دو فصل نامه علمی ـ اختصاصی فقه و حقوق معاصر

سال چهارم، شماره هفتم، بهار و تابستان ۱۳۹۸

صفحات٤٨ تا ٦٦

جرایم علیه اموال و جرایم علیه عفت عمومی با توصیف سایبری

رضا پورمحمدی[۱]

چکیده

در کنار تأثیرات مثبتی که رایانه و فضای مجازی در زندگی انسان ها می گذارد تعدادی از افراد سودجو و فرصت طلب با سوء استفاده از عدم آگاهی مردم نسبت به فضای مجازی اقدام به انجام اعمال مجرمانه و ایراد خسارت های مادی و معنوی به بزه دیدگان نموده اند. فضای سایبر فضایی غیرمادی و ناملموس است که توسط رایانه هاو شبکه های رایانه ای به وجود آمده و دنیای مجازی را در کنار دنیای واقعی ما به وجود آورده است. بنابراین فضای سایبر همان فضای مجازی و بیکران است که از طریق اتصال شبکه های رایانه ای به هم به وجود آمده است. ذات مخفی و پوشیده فضای سایبر و حس ناشناخته ماندن ناشی از فضایی که چنین ابزاری در اختیار افراد می گذارد به همراه لذتی که تازی در پهنه وسیعی که فارغ از هرگونه مرز و محدوده ای است محیط ناملموس اما واقعی این فضا را بعضاً با هرج و مرج و ویرانگری مواجه می سازد. از همین روست که به موازات پیدایش فضای سایبر ، دسته نوینی از جرایم که به جرایم سایبری

---

[۱] – طلبه سطح ٤ مرکز تخصصی فقه و اصول، حوزه علمیه، قم؛ دانشجوی دکتری حقوق خصوصی دانشگاه شهید بهشتی، تهران.

شهره گشته اند نمود یافته است که نیازمند بررسی و تدقیق می باشد و علاوه بر آن امکان وقوع سایر جرایم هم به صورت اینترنتی حائز اهمیت می باشد.

کلمات کلیدی: جرایم سایبری، جرایم علیه اموال و مالکیت، جرایم علیه امنیت و آسایش عمومی.

مقدمه

انسان به عنوان اشرف مخلوقات با استفاده از مزیت و برتری خود نسبت به حیوانات که همانا عقل او می باشد زندگی را روز به روز برای خود آسان و آسان تر می کند. نمونه ی بارز آن اختراع ماشین بخار به وسیله ی انسان بود که باعث تحول عظیمی در کلیه ی مراحل زندگی اجتماعی گردید و از آنجایی که نفس و روح انسان سیری ناپذیر است به تلاش خود هم چنان ادامه می دهد.حاصل این تلاش ها را در چند دهه ی اخیر می توان در اختراع رایانه عنوان نمود. اختراعی که ابعاد وسیعی از زندگی، حکومت، سیاست و اقتصاد را تحت تأثیر قرار داد و به زعم برخی مهم تراز انقلاب صنعتی بود که در قرن هیجدهم در اروپا به وقوع پیوست. اما همان گونه که پیش تر بیان گردید انسان همیشه از نیروی تفکّر و تعقّل خود در مسیر مثبت استفاده نمی نماید بلکه برای رسیدن به کمال ظاهری از هر گونه ترفند و حیله استفاده می کند که تکنولوژی پیشرفته رایانه این راه را آسان تر نموده است، لذا رایانه با تمام ویژگی ها و خصوصیات مثبتش ویژگی های منفی بسیاری نیز دارد و بدین ترتیب زمینه ی ارتکاب جرم آسان تری را برای مجرمان فراهم می آورد.

در مقابل تکنولوژی رایانه و اطلاعات موجب پیدایش و تکوین رشته ها و دکترین های جدیدی هم چون حقوق رایانه ،حقوق اطلاعات و حقوق

اطلاعات کیفری شده است و هم چنین استفاده نامطلوب و غیر قانونی از این پدیده متخصصان و علمای حقوق جزارا بر آن داشته است که به کنکاش و تفحص در این زمینه پرداخته است.

با توجه به افزایش چشم گیر کاربرد رایانه در هزاره ی سوم و همچنین افزایش جرایم سایبری در عصر حاضر بسیاری از مردم با این مسأله مواجه شده اند که جرایم سایبری چگونه به وقوع می پیوندند. ما در این نوشتار، این موضوع را در مورد جرایم علیه اموال و مالکیت و جرایم علیه اخلاق و عفت عمومی و جرائم علیه امنیت و آسایش عمومی انجام خواهیم داد.

بنا به این علت که تعریف جرایم سایبری در نوشتار دیگری گذشته است در این مقاله از آوردن آن مطالب اجتناب می شود و برای مطالعه به آن مقاله[1] ارجاع داده می شود، در این مقاله مطلب از توضیح مصادیق جرایم شروع خواهد شد.

۱- جرایم علیه اموال و مالکیت

یکی از تقسیم بندی های جرایم در حقوق موضوعه، جرایم علیه اموال و مالکیت می باشد. هدف از پیش بینی چنین جرایمی، حمایت از اموال دیگران در مقابل تعدی افراد است. حال این تعدی و تجاوز به چه نحوی صورت گیرد تأثیری در حکم ندارد؛ یعنی تعدی چه به روش سنتی انجام گیرد و چه به طریق دیگر (از جمله از طریق رایانه) مشمول حمایت قانون می باشد.

[1] – عباسیان، پیمان و رحیق اغصان، حسن، بررسی وقوع جرایم علیه اشخاص با توصیف سایبری، همایش منطقه ای پژوهش های کاربردی در علوم انسانی و علوم اسلامی، ۱۳۹۸.

جرایم علیه اموال متنوع اند ولی ما در این مبحث سه نوع جرمی که بیشتر رایج اند و قابلیت ارتکاب از طریق رایانه را دارند، بررسی می کنیم. این جرایم عبارتند از: کلاهبرداری رایانه ای، سرقت رایانه ای و تخریب رایانه ای.

۱-۱- کلاهبرداری رایانه ای

کلاهبرداری، یکی از جرایم علیه اموال و مالکیت است که بعد از تکوین و تکامل سیستم های کامپیوتری یکی از مطرحترین و مهمترین اشکال جرایم اقتصادی در فضای سایبر به شکل کلاهبرداری کامپیوتری بروز کرده است.

مجرم در این جرم اموال دیگری را از طریق برنامه سازی کذب، تغییر داده ها، سوء استفاده از سیستم کامپیوتری و... تصاحب می کند. این جرم از لحاظ ساختاری با جرم کلاهبرداری کلاسیک متفاوت است، زیرا موضوع کلاهبرداری رایانه ای، داده ها به عنوان نماینده اموال مادی در سیستم های پردازش داده هاست. در اکثر پرونده های کلاهبرداری کامپیوتری اموالی که داده های کامپیوتری نماینده آن هاست غیر مادی اند مانند سپرده ها، مطالبات، زمان کار، ارزش اعتبارات و نتایج محاسبات ترازنامه ها.(اواریش، ۱۳۸۳، ص۲۰)

کلاهبرداری رایانه ای در زمره جرایم نسل اول رایانه ای است. در این نسل رایانه صرفاً وسیله ارتکاب جرم تلقی می شود و بنابراین می توان کلاهبرداری رایانه ای را یکی از اولین جرایم رایانه ای پس از دخالت بی چون و چرای رایانه در فعالیت های روزمره زندگی بشر دانست.(عالی پور، ۱۳۸۳، ص۲۱۲)

در قوانین فعلی ایران از جرم کلاهبرداری تعریفی ارایه نشده و مثل برخی جرایم فقط به ذکر مصادیق اکتفا شده است. این مصادیق در ماده اول

قانون تشدید مجازات مرتکبین ارتشا و اختلاس و کلاهبرداری (مصوب ۱۳٦٤/٦/۲۸ مجلس شورای اسلامی و تأیید مجمع تشخیص مصلحت نظام در مورخه ۹/۱۵/ ۱۳٦۷)، بیان شده است. با توجه به قانون مذکور یکی از اساتید حقوق جزا کلاهبرداری را چنین تعریف کرده است :

کلاهبرداری عبارت است از بردن مال دیگری از طریق توسل توأم با سوء نیت به وسایل یا عملیات متقلبانه.

همچنین در تعریف دیگر آمده است:« بردن مال غیر با توسل به وسایل متقلبانه یا بردن متقلبانه مال غیر»

در حقوق کیفری ایران قبل از سال ۱۳۸۲ بحثی از کلاهبرداری رایانه ای نشده بود تا این که در سال ۱۳۸۲ که قانون تجارت الکترونیکی تصویب شد، قانون گذار در ماده ٦۷ این قانون بدون این که به تعریف کلاهبرداری رایانه ای بپردازد به ذکر مصادیق آن پرداخت. یکی از حقوق دانان با توجه به ماده ٦۷ قانون تجارت الکترونیکی جرم کلاهبرداری رایانه ای را این طور تعریف کرده است :

کلاهبرداری رایانه ای عبارت است از تحصیل مال غیر با استفاده متقلبانه از رایانه.

به نظر می رسد، این تعریف بهترین و مختصرترین تعریف برای کلاهبرداری رایانه ای است.

در نتیجه کلاهبرداری رایانه ای که یکی از شایع ترین جرم رایانه ای می باشد، برخلاف سایر جرایم در قوانین ما (قانون تجارت الکترونیکی) به رسمیت

شناخته شده است، ولی با این همه محدوده آن فقط در مبادلات الکترونیکی می باشد و علاوه بر آن عنصر مادی مشخص و دقیقی ندارد. همچنین در برخی موارد از قوانین کلاهبرداری سنتی کمک گرفت، ولی به دلیل مجازات اندک این جرم و اصولاً کم اهمیت بودن عنوان مجرمانه که تحصیل مال از طریق نامشروع را یدک می کشد، از حیث روان شناسی مرتکبان را گستاخ در سوءاستفاده های رایانه ای می کند و نمی تواند یک سیاست جنایی مناسب برای مبارزه با کلاهبرداری رایانه ای باشد.

۱-۲- سرقت رایانه ای

قانون مجازات اسلامی سرقت را این طور تعریف کرده است: ربودن مال دیگری به طور پنهانی. این تعریف بیشتر در مورد سرقتی است که در عالم فیزیکی اتفاق می افتد. در مورد تعریف و مفهوم سرقت رایانه ای اختلاف وجود دارد که آیا تعریف سرقت عمومی هم در این جا قابل اعمال است؟ در قوانین موجود به صراحت بحثی از سرقت رایانه ای نشده است، ولی با توجه به نظر متخصصان این رشته و با توجه به قوانین ملی و بین المللی موجود می توان گفت: آن چه موضوع سرقت رایانه ای است، اطلاعات (داده) پول، مال (سخت افزار و نرم افزار) و سرقت خدمات می باشد که به نظر می رسد محدوده چنین سرقتی از سرقت عمومی وسیع تر می باشد، چرا که اطلاعات و داده هایی را که جنبه مالی هم ندارند نیز در بر می گیرد؛ مثل این که شخصی رمز عابر بانکی را بدزدد، یا این که اطلاعات سری کد شده و رمزدار را از شبکه رایانه ای برباید.

ولی به نظر می رسد که چنین عقیده ای درست نیست، چون نظر فقها با چنین عقیده ای مغایرت دارد، زیرا فقها یکی از عناصر اصلی سرقت را« مال » می دانند و برای چیزی که مالیت نداشته باشد عنوان سرقت قایل نیستند، هر چند

ممکن است از جهات دیگری عنوان مجرمانه پیدا کند. البته منظور از مالیت داشتن، رواج داشتن و مالیت داشتن آن در بازار نیست، بلکه ممکن است چنین داده هایی برای اشخاص دیگر فاقد ارزش اقتصادی باشد، ولی برای برخی ارزش داشته باشد و شرع و عرف دادن مال در مقابل آن را مذموم نشمارد (متقوم نسبی).

ولی به نظر می رسد شرط دانستن « مالیت » در بحث سرقت رایانه ای درست نباشد، زیرا سبب می شود برخی موارد که مالی نیستند، ولی از جهات دیگر مهم تلقی می شوند، از محدوده قانون جزا خارج شوند. نکته قابل توجه این است که ما در مقام بیان مفهوم سرقت رایانه ای هستیم نه سرقت عمومی، که مالیت در آن شرط است و هر کدام برای خود مفهوم مستقلی دارند.

نکته دیگر در بحث تعریف سرقت رایانه ای این است که آیا پنهانی بودن مانند سرقت سنتی شرط می باشد یا خیر؟ به نظر می رسد که در سرقت رایانه ای هم پنهانی بودن شرط لازم است، زیرا اگر پنهانی بودن شرط نباشد موضوع جرم سرقت منتفی است، اعم از این که سرقت عمومی باشد یا رایانه ای. البته در سرقت رایانه ای، فعالیت های رایانه ای غالباً پنهان است، زیرا نمی توان محیط مجازی را همانند محیط فیزیکی زیر نظر داشت.

بحث دیگر این است که پنهانی بودن سرقت را در چه محلی ملاک قرار بدهیم: محلی که جرم واقع شده یا محلی که داده ها از آن جا برداشته می شود؟ در سرقت سنتی، محل وقوع مال ملاک عمل است، ولی در سرقت رایانه ای تعیین محل وقوع جرم به این راحتی نیست و در برخی موارد حتی امکان ناپذیر است. به نظر می رسد که ملاک همان محلی است که مجرم فعالیت های مجرمانه اش را در آن جا انجام می دهد. در این امر هم مسئله دیگری پیش می آید اگر

همراه مجرم چند نفر حاضر باشند و مجرم فعالیت های خویش را در رایانه انجام دهد آیا می توان گفت که عمل پنهانی است؟ در صورتی که همراهان اطلاع یابند که شخص مشغول انجام جرم است شاید بتوان گفت عمل پنهانی نیست، ولی در موردی که همراهان از فعالیت های مجرمانه مرتکب اطلاع نداشته باشند بعید است بگوییم فعالیت های مرتکب پنهانی نبوده است، زیرا در این صورت به نظر می رسد ربوده شدن داده ها و اطلاعات در محیط مجازی متوجه این عمل شود.

از لحاظ رکن مادی باید گفت که ربایش، نخستین پایه اساسی جرم سرقت را تشکیل می دهد و شامل دو مرحله است: وضع ید بر مال یا شیء متعلق به غیر و بیرون بردن از سلطه مالک یا متصرف. حال اگر داده ها در فضای مجازی به معرض نمایش گذاشته شود، ولی امکان کپی کردن اطلاعات از کاربران سلب شود و شخصی بتواند از اطلاعات غیر قابل کپی، کپی بگیرد آیا مرتکب سرقت اطلاعات شده است، در حالی که اصل اطلاعات از دسترس مالک خارج نشده است؟ این در صورتی است که در سرقت سنتی مال باید از دسترس مالک خارج شده باشد. با توجه به این که ارایه دهنده اطلاعات رضایت به کپی نداده است شاید بتوان گفت که سرقت محقق می شود، ولی باز هم مسئله قابل تأمل است و شاید عنوان مجرمانه دیگری به خود بگیرد.

نکته مهم دیگر در بحث عنصر مادی، امکان تحقق هتک حرز در بحث سرقت حدی است که آیا در سرقت رایانه ای قابل تصور است؟ حرز طبق تبصره یک ماده ۲۶۹ قانون مجازات اسلامی عبارت است از محل نگهداری مال به منظور حفظ از دست برد. با توجه به این که انواع حرز در شرع و در قانون محدود نشده است، باید برای تشخیص آن به عرف مراجعه کرد که عرف چه

جایی را محل نگهداری مال می داند. بدیهی است قضاوت عرف نسبت به این مسئله با توجه به زمان و مکان و نیز در مورد اشخاص مختلف فرق می کند.

حال سؤال این است که آیا رایانه می تواند حرز اطلاعات باشد؟ یا این که نه، اگر رایانه به سیستم امنیتی مجهز شده باشد می توان گفت که حرز محسوب می شود؟ اگر به عرف مراجعه کنیم راجع به اطلاعاتی که در فضای سایبر ارایه می شود شکی نیست که رایانه را حرز اطلاعات به شمار می آورد.

۱-۳- تخریب رایانه ای

تخریب عبارت است از لطمه زدن عمومی به مال متعلق به غیر. این تعریف را می توان در مورد تخریب رایانه ای نیز قابل اعمال دانست، زیرا خصوصیتی در تخریب رایانه ای وجود ندارد تا آن را از تعریف تخریب سنتی متمایز سازد. جرم تخریب رایانه ای همانند سابوتاژ رایانه ای است با این تفاوت که در جرم سابوتاژ، مرتکب با قصد معارضه با نظام و اخلال در نظم عمومی به شکل وسیع اقدام به اختلال در سیستم ها و برنامه های رایانه ای میکند؛ هدف، وسعت مورد نظر مجرم، موضوع مورد نظر وی و روش به کار گرفته شده، نشانه سابوتاژ رایانه ای است. اما در تخریب رایانه ای اولاً و بالذات هدف اخلال در نظم سیاسی و اجتماعی نیست و ثانیاً و بالعرض اعمال مجرم رویکرد مالی دارد و سازمان دولتی یا یکی از نهادهای دولتی مدنظر مجرم نیست.

عنصر مادی تخریب رایانه ای همانند جرم تخریب سنتی است و با توجه به تقسیم اینترپل شامل دو قسم است: ۱. تخریب نرم افزار؛ ۲. تخریب سخت افزار.

مورد اول به این شکل صورت می گیرد که شخصی نرم افزار متعلق به دیگری را که حاوی اطلاعات و برنامه هاست از بین ببرد. مثلاً بشکند یا بسوزاند و یا خسارتی وارد کند که در حکم تلف قرار بگیرد. تطبیق این مورد با مقررات تخریب سنتی کاملاً هماهنگ است. البته گفتنی است که تخریب نرم افزار از طریق رایانه و فضای مجازی نیز قابل تصور است؛ مثلاً شخصی با ارسال برنامه مخربی مثل ویروس، به رایانه دیگر که در حال استفاده کردن از نرم افزار می باشد، آن را عامدانه و با سوءنیت از بین ببرد.

اما تخریب سخت افزار به دو طریق صورت می گیرد: از طریق رایانه و از طریق غیر رایانه. در تخریب از طریق رایانه مثلاً شخصی با ارسال ویروسی به رایانه دیگری هارد کامپیوتر او را از بین می برد یا سبب می شود بسوزد و تخریب از طریق غیر رایانه و در عالم واقعی این است که با ضربه ای کامپیوتر یا CPU که مانیتور یا اجزای کامپیوتر دیگری را از بین ببرد. البته – همان طور که بیان شد – این مورد بیشتر تخریب سنتی است تا رایانه ای . عمل فیزیکی در عنصر مادی معمولاً به شکل فعل مثبت ارتکاب می یابد، ولی تصور تحقق این جرم با ترک فعل، هر چند بعید به نظر می رسد، لیکن ممکن است. مثلاً شخصی که سیستم امنیت رایانه ها را بر عهده داشته و موظف بوده است که در موارد مشاهده ویروس یا برنامه های مخرب دیگر، مانع از بروز خسارت و یا ورود ویروس به رایانه های دیگر بشود، عمداً به وظیفه خود عمل نمی کند تا این که ویروس مذکور یکی از اجزای رایانه را از بین ببرد. البته در این جا باید دو مسئله را از هم تفکیک کرد: در موردی که شخص ویروسی را عمداً به قصد تخریب فرستاده است و شخص مأمور هم عامداً ترک فعل کرده است؛ در این جا مسئولیت به مانند اجتماع سبب و مباشر است که مباشر مسئول می باشد و سبب به عنوان معاون مسئول می باشد، زیرا وقوع جرم را تسهیل کرده است. ولی در

موردی که شخص فرستنده ویروس قصد تخریب نداشته، اما تارک فعل چنین قصدی داشته، در این جا سبب اقوا از از مباشر می باشد و شخصی که سیستم امنیت رایانه ها را بر عهده داشته مسئول تلقی می شود.

جرم تخریب رایانه ای همانند تخریب سنتی، از جمله جرایم عمدی است. سوء نیت عام، عمد در خراب کردن و لطمه زدن به مال می باشد و سوء نیت خاص، قصد ضرر زدن به دیگری است. علاوه بر این ها مرتکب باید عالم باشد که مال متعلق به دیگری است. البته برخی معتقدند که قصد اضرار به عنوان سوء نیت خاص در این جرم لازم نیست، بلکه قصد اضرار جزو ارکان اصلی این جرایم است و بنابراین می توان آن را در سوء نیت عام به حساب آورد.

با توجه به توضیحاتی که داده شد تخریب رایانه ای قابل تصور و تحقق است و با قوانین سنتی هم قابلیت انطباق دارد.

۲- جرایم علیه اخلاق و عفت عمومی

جرایم علیه اخلاق و عفت عمومی عبارت است از هر نوع عمل، رفتار و گفتاری که برخلاف عفت و پاکدامنی جامعه باشد. این جرایم متنوع و متعددند: برخی از آن ها از جمله جرایم حدی می باشند، مثل زنا، لواط و قوادی و بعضی تعزیری هستند، مثل روابط نامشروع مادون حد و عرضه و خرید و فروش صور قبیحه. وقوع برخی از این جرایم (اعم از حدی و تعزیری) با ظهور اینترنت از محیط فیزیکی به محیط مجازی انتقال یافته است؛ ولی در برخی از آن ها رایانه و اینترنت نمی تواند به عنوان واسطه ارتکاب جرم شود، مثل زنا و لواط، چرا که در وقوع چنین جرایمی حضور فیزیکی افراد شرط است.

ما در این قسمت به بررسی قسم اول جرایم که اینترنت در آن ها به عنوان واسطه نقش به سزایی دارد می پردازیم. مهم ترین و شایع ترین این جرایم عبارتند از پورنوگرافی، قیادت (قوادی) و روابط نامشروع.

۲-۱- پورنو گرافی[۱]

پورنوگرافی یا هرزه نگاری یکی از جرایم مرتبط با محتواست که در تقسیم بندی حقوق موضوعه، یکی از جرایم علیه اخلاق و عفت عمومی شمرده می شود. پورنوگرافی در مفهوم عام به معنای مطالبی است که عمدتاً به قصد تحریک جنسی ارایه می شود.

هرزه نگاری در فضای سایبر از سه جنبه، تهدیدی جدی محسوب می شود: اولین تهدید آن است که امکان دارد کودکان به هرزه نگاری وقیحانه در اینترنت دسترسی پیدا کنند. دومین تهدید آن است که هرزه نگارها، هرزه نگاری کودکان را راه آسانی برای فروش محصولات خود یافته اند، به این دلیل که باعث شده سوء استفاده جنسی از کودکان تا این حد رواج یابد و سومین و بزرگ ترین تهدید برای کودکان آن است که بچه بازها و افراد خطرناک دیگر می توانند از طریق اینترنت و به واسطه مکاتبه، ایمیل یا گپ زدن قربانیان خود را جذب کنند و آن ها را در دنیای واقعی به دام بیندازند.

در قوانین داخلی ایران، اولاً، اصطلاحی به نام پورنوگرافی وجود ندارد. ثانیاً، در مورد جرایم رایانه ای مشکل عنصر قانونی تا به حال حل نشده است که پورنوگرافی غیر مجاز رایانه ای جزو آن هاست. ولی قوانینی وجود دارد که می توان گفت پورنوگرافی در ایران جرم است (البته بدون این که محدود به فضای سایبر شده باشد). از جمله قانون نحوه مجازات اشخاصی که در امور سمعی و

۱- pornography

بصری فعالیت های غیر مجاز کنند (مصوب ۱۳۷۳/۱۱/۲٤) و قانون مجازات اسلامی، به جرم انگاری تهیه و توزیع تصویرها و فیلم های پورنوگرافی پرداخته اند.

۲-۲- قیادت (قوادی)

قیادت یا واسطه گری در اصطلاح عبارت است از به هم رساندن دو نفر برای انجام اعمال منافی عفت. قیادت از مصادیق بارز و آشکار کمک و یاری در گناه و معصیت است، که به همین جهت در شرع از آن نهی شده و تحریم گردیده است و احادیث در مذمت آن بسیار است؛ از جمله در حدیث ابراهیم بن زیاد کرخی آمده است:

سمعت اباعبدالله (ع) یقول: لعن رسول الله (ص) الواصله و المستوصله – یعنی الزانیه و القواده؛ شنیدم امام صادق (ع) فرمودند: رسول خدا (ص) واصله و مستوصله یعنی زناکار و جاکش را لعنت کرده است.

ما در این جا به دنبال بحث تفصیلی جرم قیادت نیستیم و فقط می خواهیم به این موضوع بپردازیم که آیا قیادت از طریق رایانه قابل ارتکاب است یا خیر؟

در قوانین ملی و بین المللی مربوط به جرایم رایانه ای به صراحت یا ضمنی به این جرم اشاره ای نشده است، در حالی که با پیشرفت جوامع و دسترسی همگانی به ابزارها و امکانات گوناگون به ویژه فن آوری ارتباطات قوادی که در قدیم به صورت یک جرم ساده و جزیی بود، امروزه به یک بحران بزرگ اجتماعی تبدیل شده و در سایه همین امکانات و گستردگی جوامع است

که اکنون قوادی را در شکل قاچاق انسان به صورت سازمان یافته حتی در عرصه بین المللی ملاحظه می کنیم.

البته از ماده سوم پروتکل الحاقی به کنوانسیون پالرمو سال ۲۰۰۰ که در مقام بیان تعریف قاچاق اشخاص است تا حدودی می توان قوادی را استنباط کرد.

در این راستا، در کشورمان بند« الف » ماده اول قانون مبارزه با قاچاق انسان (مصوب ۱۳۸۳) بیان می دارد :

قاچاق انسان عبارت است از: الف) خارج یا وارد ساختن و یا ترانزیت مجاز یا غیر مجاز فرد یا افراد از مرزهای کشور با اجبار و اکراه یا تهدید یا خدعه و نیرنگ و یا با سوء استفاده از قدرت یا موقعیت خود یا سوء استفاده از وضعیت فرد یا افراد یاد شده، به قصد فحشا یا برداشت اعضا و جوارح، بردگی و ازدواج.

در این ماده قصد فحشا اطلاق دارد و شامل قوادی نیز می شود. در نتیجه می توان گفت که قوادی از طریق رایانه قابل تحقق است و از نظر فقهی تفاوتی با قوادی سنتی نداشته و از نظر حقوقی با قانون مجازات اسلامی و قانون مبارزه با قاچاق انسان و ... منطبق می باشد.

۲-۳- روابط نامشروع

یکی دیگر از جرایم سنتی علیه اخلاق و عفت عمومی که قابلیت ارتکاب در فضای مجازی یا از طریق رایانه را دارد، روابط نامشروع است. رابطه نامشروع چیست و چه مفهومی دارد؟ و نحوه تحقق آن در فضای مجازی به چه شکلی است؟

در قوانین جزایی ایران از رابطه نامشروع تعریفی ارایه نشده است و فقط قانون مجازات اسلامی در ماده ٦٣٧ در این مورد بیان می دارد:

هر گاه زن و مردی که بین آن ها علقه زوجیت نباشد، مرتکب روابط نامشروع یا عمل منافی عفت غیر از زنا از قبیل تقبیل یا مضاجعه شوند به شلاق تا ۹۹ ضربه محکوم خواهند شد و اگر عمل منافی با عفت و اکراه باشد فقط اکراه کننده تعزیر می شود.

این ماده تنها عنصر قانونی روابط نامشروع غیر از عمل منافی عفت در حقوق سنتی است.

روابط نامشروع هم با توجه به این که از نظر فقهی و حقوقی منحصر به رابطه فیزیکی نیست، در فضای سایبر قابلیت تحقق دارد. به عبارتی همان طور که افراد می توانند در عالم فیزیکی با هم ارتباط نامشروع داشته باشند، می توانند از طریق فضای مجازی نیز این رابطه را داشته باشند، زیرا آن چه ملاک رابطه نامشروع است، فساد و فتنه است نه وسیله.

نتیجه گیری

کوتاه سخن اینکه در دنیای امروز رایانه از لوازم و ضروریات نوع بشر برای تسهیل امور روزمره مبدل شده است، به ویژه فن آوری اینترنت که بیشترین فراوانی استفاده ها و کاربردها در آن صورت می گیرد، خدماتی مانند بانک ها، ادارات و پیشخوان ها برای تسریع در انجام امور به کاربران ارائه می دهند و مورد استفاده های بسیاری که ذکر آن در این مجال نمی گنجد. اما همانطور که پیش تر هم ذکر شد روی دیگر این خدمات سوء استفاده هایی است که از سوی افراد حقیقی و حقوقی و البته در برخی موارد از سوی بعضی دولت ها که عموماً

از سوی سرویس های اطلاعاتی آن هاست، رخ می دهد. که این جرایم هر کدام به نوبه خود در برابر کاربران خاص خود شکل می گیرد، برای مثال دولت ها برای پیشبرد منافع و اهداف خود در یکی از این تخلفات از ویروس هایی به قصد اخلال و تخریب به سامانه مورد نظر خود هجوم می برند مانند ویروس استاکس نت از سوی برخی سرویس های اطلاعاتی کشورهای غربی به قصد از بین بردن اطلاعات هسته ای جمهوری اسلامی ایران.

آنچه که از این پژوهش حاصل گشت بدین شرح است:

جرم در فضای مجازی و سایبری قابل تحقق است و ما جرم سایبری داریم.

با غلبه اینترنت بر زندگی روزانه ی انسان ها طبیعی به نظر می رسد که بسیاری از مشخصه های جامعه سنتی به درون اینترنت کشیده شوند و در آنجا شکل گیرند. امروزه، امور زیادی از قبیل خرید و فروش، تحصیل، مشاوره خانوادگی، ازدواج و حتی مشاوره های پزشکی میان پزشکان و بیماران در اینترنت انجام می گیرد. از این رو هیچ جای تعجبی نیست که مجرمان اینترنتی در فضای مجازی مرتکب جرم شوند. به خصوص گمنامی این فضا بر گسترش این نوع جرایم دامن می زند، در این فضا کمتر هویت واقعی مشخص می شود و افراد با کتمان هویت خویش به راحتی مرتکب انواع جرایم می شوند. در نتیجه این فضا با امکاناتی که در اختیار مجرمان قرار می دهد از یک سو ارتکاب جرایم را سهل تر می سازد و نسبت به دنیای فیزیکی خسارت بیشتری را وارد می کند و از سوی دیگر به لحاظ فراملی بودن آن و امکان ارتکاب جرم بدون نیاز به حضور فیزیکی مجرمان، تعقیب و پیگیرد و در نهایت دستگیری آن ها با مشکلات زیادی همراه خواهد شد.

منابع

۱. احمد الشوابکه، محمد امین، جرایم الحاسوب و الإینترنت، الطبعه الاولی، دارالثقافه، عمان، ۲۰۰٤م.

۲. اولریش، زیبر، جرایم رایانه ای، ترجمه محمد علی نوری، رضا نخجوانی، مصطفی بختیاروند و احمد رحیمی مقدم، چاپ اول، انتشارات گنج دانش، تهران، ۱۳۸۳.

۳. بداغی، سعید، بررسی فقهی و حقوقی جرایم در عالم مجازی(سایبری)، پایان نامه کارشناسی ارشد دانشگاه مازندران، ۱۳۹۱.

٤. جینادی، آنجلیز، جرایم سایبر، ترجمه سعید حافظی و عبدالصمد خرم آبادی، شورای عالی و توسعه قضایی، تهران، ۱۳۸۲.

۵. حبیب زاده، محمد جعفر، حقوق جزای اختصاصی (جرایم علیه اموال)، چاپ سوم، انتشارات سمت، ۱۳۸۰.

٦. حر عاملی، محمد حسن، وسائل الشیعه، چاپ دوم، نشر مؤسسه آل بیت، قم، ١٤١٤ ق.

۷. دزیانی، حسین، گزارش توجیهی جرایم کامپوتری (مقررات لازم در حقوق جزای ماهوی)، ج۲، پیوست فصل چهارم شورای عالی انفورماتیک، ۱۳۸۱.

۸. زراعت، عباس، شرح قانون مجازات اسلامی (حقوق جزای عمومی)، چاپ اول، نشر ققنوس، تهران، ۱۳۷۹.

۹. شامبیانی، هوشنگ، حقوق کیفری اختصاصی، ج ۱، چاپ سوم، انتشارات ویستار، ۱۳۷٦.

۱۰. عالی پور، حسن، کلاهبرداری رایانه ای، مجله پژوهش های حقوقی، ۱۳۸۳ ، شماره ٦.

۱۱. عباسیان، پیمان و رحیق اغصان، حسن، بررسی وقوع جرایم علیه اشخاص با توصیف سایبری، همایش منطقه ای پژوهش های کاربردی در علوم انسانی و علوم اسلامی، ۱۳۹۸.

۱۲. گلدوزیان، ایرج ، حقوق جزای خصوصی، چاپ یازدهم، دانشگاه تهران، ۱۳۸٤.

۱۳. مرهج الهیتی، محمد حماد، التکنولوجیا الحدیثه، الطبعه الاولی، دارالثقافه، عمان، ۲۰۰٤ م.

۱٤. میرمحمدصادقی، حسین، جرایم علیه اموال و مالکیت، چاپ دوازدهم، نشر میزان، تهران، ۱۳۸٤.

۱۵. ولیدی، محمد صالح، حقوق جزای اختصاصی (جرایم علیه اموال و مالکیت)، چاپ پنجم، انتشارات امیرکبیر، نشرداد، ۱۳۷٦.