطلاعاتی و ضعف آنها در برخورد با مسایل فنی جرایم رایانه ای عاملی است برای تشدید هر چه بیشتر مشکلات فوق الذکر. (چاشنام، ۱۳۸۲، ص ۴۰)

۲- علاوه بر دلیل مذکور به خاطر دلایل دیگری، مثل ترس از دست دادن شهرت تجاری و مواجه شدن با ضرر و رکود اقتصادی به طور کلی نا امید بودن به نتایج تحقیقات و رسیدگی، بزه دیدگان وقوع جرم را به مقامات ذی‌صلاح اطلاع نمی‌دهند و ترجیح می‌دهند تا فقط آثار جرم ارتکابی را متحمل شوند.[1]

در فرانسه نیز آمار این جرایم خاص، نه آمار کلی جرم و جنایت، در سالنامه آماری توسط وزارت کشور صادر شده، می‌تواند احتمالا اشتباه باشد، و به استنباط از آنها صدمه بزند.[2] در واقع، این احتمال وجود دارد که شرکت ها یا اداراتی که قربانیان این جنایات هستند تمایلی به اعلام نداشته باشند که اعتماد عمومی مشتریان خود و یا ایمنی و قابلیت اطمینان شبکه خود را از دست ندهند. با توجه به مطالعه انجام شده در سطح اروپا، »تنها یک دهم بزه ها شناخته شده است و بسیاری از موارد مثل اختلاس یا جرایم خارج از مرزها اصلاًکشف نمی شود.

[1] -Arkin s. Prevention and Prosecution of computer and hiy tecnology crime.p۱۹۸۹

[2] -Code de procedure penale de france L'article-5

اما با توجه به گزارشCERT تیم واکنش اضطراری کامپیوتر) تعداد حملات تروریستی علیه شرکت‌های اروپایی از ۶۶ مورد در سال ۱۹۸۸ به ۳۷۳۴ در سال ۱۹۹۸ و به ۰۰۰، ۱۵ در سال ۲۰۰۰ افزایش یافته است. با وجود تمامی مشکلات برآورد جهانی جرایم اینترنتی پیشرفت مواجه شده است. به عنوان مثال، آماری که توسط آقای دیویدBenichou ، بازپرس، تهیه شده نشان می‌دهد روشهای مربوط به تقلب در پرداخت از ۱۰۰ مورد در سال ۱۹۹۵ به حدود ۶۰۰ مورد در سال ۱۹۹۸ رسیده است. استفاده جعلی از شماره کارت اعتباری در هنگام خرید تلفنی و یا اینترنتی، با توجه به آمار و ارقام منتشر شده توسط وزارت کشور بین سالهای ۱۹۹۹ و۲۰۰۰ به شدت افزایش یافته است. لازم به ذکر است دفتر مرکزی مبارزه با جرم و جنایت در فن آوری اطلاعات و ارتباطات فرانسه توسط فرمان شماره ۲۰۰-۴۰۵ در ۱۵ مه ۲۰۰۰ ایجاد شده است (ضیایی پرور، ۱۳۸۳صص۳۰۶ و ۳۷۰).

۳- گاهی عدم کشف یا دشواری آن به دلایل فنی است. مثلاً تشخیص و شناسایی ویروسهای مرسوم به بمب‌های ساعتی یا منطقی[1] بسیار سخت است. کار این بمب‌های ساعتی این است که اقدامات خطرناک خود را به محض ورود به سیستم آغاز نمی‌کنند، بلکه در گوشه ای از آن پنهان می‌شوند و در وقت معین، ناگهان فعال شده و مثل یک بمب ساعتی استفاده کننده از سیستم را شوکه می‌کنند. گاه تاریخ خاصی را برای فعال شدن ویروس تعیین می‌کنند. مثلاً اول تیر ماه رایانه به محض اینکه به این تاریخ برسد، ویروس اقدامات تخریبی خود را شروع می‌کند. برخی از این ویروسها، پس از خرابکاری، دوباره به خواب می‌روند و این خود بر دشواری کشف آنها می‌افزاید. (عرب مازاد، ۱۳۷۴، ص۳۹ ۴۳ و ۴۴، ص۲۳.)

۴- کثرت داده ها: تکنولوژی پیشرفته، یعنی ظرفیت حافظه رایانه و سرعت بالای عملیات آنها خود یکی دیگر از دلایل مهم محسوب می‌شود۸. تعداد بسیار زیاد داده های پردازش شده در سیستم‌های داده پردازی که کنترل آنها ممکن نیست، نیز مانعی در راه کشف و تعقیب جرایم رایانه ای محسوب می‌شود.

۵-بسیاری از بزه دیدگان برنامه ریزی لازم برای مقابله با حوادث مربوط به جرایم رایانه ای را ندارند و ممکن است حتی توان تشخیص وجود مشکل امنیتی را نداشته باشند.

۶-دقت، مهارت و تمهیدات مرتکبین جرایم مرقوم، خود دلیل دیگری است. این عده همیشه یک گام جلوتر از پلیس حرکت می‌کنند.

۷- اخفای جرم :در موارد بسیاری امکان کشف موارد نقض حریم خصوصی اشخاص و کشف جرم، برای بزه دیده و مقامات دولتی فراهم نیست زیرا اعمال مجرمانه در مراکز رایانه ای ارتکاب می‌یابند که از آنها به نحوی محافظت می‌شود. برای نمونه کلاهبرداری رایانه ای غالباً از طریق دست‌کاری پرینت‌های داده پردازی کتمان می‌شود. (پیشین، ص۲۳۲)

۸-آثار نامرئی : در بسیاری از موارد، کشف و تعقیب جرایم رایانه ای به این دلیل با مشکل مواجه می‌شود که تغییرات صورت گرفته در برنامه‌ها و داده ها آثاری مانند آثار ناشی از جعل سنتی بر جای نمی‌گذارد. اسناد و مدرک رایانه ای فقط به وسیله سیستم‌های رایانه ای قابل رویت و خواندن می‌باشند؛ مثلاً جعل رایانه ای با تغییر در داده ها آثاری همچون جعل سنتی ندارد۲.امروزه تحلیل و بررسی خط افراد در بانک‌های داده الکترونیکی غیر ممکن است. به منظور تقلیل مشکلات مربوط به تشخیص نویسنده واقعی داده های وارد شده (ضیایی پرور، ۱۳۸۳صص۳۰۶ و ۳۷۰) باید در جهت شناسایی اشخاص تلاش نمود که داده ها از چه طریق به رایانه وارد شده است. روش دیگر برای انجام تحقیق، پیگیری رد مبالغ سرقت شده است که این مبالغ در اکثر موارد به مرتکب انتقال می‌یابد.

[1] -Padova, Yann , Un apercu de la lutte contre la cybercriminalite en France , Revue de science .2002, criminelle

۹-نامرئی بودن مدارک :تعقیب جرایم رایانه ای مستلزم کنترل گسترده داده های رایانه ای است. بیشترین داده ها به شکلی مرئی که توسط انسان قابل خواندن باشد نگه داری نمی‌شوند بلکه در قالب‌هایی نامرئی که فقط دستگاه قادر به خواندن آنهاست و به صورت بسیار متراکم در ابزار های ذخیره سازی الکترونیکی نگه داری می‌شوند. بنابراین یکی از مشکلات مراجع تعقیب و دادگاهها در کشف و پیگیری جرایم رایانه ای فقدان مدارک مرئی و مفهوم است که این فقدان حاصل مجهول بودن، تراکم و حتی در بیشتر موارد کدگذاری داده هایی است که به صورت الکترونیکی ذخیره شده اند. (فهیمی، ۱۳۹۶ ص ۶۵)

۱۰- امحای مدارک: مشکل دیگر این است که مجرمین به راحتی می‌توانند از طریق حذف و پاک کردن دلایل علیه خود را از بین ببرند. مثلاً مجرم می‌تواند دستورهای معمولی در سیستم عامل را به گونه ای تغییر دهد که با وارد کردن دستور کپی یا چاپ از طریق صفحه کلید رایانه همه داده ها حذف شوند. یا از طریق میدان الکتریکی به هنگام گشوده شدن فایل داده ها به وسیله اشخاص غیر مجاز آن فایل پاک شود.

۱۱-کدگذاری مدارک : مجرمین قادرند فعالیت‌های تعقیب و پیگیری را با به‌کارگیری تدابیر امنیتی مانند استفاده از گذرواژه ها، ارایه دستورالعمل‌های مانع و روشهای کدگذاری با مشکلات حادتری مواجه نمایند. یکی از موانع راه تحقیقات رمز گذاری است که مجرمان به عنوان مانعی برای تحقیقات جنایی از آن استفاده می‌کنند. روشهای رمزنگاری در سالهای اخیر به شد ت دست‌خوش دگرگونی شده است. افراد برای اطلاعات خصوصی و تجارت الکترونیکی ممکن است نیاز به استفاده از رمزنگاری داشته باشند. از طرفی متخلفین نیز برای مراقبت از اطلاعات خود از این فناوری بهره می‌گیرند. بنابراین اگر مجری قانون مجهز به تکنیک‌های رمزنگاری در چارچوب تعیین شده نباشد، به سختی می‌توان وارد اطلاعات متخلفین شده و اسناد لازم برای محکمه را آماده کرد. (زیبر، اولریش، ۱۳۹۸، ص۲۳۱)

۱۲-نارسایی‌های حقوقی و محدودیت‌های مرزی :در صورت ارتکاب جرایم رایانه ای فراملی یا فرامرزی، کشورها اغلب با مشکلات دیگری به ویژه در خصوص همکاری‌های دوجانبه و استرداد مجرمین رو به رو هستند.

البته در فرانسه طبق ماده ۳ قانون ۱۰ مارس ۱۹۲۷، همکاری قضایی در استرداد به رسمیت شناخته شده است (فهیمی، ۱۳۹۰، صص ۲۳و۲۴). اما محدودیتی که در این زمینه وجود دارد این است که مطابق ماده ۶ کنوانسیون اروپایی استرداد مورخ ۱۳۳ دسامبر ۱۹۵۷ حق امتناع از استرداد اتباع خود به رسمیت شناخته شده است[1]. محدودیت دیگری که وجود دارد این است که، با توجه به قانون فعلی فرانسه، استرداد تنها در صورتی امکان پذیر است که عمل در کشوری که درخواست استرداد کرده و کشوری که از او تقاضا شده جرم و قابل مجازات باشد (حاکمیت قاعده تبهکاری دوگانه۴)و۵.در ایران نیز مطابق قانون استرداد مجرمین که در سال ۱۳۳۹ به تصویب رسید استرداد پذیرفته شده است[2].

در خصوص مشکل »تبهکاری دوگانه« در فرانسه، که مطابق آن اقدام فرد هم باید در کشور متقاضی و هم تقاضا شونده جرم باشد، باید گفت با این حال، در پی حملات ۱۱ سپتامبر ۲۰۰۱، ۱۵ کشور عضو اتحادیه اروپا در اجلاس سران اتحادیه اروپا در Laekenدر ۱۴ و ۱۵ دسامبر ۲۰۰۱ ۱تصمیم گرفتند که حکم بازداشت اروپایی، »جایگزین سیستم فعلی استرداد میان کشورهای عضو« باشد که اجازه می‌دهد که تسلیم افراد توسط مقام قضایی به مرجع قضایی کشور متقاضی امکان پذیر باشد بدون حکومت تبهکاری دوگانه که برای جرائم خاصی مورد نیاز است.

[1] - règle de la double incrimination. Padova, Yann, Un apercu de la lutte contre la cybercriminalite en France , Revue de science .2002, criminelle

[2] -http://www.dalloz.fr/PopupDocumentPrint?famille-id=REVUES&produit-id=RSC&c...۳

طرق کشف جرایم در حقوق ایران و فرانسه

نظر به اینکه وجود اشکالات مذکور در زمینه کشف، سبب بروز نتایج نامطلوبی مثل تجری مرتکبین خواهد شد، ضروری است تا در رفع این موانع اقدامات موثری را به انجام رساند. یکی از این طرق عبارت است از نقش و ابتکار بزه دیدگان و شاکیان (اعم از بالفعل یا بالقوه). در این خصوص می‌توان به اتحادیه گزارشگران نرم افزار در فرانسه اشاره کرد که غالب پیگیری‌های آن از طریق تماس مستقیم بزه دیدگان و شاکیان است. راه حل دیگر ایجاد تهمید قانونی برای مدیران سازمانها در خصوص ارایه گزارش به پلیس در رابطه با جرایم ارتکاب یافته در محدوده شبکه های داده پردازی الکترونیک است و در نقطه مقابل، عدم گزارش جرم است.

مطابق ماده ۱۵۶ قانون جدید آیین دادرسی مدنی فرانسه، »در هر حوزه قضایی، تحقیق و آزمایش در مورد یک وسیله فنی، ممکن است، با درخواست دادستان عمومی و یا به درخواست هر یک از طرفین، به یک متخصص ارجاع داده شود« در این زمینه، این کارشناس همچنین ممکن است تحقیقات، تجزیه و تحلیل فن آوری و تمام عملیاتی که از نظر بازپرس برای کشف حقیقت لازم است انجام دهد .بنابراین، این تجزیه و تحلیل ناقص خواهد بود اگر آن را به کارشناسان، که نقش ضروری در یک محیط دیجیتال دارند ندهند. (گاتن، آلن ام؛ ۱۳۸۳، ص۳۸)

لزوم بهره گیری از بخش خصوصی در حقوق ایران و فرانسه

برخی از شهروندان به طور شخصی به پلیس در کشف جرایم و شناسایی مجرمان همکاری می‌کنند، به این معنا که شخصاً از طریق رایانه به تحقیقات می‌پردازند و نتیجه را به پلیس گزارش می‌دهند.۲و۳ در برخی کشورها مثل فرانسه شرکت‌هایی تحت عنوان خدمات ادله رایانه ای تأسیس شده اند که به صورت خصوصی به افراد سرویس می‌دهند و متخصصانی در اختیار آنها قرار می‌دهند. این امر می‌تواند الگوی وکلا و حقوقدانان در تأسیس چنین شرکت‌هایی با مشارکت متخصصان رایانه باشد.

ایجاد دادگاههای تخصصی در حقوق ایران و فرانسه

یکی از ارکان نظام عدالت کیفری که نیازمند تغییر به سمت تخصصی شدن است، مراجع قضایی رسیدگی‌کننده به این‌گونه جرایم تخصصی است. اختصاص دادگاههای جزایی ویژه و قضات متبحر در این حیطه با توجه به افزایش میزان وقوع این دسته از جرایم امری اجتنابناپذیر است. در کشور فرانسه این اقدام صورت گرفته موضوعی که متأسفانه قانون جدیدالتصویب جرایم رایانه‌ای ایران به آن کم لطف بوده و مانند جرایم ارتکابی از سوی اطفال و نوجوانان بزهکار با این قضیه برخورد کرده است. به این صورت که در زمینه بزههای ارتکابی توسط اطفال به رغم احساس نیاز به تاسیس مراجع قضایی تخصصی برای رسیدگی به پرونده های این قشر خاص از بزهکاران، قانون آیین دادرسی دادگاههای عمومی و انقلاب در امور کیفری مصوب سال ۱۳۷۸ فقط به تشخیص رییس قوه قضاییه شعبی از دادگاههای عمومی را برای رسیدگی به این امر اختصاص داده و ارجاع این پرونده های خاص، مانع رسیدگی به سایر پرونده ها نیست. طبق مادهی ۳۰ از قانون جرایم رایانه‌ای، قوه قضاییه موظف شده تا به تناسب ضرورت شعبه یا شعبی از دادسراها، دادگاههای عمومی و انقلاب، نظامی و تجدیدنظر را برای رسیدگی به جرایم رایانه‌ای اختصاص دهد! به نظر می‌رسد صرف تدوین تبصره ماده فوق الذکر که اشعار داشته، قضات دادسراها و دادگاههای مذکور از میان قضاتی که آشنایی لازم به امور رایانه دارند، انتخاب خواهند شد، به عنوان یک راه کار اساسی کفایت نمی‌کند (دزیانی، ۱۳۹۳، ص۳۷).

ماده ۱- ۲۳۰ قانون آیین دادرسی کیفری فرانسه، برگرفته از قانون نوامبر سال ۲۰۰۱، امکان رمزگشایی از داده های بدست آمده در یک تحقیق را برای دادستان، قاضی یا دادگاه به منظور فراهم می‌کند. مطابق این ماده هنگامی که معلوم می شود که داده های موجود یا حاصل از جریان تحقیق یا رسیدگی، موضوع اقدامات تغییر دهنده ای قرار گرفته اند که دسترسی به اطلاعات قابل فهم موجود در آنها را ممنوع می کند، دادستان شهرستان مرجع تحقیق یا مرجع انشای رأی مسئول پرونده می تواند هر شخص حقیقی یا حقوقی صلاحیت دار را برای انجام اقدامات فنی و اجازه کسب نسخه ی قابل فهمی از این اطلاعات و در صورت استفاده از دستگاه کشف رمز در صورت ضرورت، کلید محرمانه کشف رمز، انتخاب نماید.

نتایج

فضای سایبری محیط فناوری اطلاعات و ارتباطات نامیده می شود که به عنوان یکی از مهم ترین منابع قدرت در عصرجدید می باشد. این فضا با ویژگی های منحصر به فرد خود سبب شکل گیری جرایم مختلفی و به وجود آمدن مجرمین سایبری گردیده است که براحتی می توانند جامعه بین المللی را مختل سازند. تکنولوژی های جدید اطلاعات موجب جلب بزهکاران فراوانی به این فضا می باشد از این فضا می توان به عنوان محیطی جهت انجام اقدامات تروریست ها برضدداده ها نام برد. همین امر باعث جلب توجه حقوقدانان، جرم شناسان، نیروی پلیس در سطح ملی و بین الملل به شناسایی و کشف اینگونه جرایم می باشد.پس تهدیدات سایبری به عنوان یکی از مسائل مهم وانکار ناپذیر در حوزه سیاست جنایی دولت ها می باشد.در واقع جامعه بین المللی با یک مشکل جدی مواجه می باشد. دولت ها باید با اتخاذ تدابیر و راهکارهای مناسب درجهت سالم سازی و مقابله با اجتماعات آلوده به فساد گام بردارند، البته قوانینی را که تا کنون دولتها وضع نموده اند ناظر بر اینگونه اهداف بوده است.

از ابتدای زندگی بشر امنیت یکی از دغدغه‌های اصلی‌انسان‌ها بوده است، امروزه با گسترش اینترنت و فضاهای شبکه‌ای در کشورمان لزوم امنیت برای فعالیت در این فضاهای مجازی بیش از پیش احساس می‌شود. ترس و بیم از تخریب مبانی اخلاقی و اجتماعی و نداشتن امنیت روانی و فرهنگی ناشی از هجوم اطلاعات آلوده و مخرب از طریق اینترنت و فضاهای مجازی واکنشی منطقی است، زیرا هر جامعه‌ای چارچوب‌های اطلاعاتی خاص خود را دارد. طبیعی است که هر نوع اطلاعاتی که این حد و مرزها را بشکند، می‌تواند سلامت و امنیت جامعه را به خطر اندازد. برخلاف وجود جنبه‌های مثبت شبکه‌های جهانی، سوءاستفاده از این شبکه‌های رایانه‌ای توسط افراد هنجارشکن، امنیت ملی را در کشورهای مختلف با خطرروبرو ساخته است. از این رو به‌کارگیری روش‌ها و راه کارهای مختلف برای پیشگیری از نفوذداده‌های مخرب و مضرو گزینش اطلاعات سالم در این شبکه‌ها رو به افزایش است. خوشبختانه با وجود هیاهوی بسیاری که شبکه جهانی اینترنت و فضاهای سایبر را غیرقابل کنترل معرفی‌می‌کند، فناوری‌لازم برای‌کنترل این‌شبکه و انتخاب اطلاعات سالم روبه گسترش وتکامل‌است.

از آنجا که تکنولوژی های کامپیوتر و اینترنت سبب تغییر ماهیت جرایم از شیوه های کلاسیک به نسل جدیدی از آن با عنوان داده ها و اطلاعات می باشد دیگر قوانین کلاسیک در حقوق کشورها کافی نبود و نیاز به وضع قوانین جدید در این خصوص احساس می گردید. قانونگذار ایران نیز در جهت مقابله با اینگونه جرایم و حفاظت از اطلاعات شخصی اشخاص و امنیت داده ها به وضع قوانینی مرتبط با اینگونه جرایم پرداخته است و این نشانگر این است که حقوق جزا وارد مرحله جدید شده است و با گونه جدیدی از جرایم مواجه است که نیاز به حمایت از اطلاعات و داده ها می باشد.

امروزه پلیس از این توانایی برخوردار است که با استفاده از نرم افزارهای قدرتمند که در اختیار دارد، با گشت زنی در فضای مجازی، در پیشگیری از وقوع جرایم سایبری و تامین امنیت داده ها نقش بسزایی ایفا نماید.تعامل و همکاری مناسب میان

شرکت های مخابراتی ارائه دهنده این گونه خدمات و پلیس می تواند در فرایند تامین امنیت داده ها کمک شایانی نماید. آموزش همگانی و همچنینی شناسایی و ارائه آموزش های خاص به اشخاص و سازمان هایی که احتمال می رود در معرض جرایم سایبری قرار گیرند، یکی دیگر شیوه های تامین امنیت در در فضای مجازی است.

پیشنهادات

۱. با توجه به گستردگی و اهمیت جرایم سایبری و اهمیت امنیت داده ها و حریم خصوصی و از نظر اینکه اینگونه جرایم ماهیتی کاملاً جدید در حوزه حقوق کیفری دارند باید تدوین قوانین و تعقیب مجرمین سایبری اهمیت بسیاری راداشته باشد. قوانین وضع شده توسط قانونگذار در زمینه جرایم سایبری از آنجا که مربوط به سال ۱۳۸۸می باشد بهتر می بود که در مجازات های نقدی که در نظر گرفته شده است تجدیدنظر صورت گرفته و مقدار آن افزایش می یافت.

۲. در زمینه تهدیدات مرتبط با امنیت داده ها از آنجا که این تهدیدات در ذیل جرایم سایبری به شمار می آیند این به معنای حذف عنوان آنها نمی باشد و اینگونه تهدیدات در قانون جرایم رایانه ای کم رنگ جلوه داده شده است باید در این مورد نیز توجه بیشتری توسط قانونگذار صورت بگیرد.

۳. در ایران با رواج و استفاده روز افزون از رایانه و اینترنت و افزایش جرایم سایبری نیاز به هماهنگی و همکاری بیشتر پلیس در زمینه کشف و تعقیب مجرمین مشاهده می شود. پس نیاز به آموزش های لازم در این زمینه به نیروی پلیس می باشد، در سطح بین الملل نیاز به همکاری با مجامع بین المللی و شناخت و دستیابی به نوعی اتفاق نظر و ایجاد راه حل‌های بنیادین در مورد شناسایی و تعقیب مجرمین می باشد.

منابع مآخذ

۱. آقاجانی، سجاد (۱۳۸۴)، بررسی راهکارهای مبارزه با جرایم رایانه ای با توجه به مقررات داخلی و بین المللی، پایان نامه کارشناسی ارشد دانشکده علوم انسانی، دانشگاه تهران.

۲. باستانی، برومند (۱۳۹۰)، جرایم رایانه ای و اینترنتی جلوهای نوین از بزهکاری، نشر بهنامی، تهران.

۳. چاشنام، پورسوانیف؛ کشف، تحقیق و تعقیب جرایم کامپیوتری، ترجمه بابازاده، قاسم، خبرنامه تخصصی انفورماتیک نشریه دبیر خانه شورای عالی انفورماتیک کشور، سال هیجدهم، شماره۹۰، سال۱۳۸۲، ص۴۰.

۴. خرم آبادی، عبدالصمد (۱۳۸۴)، تاریخچه، تعریف و طبقه بندی جرم های رایانه ای، مجموعه مقاله های همایش بررسی جنبه های حقوقی فناوری اطلاعات.

۵. خلیلی پور رکن آبادی، یاسر و نورعلی وند، یاسر (۱۳۹۱)، تهدیدات سایبری و تأثیرات آن برامنیت ملی . فصلنامه مطالعات راهبردی ش۲۰.

٦. دزیانی، محمد حسن، پی جویی صحنه جرم الکترونیک (مقاله)، ترجمه و تلخیص خبرنامه تخصصی انفورماتیک نشریه دبیر خانه شورای عالی انفورماتیک کشور، سال نوزدهم، شماره۹۴، بهمن سال ۱۳۸۳، ص۳۷.

۷. رضوی، محمد (۱۳۸۶)، جرایم سایبری و نقش پلیس در پیشگیری از این جرایم، فصلنامه دانش انتظامی، ش۹.

۸. زندی، محمدرضا (۱۳۸۹)، تحقیقات مقدماتی در جرایم سایبری، انتشارات جنگل، تهران.

۹. زیبر، اولریش؛ جرایم رایانه ای، ترجمه محمد علی نوری، رضا نخجوانی، مصطفی بختیاروند، احمد رحیمی مقدم، چاپ اول، سال۸۳، چاپ گنج دانش، ص۲۳۱.

۱۰. ضیایی پرور، حمید، جنگ نرم (۱): ویژه جنگ رایانه ای، تهران، مؤسسه فرهنگی مطالعات و تحقیقات بین المللی ابرار معاصر، چاپ اول، سال ۱۳۸۳صص۳۰۶ و ۳۷۰ .

۱۱. ضیایی پرور، حمید، جنگ نرم (۱):ویژه جنگ رایانه ای، تهران، مؤسسه فرهنگی مطالعات و تحقیقات بین المللی ابرار معاصر، چاپ اول، سال ۱۳۸۳صص۳۰۶ و ۳۷۰ .

۱۲. عرب مازاد، محمد؛ کابوس ویروس های کامپیوتری، انتشارات همراه، چاپ اول، سال ۱۳۷۴، ص۳۹.

۱۳. فضلی، مهدی (۱۳۸۳)، مسؤلیت کیفری در فضای سایبر، انتشارات خرسندی، تهران.

۱۴. فهیمی، مهدی ؛ جرم رایانه ای و روش های پیشگیری از آن (مقاله)، پایگاه اینترنتی پژوهشگاه اطلاعات و مدارک علمی ایران ص ۶۵.

۱۵. فهیمی، مهدی، جرائم رایانه ای و روش های مقابله و پیشگیری از آن، فصلنامه دیدگاه های حقوقی، دانشکده علوم قضائی و خدمات اداری شماره بیست و سوم و، ۱۳۸۰، صص ۲۳و۲۴.

۱۶. گاتن، آلن ام؛ ادله الکترونیکی، (ترجمه مصیب رمضانی)، تهران: انتشارات دبیرخانه شورای عالی اطلاع رسانی کشور، چاپ اول، سال ۱۳۸۳، ص۳۸.

۱۷. مقدسی، حمید و عیانی، شیرین (۱۳۹۲)، امنیت دادهها در سیستمهای اطلاعات سلامت، فصلنامه پژوهشهای حفاظتی ـ امنیتی دانشگاه جامع امام حسین (ع)، ش۲.

۱۸. نشریه بین المللی سیاسات جنایی، دبیر خانه شورای عالی انفورماتیک، شماره های ۴۳ و ۴۴، ص۲۳.

19. Arkin s. Prevention and Prosecution of computer and hiy tecnology crime.p1989

20. Code de procedure penale de france L'article-5

21. Padova, Yann , Un apercu de la lutte contre la cybercriminalite en France , Revue de science .2002, criminelle

22. règle de la double incrimination. Padova, Yann, Un apercu de la lutte contre la cybercriminalite en France , Revue de science .2002, criminelle

23. http://www.dalloz.fr/PopupDocumentPrint?famille-id=REVUES&produit-id=RSC&c...

مطالعات علوم سیاسی، حقوق و فقه

دوره ۱۱، شماره ۲، تابستان ۱۴۰۴، صفحات ۳۵۱-۳۳۴

Comparative Study of Cyberspace Crimes in Iranian and French Law

Abdolhossein Sobhanpour, Ehsan Azizi[2]

1-Master's student, Department of Criminal Law and Criminology, Noorabad Mamasani Branch, Islamic Azad University, Noorabad Mamasani, Iran.

3- Faculty of the Department of Private Law, Noorabad Mamasani Branch, Islamic Azad University, Noorabad Mamasani, Iran.

Abstract

The evolution of information and the increasing use of computers and the Internet in all aspects of human life and the need for it by companies, organizations, and groups has led to the occurrence of various crimes in cyberspace. Cyberspace, with its characteristics such as transnationality, multiplicity of actors, and secrecy, has caused individuals to enter this space and commit various crimes without being easily identified. In this cyberspace, however, real and genuine crimes such as theft, fraud, forgery, and espionage occur. Some of these crimes cause harm and damage to society and are considered a threat to data security. Some of these crimes cause financial and economic damage, and some are threats and harm to individuals. Cybercrime is an undeniable issue in the criminal policy of countries, and for this reason, governments are trying to combat such crimes. Data security in every country is one of the concerns of governments that are trying to ensure internal and external security. For this reason, in order to combat unauthorized access to data and crimes that occur through electronic means and in an advanced manner, regulations and laws were enacted by the legislator to block the way for profit-seeking individuals and to provide data security.

Keywords: Criminal Protection, Security, Data Security, Cybercrime, Cyberspace.