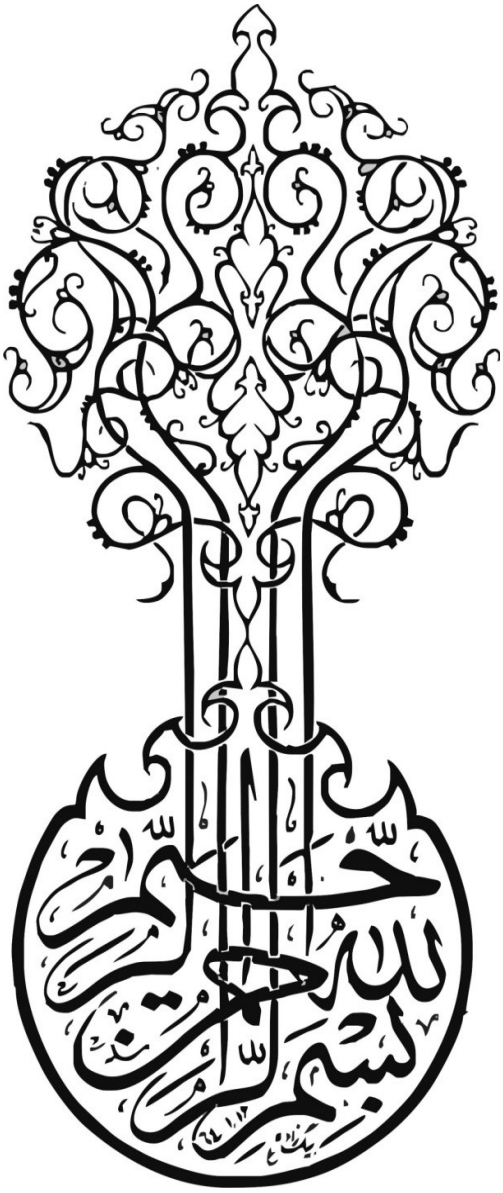
بسم الله الرحمن الرحيم

نگرش حقوقی بر فضای مجازی

فرصت ها، تهدید ها و تدابیر

اداره کل امور حقوقی،املاک وقراردادها و رسیدگی به شکایات

زمستان ۱۳۹۸

فهرست مطالب

عنوان	صفحه

چکیده

فضای مجازی مانند دنیای واقعی ویژگی های یک جامعه را دارا است و این امر سبب شده است که فضای مجازی به مهم ترین و قوی ترین عامل نفوذ و تأثیر در جامعه تبدیل شود. شکل گیری شبکه های مجازی در عین ایجاد فرصت های مثبت و سازنده می تواند نقشی اساسی و مؤثری در بروز جرایم بالاخص جرایم امنیتی ایفا کند . جرایم ارتکابی در شبکه های مجازی چالش های جدی برای مدل سنتی حقوق کیفری ایجاد کرده است به نحوی که حقوق کیفری کنونی کارایی کافی و لازم در مواجهه با مشکلات حادث در این فضا را نخواهد داشت. با توجه به گسترش شبکه های مجازی و ویژگی های خاص آن و قابلیت ارتکاب جرایم در شبکه های مجازی، استفاده از شیوه های نوین جهت پیشگیری و مقابله با اینگونه جرایم را امری ضروری و اجتناب ناپذیر ساخته است .

نتیجه ها نشان می دهد علی رغم تلاش های صورت گرفته فضای مجازی هنوز محیطی کنترل نشده، نامنظم و بی قانون بوده که نیازمند اتخاذ تدابیر تقنینی، اجرایی و قضایی در این حوزه می باشد. به این نحو که با شناسایی، باز تعریف و تدوین قوانین (تدابیر تقنینی) و نظارت بر فضای مجازی، اقدامات امنیتی در حفاظت از سیستم ها و شبکه ها و نیز آموزش و آگاه سازی عموم جامعه(تدابیر اجرایی) و همچنین به کارگیری شیوه های نوین مواجهه و برخورد انتظامی و قضایی مناسب در راستای پیشگیری از جرایم امنیتی که در فضای مجازی رخ می دهد (تدابیر قضایی)، از گسترش روز افزون این دسته از جرایم کاست .

فصل اول

تعاریف، مفاهیم و تاریخچه

مقدمه

تحول و پیشرفت عظیم و شگرفی که امروز در دنیای علم و دانش فناوری شاهد هستیم، از چنان سرعتی برخوردار است که به صورت مستمر زیر ساخت های مهم جامعه را تحت تأثیر قرار داده و تغییرات عمده ای را در آن ایجاد می کند. فضای مجازی همانگونه که رویکرد نو و فضایی دوست داشتنی را برای ما به ارمغان آورده است، به تبع آن تهدیدهای این فضای نیز برای افراد و جامعه، جای تأمل دارد. فضای مجازی با توجه به قابلیت های بسیار زیاد همچون دقت بالا، سرعت زیاد، ذخیره سازی حجم زیاد، اطلاعات، خستگی ناپذیری، تبادل سریع اطلاعات، دسترسی آسان و محاسن بی شمار دیگر، امکانات زیادی را برای بشر به ارمغان آورده است، اما از منظر دیگر سبب بروز جرایم جدیدی شده است که قابل مقایسه با هیچ یک از جرایم کلاسیک موجود نبوده و چه بساکه خطر ناک تر باشد.[1]

در همه کشورها حقوق کیفری با مشکلات قابل ملاحظه ای در برخورد با جرایم در فضای مجازی مواجه است. در حال حاضر بدلیل گسترش تکنولوژی اطلاعاتی و کامپیوتری و اجزاء وابسته به آن در اکثر کشورها، مشکلاتی ناشی از جرایم فضای مجازی گریبان گیر تمامی این کشورها را بطور کم و بیش گشته است. زمینه مشترک همه این مسائل مربوط به تکنولوژی کامپیوتری، از این واقعیت ناشی می شود که در حال حاضر همه قوانین کیفری غالباً اشیاء ملموس و قابل روئیت را مورد حمایت قرار می دهند . حمایت از اطلاعات و سایر اشیاء ناملموس و غیر فیزیکی مورد حمایت قانونی عملاً تا اواسط قرن بیستم صورت نگرفته بود. به تدریج توسعه تکنولوژی و گذر از جوامع صنعتی به فرا صنعتی، افزایش ارزش اطلاعات نیز اهمیت روبه رشد تکنولوژی کامپیوتری منتهی به مشکلات جدیدی در زمینه حقوق اطلاعاتی شده است. در سالهای اخیرنتیجه تغییر الگوها از فیزیکی به غیر فیزیکی باعث شد تا حقوق کیفری در موارد گوناگون با الزام قانونگذار در موارد جرایم رایانه ای روبه رو شود. همچنین در زمینه آئین دادرسی کیفری نیز مسائلی مطرح شده است. جایگزینی ادله غیر قابل رؤیت و غیر ملموس در عرصه فضای سایبر به جای موضوعات ملموس و قابل رؤیت، مأمورین قضایی را با مشکلات عدیده ای در زمینه تحقیق، تفتیش و جمع آوری ادله لازم جهت

۱صبح خیز، رضا، چالش های حقوقی جرایم سایبری در نظام حقوق بین الملل و نظام حقوقی ایران،۱۳۹٤،ص ۱۱۸ .

ثبوت جرم مواجه نموده است و برای جامعه حقوقی این سوال مطرح می شود که آیا اختیارت و مقررات موجود در آئین دادرسی کیفری برای حسن انجام تحقیقات مقدماتی و رسیدگی به پرونده های مربوطه کافی است؟.[۲] استفاده از ابزارها و وسایل نوین مخصوصاً شبکه های مجازی، فرصت جدیدی برای ارتکاب جرم مجرمین به وجود آورده است، در همین راستا چنانچه حقوق کیفری در درون هر جامعه ای نتواند متناسب با این پیشرفت تغییر پیدا کند، تبعاً جرایم و بزهکاری های زیادی به وجود می آید که بدون مجازات باقی خواهند ماند[۳]. بنابراین، پرداختن به علل ارتکاب جرایم در شبکه های مجازی و همچنین در نظر گرفتن تدابیر و راهکارهای نوین جهت مقابله با ارتکاب جرایم در این فضا الزامی می باشد.

۱-واژه شناسی

پیش از هر چیز، ضرورت واژه شناسی در ابتدای بحث مطرح می شود؛ بر این اساس نخست به تبیین برخی واژه های کلیدی در موضوع بحث می پردازیم . موضوع مورد بحث ما مرکب از دو کلمه« جرم » و «شبکه های مجازی» می باشد که هر کدام از آن دو در جای خود، مباحث زیادی را دنبال داشته است، برای اینکه مفهوم ترکیب شده این دوکلمه را بتوانیم درک کنیم، لازم است، هر کدام را بصورت جدا از هم بشناسیم.

۱-۱-جرم

بزهکاری ریشه در تاریخ زندگی اجتماعی انسانها دارد و به سبب همین استمرار جرم در بستر زمان است که دورکیم، جامعه شناس فرانسوی نیمه اول قرن بیستم، از آن به عنوان «پدیده ای عادی» و اجتناب ناپذیر در کنار سایر پدیده های زندگی اجتماعی یاد می کند؛ همانگونه که جامعه ای بدون قانون و ضابطه وجود ندارد، اجتماع بشری که در آن جرم و جنایت اتفاق نیفتد- و به تعبیر جامعه شناختی همه افراد بدون

---

۲ باستانی، برومند،جرایم کامپیوتری و اینترنی- جلوه ای نوین از بزهکاری،تهران،انتشارات بهنامی، چاپ سوم، سال ۱۳۹۰،ص ۸۱-۸۰ .

۳ رضوی فرد، بهزاد؛موسوی، سید نعمت اله،مسئولیت کیفری در فضای سایبر در حقوق ایران، فصلنامه پژوهش حقوق کیفری ،سال پنجم، شماره شانزدهم، پاییز ۱۳۹۵، ص ٤٣ .

استثناء«ارزشهای» حاکم بر جامعه را محترم شمرده و آنها را از آن خود شمارند- نیز جز در عالم خیال وجود خارجی ندارد[۴]. اما دانشمندان علوم گوناگونی مانند حقوق کیفری، جرم شناسی، روان شناسی و جامعه شناسی، به تناسب ارتباط رشته علمی خود با جرم، به بررسی و تعریف آن پرداخته اند. معمولاً حقوقدانان پیش از تعریف جرم، به این نکته می پردازند که جرم امری نسبی است و از زمانی به زمانی و از جامعه ای به جامعه ای دیگر تفاوت می کند . مثلاً عملی مانند سِحر در گذشته جرم بوده، ولی امروز از آن جرم زدایی شده است. یا چند همسری در جامعه ای جرم و در جامعه ای دیگر امری قانونی است برای مثال، نویسنده کتاب حقوق کیفری می نویسد:«امروزه تعریف جرم در ابتدای کتاب های حقوق چندان مرسوم نیست؛ زیرا تعریف جامع و مانع ممکن نیست. از طرفی دیگر، تعریف جرم با این مشکل مواجه است که نمی توان معیاری برای شناخت جرم به ما بدهد . بنابراین، حقوقدانان به جای تعریف[۵] جرم به ذکر مشخصات آن می پردازند».[۶] جامعه شناسان و جرم شناسان در تعریف جرم گفته اند: جرم عملی است ضد اجتماعی که طبعاً مخالف وجدان عمومی نیز می باشد. اما تعریف قانونی جرم، یعنی چیزی که مردم و قوه قضاییه با آن روبرو هستند، مورد توجه تمامی حقوقدانان قرار گرفته است[۷]. در قانون مجازات اسلامی مصوب ۱۳۹۲ در ماده(۲)اینگونه جرم تعریف شده است: هر رفتاری اعم از فعل یا ترک فعلی که در قانون برای آن مجازات تعیین شده است، جرم محسوب می شود[۸].

۱-۲-مفهوم فضای مجازی (سایبری)

فضای سایبر یا فضای هدایت شده [۹]در زبان فارسی لغت سایبر را معادل واژه مجاز و لغت اسپیس را معادل واژه فضا ترجمه کرده اند و سایبر اسپیس را معادل فضای مجازی دانسته اند و ترکیبات دیگری نظیر

---

٤ نجابتی، مهدی، پلیس علمی(کشف علمی جرایم)،تهران، انتشارات سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه ها(سمت)، مرکزتحقیق و توسعه علوم انسانی، چاپ چهاردهم، سال ۱۳۹٤ ، ص ۱ .

٥Defenito

٦ ساریخانی، عادل؛ قیاسی، جلالدین؛ خسروشاهی، قدرت الله، مطالعه تطبیقی حقوق جزای عمومی؛ اسلام و حقوق موضوعه (جلد دوم) ارکان جرم،قم، انتشارات پژوهشگاه حوزه ودانشگاه، چاپ سوم ، بهار ۱۳۹۱، ص ۵ .

۷ ساریخانی، عادل؛ قیاسی، جلالدین؛ خسروشاهی، قدرت الله، پیشین، ص ۷ .

۸ گلدوزیان،ایرج، محشای قانون مجازات اسلامی مصوب ۱۳۹۲/۰۲/۰۱، انتشارات مجد، چاپ سوم، سال ۱۳۹۳، ص ۲۸.

۹ حسین پور، پری؛ صابرنژاد، علی،آزادی اطلاعات در فضای سایبراز منظر حقوق بین الملل،تهران،انتشارات مجد،۱۳۹٤، ص ۳۰ .

جامعه مجازی یا شهروند مجازی و فروشگاه های مجازی همه این ترکیبات فضای مجازی مطرح می شوند.در واقع منظور از فضای مجازی یا همان فضای سایبر عبارت است از فضایی که ما از طریق فن آوری مبتنی بر رایانه وارد آن می شویم.برای فضای سایبر تعاریف متعددی شده است که در اینجا به برخی از آنها که حائز اهمیت بیشتری هستند اشاره می شود:[۱۰]برخی فضای سایبر را اینگونه تعریف کرده اند:«محیطی است مجازی و غیر ملموس موجود در فضاهای شبکه ای بین المللی که این شبکه ها از طریق شاهراه های اطلاعاتی مثل اینترنت به هم وصل هستند. در این شبکه ها تمام اطلاعات راجع به افراد، فرهنگ ها، ملت ها، کشور ها، و به طور کلی هر آنچه روی کره خاکی به صورت فیزیکی و ملموس وجود دارد به صورت نوشته، تصویر، صوت و اسناد وجود داشته و قابل دسترسی و استفاده برای کاربران می باشند».همانطور که بسیاری از نویسندگان ایرانی معادل کلمه فضای سایبر واژه فضای مجازی را در نوشته های خود بکار برده اند و به نظر می رسد مناسب ترین معادل برای آن در زبان فارسی همین واژه باشد.[۱۱] فضای مجازی(سایبر) به مجموعه هایی از ارتباطات درونی انسانها از طریق کامپیوتر و وسایل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می شود. این روابط در فضای غیر فیزیکی(مجازی) اتفاق می افتد و به همین دلیل بسیاری از محدودیتهای دنیای معمول را ندارد.

فضای مجازی اصطلاحی است که می توان آن را در کنار عبارت مشهور «دهکده جهانی» قرار داد یا حتی، امروز چنین فضایی را عامل محوری تحقق دهکده جهانی دانست. دنیای تخیلی امروز به واقعیتی بدل شده که برای بسیاری از مفاهیم و موجودی های فیزیکی، معادل مجازی دارد: کتابخانه، فروشگاه، اتاق گفتگو و دید و بازدید، ارسال و دریافت و اشتراک، چاپ و نشر، گردشگری، کاریابی و حتی تقلب و سوء استفاده و کلاهبرداری.اگر رایانه اختراع نمی شد یا رایانه ها به هم وصل (شبکه) نمی شدند و ارتباطات، تنها محدود به تلفن می شد. هرگز چنین فضایی- به این وسعت – که ارزش بررسی حقوقی را داشته باشد، به وجود نمی آمد. صرف نظر از سامانه های مخابراتی همچون تلفن و تلگراف که محدودیت های خود را داشته و امروزه دیگر قدیمی محسوب می شوند. آنچه که امروزه واقعاً موجب قابل تصور شدن فضای مجازی

---

۱۰ شکری، محمد، پیشگیری از جرائم سایبری علیه امنیت ملی ایران،پایان نامه کارشناسی ارشد ، دانشگاه آزاد واحد قم،تابستان ۱۳۹۵ ، ص ۱۷ .

۱۱ البوعلی، امیر، پیشین، صص ٦-٤ .

شده است، دو پدیده«رایانه» و «اینترنت» می باشد.[۱۲]

۱-۳-مفهوم شبکه مجازی

شبکه مجازی چند موسسه یا دستگاه وابسته به هم را می گویند که در یک رشته کار می کنند . شبکه مجازی نیز معنای نزدیک به همین را دارد و این واژه هم اکنون به اندازه ای کاربرد دارد که هرگاه واژه "شبکه" به تنهایی به کار می رود، منظور همان شبکه رایانه ای و مجازی است و این به دلیل فرمانروایی بی چون و چرای هنجارهای رایانه ای و مجازی در زندگی بشر است که همگان وقتی واژگان چون داده ها، اطلاعات و سیستم و شبکه می شنوند، با وجود اینکه عمری بسیار درازتر از رایانه دارند و پیش تر از این کاربرد عمومی داشته اند، اما در گام نخست پیوند این واژگان با رایانه و فضای مجازی را به یاد می آورند . شبکه به گروهی از رایانه ها و وسایل مرتبط دیگر مرتبط دیگر گفته می شود که به وسیله تسهیلات ارتباطاتی به یکدیگر متصل می شوند. ارتباط موارد مذکور در یک شبکه ممکن است با اتصالات دائمی مثل کابل ها، یا اتصالات موقتی چون خطوط تلفن یا دیگر پیوند های ارتباطی باشد. یک شبکه می تواند به شبکه کوچک محلی (LAN) متشکل از چند رایانه و سایل دیگر می باشدو یا تعداد زیادی رایانه کوچک و بزرگ در نقاط جغرافیای مختلف توزیع شده اند، تشکیل شود. انواع شبکه های مجازی عبارت است از شبکه های حوزه شخصی[۱۳]، شبکه حوزه محلی[۱۴]، شبکه حوزه دانشگاهی[۱۵]، شبکه حوزه مادر شهری[۱۶]، شبکه حوزه گسترده[۱۷] و شبکه حوزه جهانی[۱۸]. این شبکه ها به ترتیب با توجه به اندازه و چگونگی رایانه ها پیشرفت داشته و خودبخود زمینه ساز تراکنش اطلاعات از رهگذر شبکه اینترنت شدند.

---

۱۲ السان، مصطفی، حقوق فضای مجازی، انتشارات موسسه مطالعات و پژوهشهای حقوقی شهر دانش، تهران، چاپ اول، سال ۱۳۹۳ ، صص ۱۶-۱۵ .

۱۳Personal Area Network(PAN)

۱٤ Local Area Network(LAN)

۱۵Campus Area Network(CAN)

۱٦Metropolitan Area Network(MAN)

۱۷Wide Area Network(WAN)

۱۸Glebal Area Network(GAN)

۱-۴-شبکه های اجتماعی

هدف کلی شبکه ها هر شبکه اجتماعی، ایجاد سرمایه اجتماعی تسهیل ارتباط بین متخصصان، هنرمندان و صاحبان حرفه های متعدد است. تبدیل سرمایه فردی به اجتماعی، از مسائل مهم و مورد توجه تمامی حوزه های علمی است. از این طریق، دانش فردی به دانش جامعه تبدیل و در واقع از دانایی جمعی برای حل مسائل و مشکلات دنیای علم بهر برداری می شود[۱۹]. با تعریف دیگر از شبکه های اجتماعی اینگونه می شود بیان کرد که شبکه های اجتماعی به مجموعه ای از افراد گفته می شود که به صورت گروهی با یکدیگر ارتباط داشته و مواردی مانند اطلاعات، نیازمندی ها، فعالیت ها و افکار خود را به اشتراک می گذارند. شبکه های اجتماعی رابطه بسیار نزدیک و مستقیمی با فن آوری اطلاعات و ارتباطات دارند.[۲۰]

۲-تاریخچه جرایم رایانه ای در ایران

در خصوص تاریخ وقوع جرایم رایانه ای در ایران نمی توان وقوع آن را به سال ۱۳۴۱ که کامپیوتر وارد ایران شد همزمان دانست. کاربرد کامپیوتر در سال های اولیه بسیار محدود بوده و در دهه ۵۰ و ۶۰ کم کم بر تعداد کامپیوتر های موجود در ایران و همچنین وسعت برنامه های کامپیوتری افزوده شد. به دلیل عدم وجود قانون مدون و آمار دقیق این جرایم و سوء استفاده از کامپیوتر نمی توان تاریخچه مشخص بیان نمود. ولیکن از اواخر دهه ۱۳۶۰ مواردی از تخلفات کامپیوتری به صورت کپی و تکثیر غیر مجاز نرم افزار ها نمود پیدا کرده است که تا اواسطه دهه ۷۰ نیز اکثر تخلفات کامپیوتری به صورت عدم ایفای تعهد توسط شرکتهای طرف قرارداد بود که خود نیز ممکن است ناشی از سوء نیت و قصور متعهد و یا عدم تبیین دقیق موضوع تعهد در قرارداد باشد. در این ایام قانون حاکم بر رفع اختلاف؛ قانون حمایت از مولفان و هنرمندان مصوب سال ۱۳۴۸ بود.[۲۱]

وقوع جرایم رایانه ای به تدریج از دهه ۱۳۷۰ در ایران شروع شده؛ سوء استفاده از رایانه برای ارتکاب

---

۱۹ رحمان زاده، سید علی، کارکرد های شبکه های اجتماعی مجازی در عصر جهانی شدن، مطالعات راهبردی جهانی شدن، سال اول، زمستان ۱۳۸۹، ص ۱۱ .

۲۰ محکم کار، ایمان؛ حلاج، محمد مهدی، شبکه های اجتماعی به دنبال چه هستند، فصلنامه دانش انتظامی خراسان شمالی،سال اول، شماره دوم،سال ۱۳۹۲،ص ۸۹ .

۲۱ باستانی، برومند،پیشین،ص ۲۹.

جرایم سنتی، به کارگیری ویروس از طریق توزیع حامل های داده آلوده به ویروس، سوء استفاده های مالی و تکثیر غیر مجاز نرم افزار های رایانه ای از جمله جرایم رایانه ای می باشند که در مقیاس بسیار کم در دهه ۱۳۷۰ واقع شده و با قوانین کیفری مرسوم مورد رسیدگی قرار گرفته اند[۲۲]. از نیمه دوم دهه ۷۰ و بالاخص ابتدای دهه ۸۰ که استفاده از رایانه های شخصی توسط سازمانها و موسسات 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. اشاعه فحشا و منکرات و انتشار عکس ها وتصاویر و مطالب خلاف عفت عمومی، ایجاد اختلاف بین اقشار جامعه از طریق طرح مسایل قومی و نژادی، انتشار مطالب نژاد پرستانه، انتشار اسناد و مسایل محرمانه، اهانت به مقدسات مذهبی و دینی، اهانت و افتراء نسبت به مقامات دولتی و اشخاص حقیقی و حقوقی، سرقت ادبی و غیره از جمله جرایمی هستند که بعد از فراهم شدن امکان استفاده از خدمات اینترنت از طریق وب سایت ها و وبلاگ ها، پست الکترونیک، گروه های خبری، چت(گپ زدن) و سایر سرویس های اینترنتی به وقوع پیوسته اند.قانونگذار در سال ۱۳۷۹ در برابر بخشی از جرایم رایانه ای واکنش نشان داده و با الحاق تبصره ۳ به ماده ۱ قانون مطبوعات مقرر داشت(کلیه نشریات الکترونیکی مشول مواد این قانون است). اولین واکنش قانونی کشور ما در برابر بعضی از جرایم رایانه ای قانون اصلاح مطبوعات ۱۳۷۹/۰۱/۳۰ مجلس شورای اسلامی است که در تاریخ ۱۳۷۹/۰۲/۰۷ مورد تأیید شورای نگهبان قرار گرفت.

دومین واکنش قانونی کشور در مقابل جرایم رایانه ای از طریق وضع(قانون حمایت از حقوق پدید آورندگان نرم افزار های رایانه ای) به عمل آمد.این قانون در تاریخ ۱۳۷۹/۱۰/۰۴ به تصویب رسیده است.

سومین عکس العمل قانونگذاردر سال ۱۳۸۲/۱۰/۰۹ از طریق تصویب قانون مجازات جرایم نیروهای مسلح به عمل آورده است. به موجب ماده(۱۳۱) این قانون جعل اطلاعات و داده های رایانه ای تسلیم و افشای غیر مجاز اطلاعات و داده ها به افرادی که صلاحیت دسترسی به آن را ندارند، سرقت و یا تخریب حامل های داده، و سوء استفاده مالی از طریق رایانه(کلاهبرداری و اختلاس) توسط نظامیان جرم تلقی و

۲۲ فضلی، حسن؛ رمضانی، حسین و لری، مجتبی، بررسی جرایم علیه امنیت ملی ایران در فضای مجازی، سال ۱۳۹۵، ص ۳ .

مرتکب حسب مورد به مجازات جرم ارتکابی محکوم می شود.

چهارمین واکنش قانونی مرتبط به جرایم رایانه ای از طریق قانون تجارت الکترونیکی مصوب ۱۳۸۲/۱۰/۱۷ مجلس شورای اسلامی به عمل آمده است.سپس شورای عالی توسعه قضایی قوه قضاییه پیش نویس قانون جرایم رایانه ای را در سال ۱۳۸۲ تهیه و طی جلسات متعددی از دی ماه تا اوایل خرداد ماه با حضور حقوقدانان و متخصصان امور رایانه آن را بررسی کرد تا پس از تصویب رئیس قوه قضاییه به عنوان لایحه جرایم رایانه ای از طریق هیئت دولت به مجلس شورای اسلامی تقدیم و با تصویب در سال ۱۳۸۸ و تأیید شورای محترم نگهبان، ابلاغ شد .

فصل دوم

علل ارتکاب جرایم در شبکه های مجازی

مقدمه

جرایم وابسته به فضای مجازی تنها می توانند با استفاده از کامپیوتر، شبکه کامپیوتری و یا دیگر اَشکال فن آوری ارتباطات و اطلاعات مرتکب شوند. فعالیت های مجرمانه جرایم اینترنتی به سرعت در حال رشد و در حال تحول هستند. بنابراین مقابله با جرایم اینترنتی باید به عنوان یک اولویت استراتژیک تلقی شود.[۲۳]سوءاستفاده از فناوری رایانه ای و اینترنتی می تواند امنیت و آسایش عمومی و موجودیت یک جامعه را به خطر اندازد و تأثیر های منفی فراوانی را بر روی زندگی افراد داشته باشد. با کمی دقت این موضوع مشخص می شود که اکثر مرتکبین این جرایم را جمعیت جوان تشکیل می دهد. این مجرمان از ظرفیت جنایی بالایی برخوردار بوده و هم دارای استعداد فراوان برای انطباق اجتماعی اند.جرم عبارت است از فعل و یا ترک فعلی که در قانون برای آن مجازات تعیین شده است و جامعه با ابزار مجازات آن را مورد نکوهش قرار می دهد. محیط سایبر به محیطی مجازی اطلاق می شود که اطلاعات در آن رد و بدل می شود.بنابراین جرایم شبکه های مجازی در اصطلاح به جرایمی گفته می شود که در محیطی غیر فیزیکی علیه فناوری از اطلاعات رخ می دهد، امروز جرایم سنتی تحت این فناوری دچار تحول شده و در سطوح وسیعی در حال انجام است. برای مثال جرایم جاسوسی، سرقت و کلاهبرداری که ضمن انجام به سبک سنتی، با شیوه های مدرن نیز در حال انجام می باشند، از آنجا که در حال حاضر شبکه های ارتباطی پیوندی جهان تحول یافته اند وصف بین المللی نیز به این جرایم افزوده شده به علاوه با ظهور و پیشرفت فناوری های جدید در این حوزه از قبیل رایانه های لپ تاپ، تلفن همراه هوشمند و.... که به صورت سیار ساخته می شوند این قابلیت راخواهند یافت که در هر زمان و مکان با وصف امحاء آثار صحنه ارتکاب جرم و تأثیر بالقوه آن بر تمامیت شبکه اتصال جهانی تحقق یابد.[۲۴]

در فضای ارتباطی جدید، عامل زمان و مکان کم رنگ شده است و دوری و نزدیکی به عنوان عامل خنثی در ارتباطات محلی و جهانی محسوب می شوند در واقع جهان جدیدی به موازات جهان واقعی به وجود آمده است که جهان بی مرز، جهان بی مکان و به تعبیر دقیق جهان مجازی نام گرفته است.با وجود

۲۳-National Crime Agency Strategic cyber industry Group" cyber crime assessment ۲۰۱٦"۷ july۲۰۱٦"p:٥-١٤.

۲٤ بابائی، حسن؛ میرزایی، محمد و مسعودی، عباس، پیشین، ص ۳-۲ .

این، فضای مجازی در نهایت محلی است که اشخاص یا شاید به تعبیر درست تر ذهن انسانها ساکن آن اند. زیرا، این ذهن ماست که در فضا سکنا گزیده و با ذهن دیگری در آنجا ملاقات می کند. در این صورت، جای هیچ گونه شگفتی نیست که بسیاری از مشکلات جهان واقعی به این قلمرو جدید منتقل شوند. جرم یکی از این مشکلات است[۲۵]و از آنجا که شبکه های مجازی، دنیای بیکرانی از امکانات و قابلیت های بی شمار است که بدون محدودیت در دسترس همگان قرارداد و هر کس با هر انگیزه ای می تواند از این موهبت استفاده کند. این حجم گسترده امکانات، قدرت پیچیده کردن روند ارتکاب جرم و گمنام کردن هویت مجرم را افزایش می دهد، این امر، دستگیری و تعقیب مجرمان را دشوار ساخته[۲۶] . حال علت هایی که می تواند نقش اساسی شبکه های مجازی در ارتکاب جرایم را آشکار سازد و نشان دهد که این فضا می تواند محیطی امن و تسهیل کننده جرایم باشد بیان می شود:

۲-۱-وقوع آن در فضای غیر واقعی

در تعریف جرم مجازی گفته شده جرم مجازی عملی است که در فضای مجازی (سایبر) واقع شده و قانون برای آن مجازات تعیین کرده باشد. بنابراین تنها خصوصیتی که چنین جرمی را با سایر جرایم متفاوت می سازد مکان وقوع آن است که در عالم مجازی است. از آنجا که معمولاً چنین جرایمی از متخصصین دانش فناوری اطلاعات هستند به گونه ای که پیشرفت نرم افزارها خود شاید متأثر از ازدیاد چنین جرایمی باشد.

۲-۲-بالا بودن رقم سیاه

با توجه به اینکه جرایم(شبکه های مجازی)در یک فضای غیر واقعی و مجازی محقق می شود و به خاطر ویژگی های منحصر به فرد فضای مجازی و به تبع آن مشکل کشف و اثبات جرایم مذکور از یک طرف و فاصله زیاد میان مجرم و قربانی و بحران قواعد سنتی در تعقیب این جرایم و کاستی های قوانین

۲۵ برجعلی، احمد؛ عبدالمالکی، سعید، روانشناسی جنایی، تهران، نشر دانشگاه پیام نور ، سال ۱۳۹۳، ص ۹۰-۸۸ .

۲۶ طارمی، محمد حسین، گذری برجرایم رایانه ای، ره آورد نور۲۱ بی تا، ص ۱۶.

مربوط به این جرایم از طرف دیگر، حصول آمار دقیق این جرایم را با مشکل مواجه کرده است. علاوه بر این، عدم گزارش جرایم از سوی قربانی، که غالباً شرکت های بزرگ اقتصادی و سیاسی می باشند، به خاطر حفظ حیثیت شرکت و جلوگیری ترک شرکت از سوی سهام داران و حفظ اعتماد مردم مزید بعلت است. این ویژگی، یعنی مشکل در آمارگیری، باعث شده که رقم سیاه این جرایم مسکوت بماند و روز به روز این رقم افزوده شود.

۲-۳-مشکل بودن کشف

مجرمان در شبکه های مجازی، هویت مشخص و یا واقعی ندارد، جرایم مجازی به خاطر اینکه اثر خارجی و مادی مشخص از خود بر جای نمی گذارند و صحنه وقوع آن هم مادی و فیزیکی نیست و بازیابی آن هم غیر ممکن است، کشف آن ها خیلی سخت و گاهی غیر ممکن می نماید و غالباً کشف آن ها به صورت اتفاقی انجام می گیرد . البته پیشرفت سریع تکنولوژی، عامل اساسی چنین صفتی برای جرایم سایبری گردیده است. مثلاً در شبکه ی اینترنت دفاتر و شرکت های بزرگی راه اندازی شده و یک خوراک خیلی مناسبی را برای مجرمین حرفه ای در ارتکاب جرایم سرقت معلومات فراهم نموده است به گونه ای که باعث کسب سود هنگفت در زمان خیلی کوتاه گردیده است. امری که بر مشکل اثبات چنین جرایمی می افزاید این است که مجرمین حرفه ای در جرایم سنگین اطلاعاتی خود سیستم های مربوط به مؤسسات دور از خود را مورد هدف قرار می دهند و همچنین به خاطر تخصص خود از همان ابتدا راه های کشف جرم خود را می بندند و با برنامه ریزی های دقیق خود مانع کشف جرم می شوند.[۲۷]موانع و مشکلات موجود 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 دادگاه ها را به موضوعی پیچیده و بغرنج تبدیل کرده است.

۲۷ البوعلی، امیر، پیشین،ص٦٧-٦١.

۲-۴-اخفای مجرمین

در آغاز بحث لازم است بگوییم که تعقیب جرایم فضای مجازی در اکثر موارد به دلیل اخفای این نوع جرایم با مانع مواجه می شود. برای نمونه کلاهبرداری رایانه ای غالباً از طریق درستکاری پرینت های داده پردازی کتمان می شود. جاسوسی رایانه ای از طریق نسخه برداری از فایل های داده و سرقت زمان، معمولاً در شرکت های بزه دیده به عنوان جرم نمایان نمی شود زیرا این شرکت ها غالباً فرصت کشف و اثبات استفاده غیر مجاز از داده های خود در شرکت رقیب را که به خوبی از ان محافظت می شود نمی یابند. خرابکاری رایانه ای اغلب به عنوان فقر سیستم و یا اشتباه نماینده می شود. در موارد بسیار امکان کشف مورد نقض حریم خصوصی اشخاص، برای بزه دیدگان و مقامات دولتی فراهم نیست زیرا اعمال مجرمانه در مراکز رایانه ای ارتکاب می یابند که از آنها بخوبی محافظت می شود.

۲-۵-نامرئی بودن مدارک

تعقیب جرایم شبکه های مجازی مستلزم کنترل گسترده داده های مجازی است. بیشترین این داده ها به شکلی مرئی که توسط انسان قابل خواندن باشد نگهداری نمی شوند بلکه در قالب های نامرئی که فقط دستگاه قادر به خواندن آن است و بصورت بسیاری متراکم در ابزارهای ذخیره سازی الکترونیکی نگهداری می شوند. بنابراین یکی از مشکلات راجع تعقیب و دادگاه ها در کشف و پیگیری جرایم فضای مجازی فقدان مدارک مرئی و مفهوم است که این فقدان حاصل مجهول بودن، تراکم و حتی در بیشتر موارد کد گذاری داده هایی است که به صورت الکترونیکی ذخیره شده اند. این معضل به ویژه در زمینه دستکاری برنامه های رایانه ای مساله ای جدی تلقی می شود .

۲-۶-کد گذاری مدارک

مجرمین حتی قادرند فعالیت های تعقیب و پیگیری جرایم ارتکابی را با به کارگیری تدابیر امنیتی مانند استفاده از گذر واژه ها،ارائه دستورالعمل های مانع و روش های کد گذاری با مشکلات حاد تری مواجه

نمایند. این روش ها همچنین مانع عمده ای در راه کنترل گردش فرامرزی داده ها به شمار می روند زیرا افرادی که مایل به پیروی از مقررات نباشند می توانند انتقال غیر قانونی داده ها را از طریق یک مکالمه تلفنی چند ثانیه ای که کدگذاری شده صورت دهند و همچنین کد گذاری داده ها در زمینه تجاوز به حریم خصوصی اشخاص، می توانند کنترل مؤثر داده های ذخیره شده به ویژه در رایانه های کوچک شخصی را بسیاری مشکل نماید.

۲-۷-امحاء مدارک

مشکلات دیگرکشف و تعقیب جرایم شبکه های مجازی از این واقعیت ناشی می شود که مجرمین براحتی می توانند از طریق حذف و پاک کردن داده ها دلایل علیه خود را از بین ببرند. یک روش خودکار پیچیده برای نابود سازی مدارک در رسیدگی به اتهامات یک قاچاقچی اسلحه در هلند افشا شد. این قاچاقچی اسلحه که نشانی مشتریان خود را در رایانه کوچک ذخیره کرده بود دستورهای معمولی در سیستم عامل را به گونه ای تغییر داده بود که وارد کردن دستور کپی یا چاپ از طریق صفحه کلید رایانه موجب حذف همه داده ها می شد. این حیله که به طور ویژه برای مقابله با تحقیقات احتمالی مراجع امنیتی برنامه ریزی شده بود به وسیله متخصصان داده پردازی هلند کشف شد. این متخصصان احساس کردند که تغییری در سیستم عامل رایانه صورت گرفته و بنابراین نسخه هایی از دیسک های ضبط شده را بر روی سیستم رایانه ای خود تولید کردند.

۲-۸-کثرت داده ها

تعداد بسیار زیاد داده ها پردازش شده در سیستم های پردازی که کنترل آنها ممکن نیست، نیز مانعی در راه کشف وتعقیب جرایم شبکه های مجازی محسوب می شود.

۲-۹-بی تجربگی مجریان قانون :

عدم آشنایی بازرسان، ماموران تحقیق با رسانه های اطلاعاتی و ضعف آنها در برخورد با مسایل فنی، عاملی است برای تشدید هر چه بیشتر مشکلات فوق الذکر. البته با عنایت به ماهیت نوین این جرایم، این مساله چندان هم تعجب آور نیست. بسیاری از اقدامات و تلاش های صورت گرفته برای تعقیب مجرمین متوقف شده و شکایات بسیاری در این زمینه رد شده و احکام بسیاری صرفاً در خصوص جنبه های حقوقی دعاوی صادر شده است که همه این امور بیانگر عدم تمایل مجریان قانون به مواجهه با مشکلات خاص پرونده های مطرح شده است.

۲-۱۰-نارسایی های حقوقی

خلاء های قانونی به ویژه در زمینه های کیفری ماهوی و شکلی نیز موانع دیگری در راه تعقیب جرایم شبکه های مجازی هستند.[۲۸]

۲۸ زیبر، اولریش، جرائم رایانه ای، مترجم، محمد علی نوری {.... و دیگران}، تهران، انتشارات گنج دانش، ۱۳۹۰،ص ۲۳۶-۲۳۱ .

فصل سوم

فضای مجازی؛ فرصت ها و تهدیدها (آسیب ها)

مقدمه

فضای مجازی، عامل موثر در فرهنگ پذیری ، انتقال ارزش ها و هنجارها و پر کردن اوقات فراغت برای نوجوانان و جوانان است . فضای مجازی، فرصت های تعاملات خانوادگی را از اعضای خانواده می گیرد و فضای خانواده را به سوی فرد گرایی پیش می برد. اینترنت، در عین جذابیت در صورتی که استفاده از آن بدون ملاحظات و برنامه باشد، آسیب های روانی، عصبی، اخلاقی را برای کاربران به دنبال خواهد داشت. در عین حال می توان از اینترنت به عنوان وسیله ای برای آموزش های رسمی از راه دور بازماندگان از تحصیل و عامل موثری در جهت رفع تبعیض و استفاده از اطلاعات و همسان سازی فرهنگی و آموزشی استفاده کرد. فضای مجازی با توجه به گسترده و نفوذ جهانی و استفاده از کیفیت برتر فن آورانه و جذابیت های تصویری، عاملی موثرتر در انتقال ارزش ها، هنجارها، و فرهنگ هاست که باید بتوان با آن رقابت کرد. رسانه ها، از جمله اینترنت، افراد را به صورت منفعل و پذیره در می آورند و غالبا قدرت انتخابی، تحلیل و تفکر را از بیننده ها، به ویژه کودکان و نوجوانان می گیرند. گسترش استفاده بی حد و حصر از رسانه های جدید موجب گسست فرهنگی و تقدس زدایی از ارزش های دینی و ملی و میراث فرهنگی به جامعه ایرانی می شود. به هر میزان که دچار کم کاری شویم و یا ورود و حضور پر رنگ در فضای مجازی را جدی نگیریم و یا تعلل و غیبت در صحنه و زمینه ها و بسترهای قابل بهره گیری در این فضای داشته باشیم، مطمئنا صدمات جبران ناپذیری در آینده در زمینه ارتباطات و تبادل اطلاعات با جهان خارج خواهیم داشت و این فرصت بسیار ارزشمند، با بی توجهی ما، تبدیل به تهدید خواهد شد. لذا شایسته است در این فضای چالش برانگیز با هدف کاهش تهدید ها در مقابل فرصت ها، بسیار زیرکانه و مسئولانه به بهره گیری از تمام توان و ظرفیت سخت افزاری و نرم افزار در این حوزه، وارد عرصه تولید و انتقال مفاهیم، محتوا و اطلاعات شویم. از سوی دیگر، باید فرهنگ سازی را در رأس برنامه های آموزشی خود قرارداده و فرهنگ صحیح استفاده از امکانات فضای مجازی را به نوجوانان و کودکان آموزش داد.

آنچه مسلم است اینکه به جای برخورد سلبی با این پدیده نوین به بررسی و ریشه یابی مشکلات و پیامدهای منفی ناشی از ان پرداخته و برای گرفته نتیجه بهتر راه های اصلاحی را در پیش گرفت

۳-۱-اثرات فضای مجازی بر کودکان

در کشورهای توسعه یافته، یک نظام درجه بندی برنامه ها در رسانه ها و فضای مجازی وجود دارد، به گونه ای که با علائم و هشدارهایی، مخاطب سنی برنامه در کشور ما نیز نیازمند این قبیل هشدارها هستیم تا کودکان ونوجوانان، دسترسی آسانی به همه برنامه ها نداشته باشند و از آسیبها و خطرات احتمالی مصون بمانند. در دنیای امروز که دسترسی کودکان به فضای مجازی گسترش پیدا کرده، کنترل کردن آنها در این فضا ها سخت تر شده است. بنابراین باید برخی محتواهای نامناسب برای کودکان و نوجوانان در فضای مجازی محدود شود تا از منظر جسمی و اخلاقی و روانی آسیب نبینند یا به ارتباطات خطرناک و کنترل نشده سوه داده نشوند . به طور مثال ، دیدن یک محتوای خشن در فضای مجازی، مناسب سن کودک نیست، زیرا این برنامه ها می توانند روحیه پرخاشگر را در کودک برانگیزند. این نظام درجه بندی محتوا در کشورهای توسعه یافته رعایت می شود و ما هم نیاز جدی به این تفکیک محتوا داریم . البته این تفکیک محتوای متناسب با سن شهروندان باید بر اساس کار کارشناسی صورت بگیرد. یعنی از نظرات همه کارشناسان متخصص در فضای مجازی استفاده شود، زیرا در غیر این صورت تلاش برای سالم سازی فضای مجازی برای کودکان و نوجوانان، موفقیت آمیز نخواهد بود. در این برنامه ها می توان با کد گذاری محتواها از سوی والدین ، مانع از دسترسی فرزندان کم سن و سال به هر نوع محتوایی شد . حضور بی ظابطه و کنترل نشده کودکان و نوجوانان در فضای مجازی می تواند فرایند اجتماعی شدن آنان را نیز مختل کند و ارتباطات خانوادگی آنها را محدود سازد. به طور مثال، حضور افراطی نوجوانان در فضای مجازی شرایطی را پیش می آورد که در ظاهر او در میان جمع خانواده است اما در واقع در عالم انزوا به سر می برد.

۳-۲-فرصت های فضای مجازی :

۱- ایجاد جوامع و گروه های مختلف از جمله گروه های خانوادگی و دانشجویی که باعث نزدیکی بیشتر آنها به یکدیگر می شود .

۲- عبور از مرزهای جغرافیایی و آشنایی با افراد جوامع و فرهنگ های مختلف .

۳- تولید اطلاعات آموزشی و انتقال مطالب و غیره .... .

۳-۳- آسیب ها (فردی، فکری، جسمی و اجتماعی) و تهدید های فضای مجازی

*آسیب های فردی

حریم خصوصی در فضای مجازی، حق حریم خصوصی حقی است نسبت به تنها ماندن، زندگی با سلیقه ی خود و با حداقل مداخله ی دیگران. به عبارتی وسیع تر می توان گفت حق افراد نسبت به حفاظت از زندگی خود در برابر:

۱- دخالت دیگران در زندگی خصوصی

۲- حملات و تعرضات به آبرو، شهرت .

۳-استفاده از نام و یا هویت افراد

۴- افشای اطلاعات

*آسیب‌های فکری

استفاده خارج از حد متعارف از اینترنت، به وابستگی شدید روانی و فکری می‌انجامد. با ورود اینترنت و رایانه به درون خانواده‌ها، بین والدین، معلمان، مربیان و دانش‌آموزان(فرزندان)جدایی فکری و عاطفی، رخ می‌دهد. نتیجه تحقیقات نشان می‌دهد که درصد بالایی از نوجوانان و جوانان از اینترنت برای فعالیت‌های

بیهوده‌ای نظیر دوست یابی، بازی و صحبت با یکدیگر استفاده می‌کنند. نوجوانی که پشت میز رایانه و اینترنت نشسته است، برنامه های سایت را لذت بخش تر از سخنان پدر و مادر و تکالیف مدرسه می داند. در نتیجه، در ارتباطات، رفتار و زندگی اجتماعی او اختلال ایجاد می‌شود.

*آسیب‌های جسمی

استفاده بیش از حد از رایانه، این آثار را به دنبال دارد:

۱ -تیک ها

۲ -فشار های عصبی

۳ -چشم درد

۴ -چاقی و اضافه وزن

۵ -خارج شدن ستون فقرات از حالت طبیعی

*آسیب های اجتماعی فضای مجازی :

۱-ایجاد نارضایتی های خانوادگی : یکی از بزرگترین معضلات اجتماعی که جوامع امروزی به آن مبتلا شده اند، ضعف بنیان خانواده است. بالا رفتن سن ازدواج، افزایش آمار طلاق، سرد شدن ارتباطات عاطفی، نارضایتی از زندگی خانوادگی همگی از مشکلات عمیقی است که دامنگیر خانواده ها شده است.

۲-اختلال در شکل گیری هویت نوجوانان : سنین نوجوانی، سنینی است که در آن هویت اصلی فرد شکل می گیرد و متأسفانه اکنون اکثر نوجوانان بیشتر وقت خود را در فضای مجازی و در ارتباط با افراد ناشناس در این فضا می گذرانند. این فضا صحنه ای فرهنگی و اجتماعی است که فرد در آن می تواند خود را در نقش های متفاوت قرار دهد و این امر منجر به چند شخصیتی شدن او خواهد گردید. فضای مجازی فضایی است که هویت شخصی و مشخصات فردی قابل پنهان کردن است و قرار گرفتن در نقش های گوناگون به ویژه در سنین نوجوانی منجر به شکل گیری هویت ناسالم و اختلالات شخصیتی آنان می گردد.

۳-تعارض ارزش ها : از دیگر معضلات فضای مجازی، ورود ارزش ها و فرهنگ غربی به درون خانواده ها و

ایجاد تغییر در نظام ارزشی خانواده هاست. نتایج مطالعات صورت گرفته نشان می دهد که حضور بیش از حد در فضای مجازی منجر به کمرنگ شدن فرهنگ ایرانی - اسلامی در درون خانواده ها شده است. این موضوع آسیب های فرهنگی زیادی را به سطح جامعه وارد کرده است.

۴-انزوای اجتماعی امروزه در زندگی اجتماعی، فضای مجازی جای دوستان و نزدیکان را گرفته و در حقیقت جایگزین روابط دوستانه و فامیلی شده است. افراد ساعت ها از وقت خود را در فضای مجازی گذرانده و به جای فعالیت های اجتماعی، به فعالیت های فردی روی می آورند. این موضوع افراد را در افسردگی و انزوای اجتماعی فرو خواهد برد، چه بسا خود آن ها از این موضوع آگاهی نداشته و حتی ممکن است آن را تأیید نکنند.

*تهدید یا خطرهای برتر موجود در فضای مجازی

۱ .سرقت هویت

حملات سرقت هویت نوعی از حملات مهندسی اجتماعی هستند. حملات سرقت هویت از ایمیل‌ها یا وب‌سایتهای خرابکاری که ظاهرا به یک سازمان قابل اطمینان تعلق دارند، برای به دست آوردن اطلاعات از افراد سوءاستفاده می کنند.

۲ .شناسایی افراد ارزشمند

یکی از کلیدهای اصلی تهدیدات دائمی، جمع‌آوری اطلاعات افراد ارزشمندی است که با استفاده از آنها، می توان به سیستم‌های مهم و حساس دسترسی پیدا کرد. در این مورد، شبکه‌های اجتماعی می‌توانند گنجینه‌ای از داده‌ها در مورد این افراد باشند. کسانی که به این اطلاعات ارزشمند دسترسی پیدا می‌کنند، از آنها برای توسعه حملات خود، نصب بدافزارها و تروجان ها و در نهایت دسترسی به سیستم های حساس و مهم استفاده می کنند .

فصل چهارم

تدابیر و راهکارهای مقابله با تهدیدهای فضای مجازی

۴-۱-تدابیر آموزشی و آگاهی سازی

یکی از علت های اصلی رشد جرایم مجازی به تنها عدم سرزنش چنین رفتارهایی از سوی جامعه است، بلکه در بیشتر موارد رفتار بزهکاران تقویت و حتی در بعضی موارد به طور ناآگاهانه افراد جامعه نیز در انجام رفتارهای مجرمانه حداقل به طور غیر مستقیم مشارکت دارند. از سوی دیگر، با توجه به غیر ملموس و غیر قابل سنجش بودن تهدیدهای سایبری، بزهکاران از این امر چه آگاهانه و چه ناآگاهانه سوء استفاده می کنند و به خود یا دیگران می قبولانند که رفتارهای آنان نسبت به رفتارهای همتایان خود در دنیای مادی، وخامت کمتری دارد. بنابراین، این دو نظریه بیش از هر نظریه دیگری نشان می دهند که تا چه اندازه تابعان فضای مجازی یا شبکه وندها به آموزش و ارتقاء سواد رسانه ای نیازمندند یا به عبارتی تا چه اندازه سواد رسانه ای ضرورت دارد تا بتوانند از بخش وسیعی از این آسیب ها پیشگیری کنند.[۲۹]

از مسایل بسیار مهمی که در سیاستگذاری رسانه ای و اجتماعی دنیا به آن پرداخته می شود، مسئله «سواد رسانه ای» است. سواد رسانه ای به زبان ساده عبارت است از مجموعه مهارت هایی که شهروندان برای مواجهه با رسانه جدید لازم است بیاموزند. امروزه در سراسر دنیا با بهره گیری از حمایت های مستقیم و غیر مستقیم نهاد های دولتی، آموزش لازم از طریق رسانه ها و برقراری دوره های آموزشی به شهروندان ارایه می شود این آموزش ها موجب می گردد، شهروندان روش های بهره گیری صحیح از رسانه جدید را فراگرفته و آسیب ها و خطرات احتمالی آن را نیز بیاموزند. با بررسی میدانی از شبکه های اجتماعی مشخص شد که استفاده کنندگان از این شبکه های اجتماعی تنها با دانست امکانات محدودی، پای در عرصه شبکه ها گذاشته که این امر موجب سوءاستفاده احتمالی توسط سود جویان را فراهم کرده و آن را ابزاری برای جاسوسی دول قدرتمند جهان تبدیل می نماید[۳۰].

در کنار تدابیر آموزشی که بذر آن باید در از دوران ابتدایی زندگی کاشته شود، می توان از تدابیر آگاهی سازی به عنوان اقدامات مکمل که می تواند فرایند آموزش را استمرار ببخشد، بهره برد. بدیهی است،

۲۹ رضوی فرد، بهزاد؛ کوره پز، حسین محمد، راهبردهای پیشگیرانه آموزشی و آگاهی سازی: ضرورتی پیش روی برنامه های کنترل انحرافات سایبری، مجله کاراگاه،دوره دوم سال هشتم شماره ۳۲، پاییز ۱۳۹٤، ص ۹۲ .

۳۰ محکم کار، ایرج؛ کلاج، محمد مهدی، پیشین، ۱۳۹۳، ص ۹۹-۹۸.

چنانچه اقدامات آموزشی به شیوه مناسبی طرح ریزی و پیاده شوند و نیز به طور مطلوبی بتوانند به آن اهدافی که هست دست یافت می توان سواد رسانه ای کاربران را تاحد بالایی تضمین کرد[۳۱].

۱- آموزش از طریق رسانه

برای اینکه افراد جامعه قادر باشند اطلاعات مورد نیاز خود را شناسایی کرده، این اطلاعات را در مجموعه دانش خود وارد کنند و به شکلی موثر با رعایت موازین اخلاقی و قانونی از آنها برای رسیدن به هدف خاص خود استفاده نمایند، لازم است تا شرایط اقتصادی، حقوقی و اجتماعی حاکم بر استفاده از آنها را درک کنند. برای این منظور باید با مفهوم ادبیات اطلاعات و رسانه آشنا شوند. از آنجا که بسیاری از والدین، مربیان و مسئولان، اطلاعات زیادی راجع به ماهیت فضای مجازی، میزان خطرات این فضا و ضرورت سلامت اینترنت ندارند. لازم است دوره های آموزشی مهارت افزایی مرتبط با ادبیات اطلاعات و رسانه را آموزش ببینند. به هر حال، آموزش هایی که از طریق رسانه عمومی در اختیار مردم قرار می گیرند باید حاوی مطالب ساده و نکات قابل درک برای اکثر اقشار جامعه باشد و از اراده مطالب پیچیده خود داری شود. همان طور که می توان هشدارهایی را درباره پیشگیری در فضای فیزیکی داد. با استفاده از رسانه ها پیام هایی در خصوص فضای مجازی نیز منعکس شود.[۳۲]

۲-آموزش و دانشگاهیان

مؤسسه های دانشگاهی و سازمان های بین حکومتی، عوامل ذی نفع مهم در پیشگیری و مبارزه با جرایم مجازی هستند. امکان دارد چنین موسسه هایی خصوصاً از خلال توسعه دانش و اشتراک آن؛ وضع قانون و ایجاد سیاست ها؛ توسعه تکنولوژی و معیارهای فنی، ارائه مساعدت فنی و همکاری با مراجع اجرای قانون کمک کنند.اشتراک و توسعه دانش در واکنش به درخواست های حکومتی و صنعتی برای افراد متخصص در زمینه امنیت سایبری و نیاز های توسعه نیروی کار، موسسه های دانشگاهی برنامه های تخصصی آموزشی، برنامه های درسی و مراکز آموزشی جهت ادغام دانش و تحقیقات و نیز افزایش اشترک مساعی در دانش در تمام حوزه ها و رشته ها ایجاد کردند. شمار رو به رشدی از دانشگاه ها، مدارک، گواهی

---

۳۱ رضوی فرد، بهزاد؛ کوره پز، حسین محمد، پیشین،ص ۹۸-۹۷ .

۳۲ سلیمانی، فرزاد؛ سلامت،وحید، پیشین، ص ۷.

ها و آموزش حرفه ای در راستای امنیت سایبری و رشته های مرتبط با جرایم مجازی جهت ارتقای آموزش و تربیت افراد جوان و متخصصان آتی در مورد روال های ایمن کار با رایانه و موضوعات فنی ارائه می کنند. دانشگاه ها همچنینی یادگیری کاربردی و توسعه شبکه های اجتماعی علیه جرم مجازی را از خلال سازماندهی اتاق های کاری و همایش ها ارتقا می دهند.این دانشگاه ها فرصت هایی برای تبادل اطلاعات و توصیه هایی در باب تدابیر واکنش و پیشگیرانه ترویج و پرورش همکاری های غیر رسمی در بعضی مواقع مکانهایی برای گزارش و نیز اقدامات و ایجاد راه حل ها و سیستم های فنی ارائه می کنند.[۳۳]

۴-۲-تدابیر پیشگیرانه غیر کیفری

جرم شناسان در صدد بوده اند تا با تعیین تفاوت ها در بین مجرمین و غیر مجرمین به دیدگاهها و راهبردهایی در جهت پیشگیری از جرم دست یابند.[۳۴] همچنان که سزار بکاریا در رساله(جرایم و مجازات ها)ی خود بیان می کند:پیشگری از وقوع جرایم بهتر از کیفر دادن است چنین است هدف اصلی هر گونه قانونگذاری صحیح که هنر رهبری انسانها به سوی بیشترین خوشبختی یا کمترین بدبختی ممکن با توجه به خیر و شر زندگی است[۳۵]. بحث پیشگیری از جرم یا به عبارت بهتر اتخاذ تدابیر مناسب جهت جلوگیری از وقوع یا تکرار جرم، موضوعی نیست که به عصر حاضر تعلق داشته باشد. از همان ابتدا که بشر با نقض ارزش های خود مواجه شد، همواره در این فکر بود که با اتخاذ تدابیری، از ارتکاب چنین اعمالی جلوگیری کند .[۳۶] در جرایم فضای مجازی نیز، پیشگیری باید به عنوان هدف عمده هرگونه سیاست گذاری در این خصوص باشد. در اصطلاحات سیاست جنایی وقتی از پیشگیری از بزهکاری سخن به میان می آید، منظوراز استفاده راهکارهای متعدد برای ممانعت از وقوع جرم است. در یک دسته بندی، پیشگیری از جرم پیشگیری غیر کیفری و کیفری تقسیم می شود پیشگیری غیر کیفری که جلوگیری از وقوع جرم با استفاده از ابزارهای

---

۳۳ سازمان ملل متحد، دفتر مبارزه با جرم و مواد مخدر، مطالعه جامع جریم سایبری، مترجم مهدی مقیمی، انتشارات دانشگاه علوم انتظامی، تهران، سال ۱۳۹۵، صص ۳۲۴-۳۲۳ .

۳٤ رستمی تبریزی، لمیاء، روانشناسی جنایی، تهران، انشارات مجد، سال ۱۳۹۳، ص ۲۹ .

۳۵ بکاریا،سزار، رساله جرایم و مجازات ها، ترجمه دکتر محمد علی اردبیلی،تهران، نشر میزان، چاپ هفتم، سال ۱۳۹۳،ص ۱۳۱ .

۳٦ جلالی فراهانی، امیر حسین،پیشگیری از جرایم رایانه ای ، مجله حقوقی دادگستر، شماره ۷۷، تابستان ۱۳۸۳، ص ۹۲ .

غیر قهر آمیز است در قالب دو نوع پیشگیری اجتماعی و وضعی مطرح می شود. پیشگیری کیفری که جلوگیری از وقوع جرم با تکیه بر مجازات ها در نظام کیفری است .[۳۷] البته باید توجه داشت که صرفاً به موجب یکی از این روشهای پیشگیری نمی توان به پیشگیری واقعی و قطعی دست یافت، بلکه مهمترین ساز و کار در مقوله پیشگیری از وقوع جرم، استفاده تلفیقی از انواع روشهای پیشگیرانه خواهد بود و صرفاً نمی توان با یک نگاه مجرد و انتزاعی با پدیده پیچیده و دایم التغییر اینگونه جرایم مقابله نمود.[۳۸]

۱-پیشگیری اجتماعی

پیشگیری اجتماعی به راهبردها و تدابیری اطلاق می شود که هدف آنها به طور کلی تغییر در وضعیت رفاه و بهبود کیفیت زندگی باشد. بدین منظور اقدامات اجتماعی با تمرکز بر عوامل خطر و عوامل حمایتی و نیز ساختارهایی که مستعد رشد و توسعه آن می باشد در اولویت قرار می گیرند[۳۹] . پیشگری اجتماعی، یکی از گونه های پیشگیری کنشی(غیر کیفری)است. این پیشگیری اجتماعی با ایجاد تغییرات و اصلاحات در فرد و جامعه به دنبال جلوگیری از ارتکاب جرم است. عده ای از صاحب نظران چنین گفته اند که پیشگیری اجتماعی، پیشگیری از طریق اعمال و اقداماتی است که برخود فرد تاثیر می گذارد و بدین ترتیب خلاء های فردی را پر می کند. و با این که پیشگیری اجتماعی، یعنی مداخله در محیط اجتماعی عمومی و شخصی که خاص خود فرد است مانند محله، خانواده و.... به طور خلاصه، در پیشگیری اجتماعی، هدف، از بین بردن انگیزه های مجرمانه است و به همین دلیل، به آن پیشگیری بزهکار محور گفته می شود. در اینجا راهکارهای اجتماعی، مانند رفع بیکاری و فقر که زمینه ساز شکل گیری انگیزه های مجرمانه مالی و حتی قتل می شوند همچنین راهکارهای تربیتی و آموزشی برای کودکان، به عنوان آسیب پذیرترین گروه سنی، هم از لحاظ بزهکاری و هم از لحاظ بزه دیدگی در دستور کار قرار می گیرند.[۴۰] پیشگیری اجتماعی مهم ترین و موثرترین نوع پیشگیری از جرم است که از آن نیز به پیشگیری زود رس و رشد مدار تعبیر می شود

---

۳۷ شایگان، محمد رسول؛ ثابت سروستانی، محمد امین، راهکارهای مقابله با جرم کلاهبرداری رایانه ای در حقوقی کیفری ایران،کاراگاه، دوره دوم، سال سوم،شماره ۹ ، زمستان ۱۳۸۸، ص ۳۸ .

۳۸ نجفی توانا، علی، جرم شناسی،نشر آموزش و سنجش،چاپ هجدهم، سال ۱۳۹٤، صص ۵۹-۵۸ .

۳۹ جندلی،منون، پیشین، ص ٦۳ .

٤۰ ابوالحسنی، ابوالحسن،پیشین ، ص ٤۲۷ .

این نوع پیشگیری با تأثیرگذاری بر خود فرد خلاء ها و ناهنجاری ها فرد را برطرف می کند.این نوع پیشگیری بر دو نکته تاکید دارد. اول نحوه آموزه و تربیت فرد در طول رشد و دوم مداخله در محیط تربیتی و آموزشی خرد و کلان مسلط بر فرد مانند خانواده، مدرسه و... ضمن اینکه به دلیل ذیل، توجه به این نوع پیشگیری از اهمیت بسزایی برخوردار است.

- طیف وسیعی از مجرمان و بزه دیدگان جرایم سایبری جوانان و افراد کم سن بوده که مخاطبان اصلی پیشگیری اجتماعی اند. نکته مهم دیگر در مورد مجرمان و بزهدیدگان این نوع جرایم این است که ایشان با بهره هوشی بالا دارای امکانات استفاده از فضای مجازی می باشند. عموماً به قول (ادوین ساترلند) یقه سفیدان و همانطور که (مارک آنسل) در کتاب خود می گوید جرایم یقه سفیدها آثار زیان بارتری به بار خواهند آورد.

پیشگیری اجتماعی یا اصلاحی، از طریق اعمال اصلاحات فردی و اجتماعی که زیر بنای اصلی و اساسی رویکردهای پیشگیری اجتماعی است. پیروان این نظریه که به پوزیتویست یا تحققی معرف هستند، بر این عقیده اند که از طریق شناخت علل ارتکاب جرم (اعم از فردی و اجتماعی) و بر طرف کردن آن ها با انجام اصلاحات فردی و اجتماعی، مثل درمان بیماری و نارسایی های جسمی و روانی مرتکبین، بالا بردن ارزش های اجتماعی و ثبات و وابستگی به آن ها، تقویت نهادهای اجتماعی مثل خانواده، مدرسه، توسعه و تعالی فرصت های اقتصادی، تحصیلی، تفریحی، مسکن و امثال این ها، می توان از ایجاد تمایلات مجرمانه در افراد جلوگیری کرد و نهایتاً آنها را از غرق شدن یا کشیده شدن به سوی شیوه های مجرمانه زندگی نجات داده.[۴۱]

۲-پیشگیری وضعی

در این نوع پیشگیری به جای تکیه به فرد به محیط تکیه می شود. در این نوع پیشگیری سعی بر این است که با جاذبه زدایی از آماج جرم، بالا بردن هزینه های ارتکاب جرم و کاهش احتمال نتیجه گیری از جرم، زمینه ارتکاب آن را از بین می بریم یا تا حد قابل قبول پایین بیاوریم.با توجه به اینکه جرایم فضای

---

٤١ ابوالحسنی، ابوالحسن، پیشین، ص ٤٢٩ .

مجازی و شبکه های برای ارتکاب، نیاز به مقدمات و وسایلی دارد و خود فضای مجازی زمینه ارتکاب جرم می شود از آن چه که در پیشگیری وضعی دنبال می شود این است که با اتخاذ تدابیری فنی از بهره برداری از اینگونه قابلیت های جرم انگیز این فضا جلوگیری شود.

نکته دیگر وجود شبکه های اطلاع رسانی مجازی است که به عنوان پل ارتباط با فضای تبادل اطلاعات عمل می کنند و بر این اساس قوانین ومقررات تحت نظر دولت اداره می شوند. درواقع از طریق مدیریت و نظارت بر این شبکه های ارتباطی و در قالب برنامه های مانند دیوار آتشین یا همان فیلترینگ، رمز گذاری و یا برنامه هایی مانند پلیس گشت سایبر و.... دسترسی به آماج جرم در جرایم سایبری از طریق پیشگیری وضعی غیر ممکن یا مشکل سازد علاوه بر این از طریق ارائه آموزش هایی که در خود سایت ها داده می شود می توان از ظرفیت های محیط سایبری در جهت پیشگیری استفاده نمود.

قانون جرایم رایانه ای

بخش یکم ـ جرایم و مجازاتها

فصل یکم ـ جرایم علیه محرمانگی داده ها و سامانه های رایانه ای و مخابراتی

مبحث یکم ـ دسترسی غیرمجاز

ماده ۷۲۹ قانون مجازات اسلامی (ماده۱-قانون جرایم رایانه ای) هرکس به طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون(۵,۰۰۰,۰۰۰)ریال تا بیست میلیون(۲۰,۰۰۰,۰۰۰)ریال یا هر دو مجازات محکوم خواهد شد.

مبحث دوم ـ شنود غیرمجاز

ماده ۷۳۰ (ماده۲ قانون جرایم رایانه ای) هرکس به طور غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری را شنود کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون(۱۰,۰۰۰,۰۰۰)ریال تا چهل میلیون (۴۰,۰۰۰,۰۰۰)ریال یا هر دو مجازات محکوم خواهد شد.

مبحث سوم ـ جاسوسی رایانه‌ای

ماده ۷۳۱ (ماده۳ ق . ج. ر) هرکس به طور غیرمجاز نسبت به داده‌های سری در حال انتقال یا ذخیره شده در سامانه‌های رایانه‌ای یا مخابراتی یا حامل های داده مرتکب اعمال زیر شود، به مجازات های مقرر محکوم خواهد شد:

الف) دسترسی به داده‌های مذکور یا تحصیل آنها یا شنود محتوای سری در حال انتقال، به حبس از یک تا سه سال یا جزای نقدی از بیست میلیون (۲۰,۰۰۰,۰۰۰)ریال تا شصت میلیون (۶۰,۰۰۰,۰۰۰)ریال یا هر دو مجازات.

ب) در دسترس قرار دادن داده‌های مذکور برای اشخاص فاقد صلاحیت، به حبس از دو تا ده سال.

ج) افشاء یا در دسترس قرار دادن داده‌های مذکور برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آنها، به حبس از پنج تا پانزده سال.

تبصره ۱ـ داده‌های سری داده‌هایی است که افشای آنها به امنیت کشور یا منافع ملی لطمه می‌زند.

تبصره ۲ـ آیین‌نامه نحوه تعیین و تشخیص داده‌های سری و نحوه طبقه‌بندی و حفاظت آنها ظرف سه ماه از تاریخ تصویب این قانون توسط وزارت اطلاعات با همکاری وزارتخانه‌های دادگستری، کشور، ارتباطات و فناوری اطلاعات و دفاع و پشتیبانی نیروهای مسلح تهیه و به تصویب هیأت وزیران خواهد رسید.

ماده ۷۳۲ (ماده۴ ق . ج. ر) - هرکس به قصد دسترسی به داده‌های سری موضوع ماده (۳) این قانون، تدابیر امنیتی سامانه‌های رایانه‌ای یا مخابراتی را نقض کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون(۱۰,۰۰۰,۰۰۰)ریال تا چهل میلیون (۴۰,۰۰۰,۰۰۰)ریال یا هر دو مجازات محکوم خواهد شد.

ماده ۷۳۳ (ماده۵ ق . ج. ر) - چنانچه مأموران دولتی که مسؤول حفظ داده‌های سری مقرر در ماده (۳) این قانون یا سامانه‌های مربوط هستند و به آنها آموزش لازم داده شده است یا داده ها یا سامانه های مذکور در اختیار آنها قرار گرفته است بر اثر بی‌احتیاطی، بی‌مبالاتی یا عدم رعایت تدابیر امنیتی موجب دسترسی اشخاص فاقد صلاحیت به داده‌ها، حامل های داده یا سامانه‌های مذکور شوند، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون(۵,۰۰۰,۰۰۰)ریال تا چهل میلیون (۴۰,۰۰۰,۰۰۰)ریال یا هر دو مجازات و انفصال از خدمت از شش ماه تا دو سال محکوم خواهند شد.

فصل دوم ـ جرائم علیه صحت وتمامیت داده ها و سامانه های رایانه ای و مخابراتی

مبحث یکم ـ جعل رایانه‌ای

ماده ۷۳۴ (ماده۶ ق . ج. ر) هرکس به طور غیرمجاز مرتکب اعمال زیر شود، جاعل محسوب و به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون(۲۰,۰۰۰,۰۰۰)ریال تا یکصد میلیون (۱۰۰,۰۰۰,۰۰۰)ریال یا هر دو مجازات محکوم خواهد شد:

الف) تغییر یا ایجاد داده‌های قابل استناد یا ایجاد یا واردکردن متقلبانهداده به آنها،

ب) تغییر داده‌ها یا علائم موجود در کارتهای حافظه یا قابل پردازش در سامانه های رایانه‌ای یا مخابراتی یا تراشه‌ها یا ایجاد یا وارد کردن متقلبانه داده‌ها یا علائم به آنها.

ماده ۷۳۵ (ماده۷ ق . ج. ر) هرکس با علم به مجعول بودن داده‌ها یا کارتها یا تراشه‌ها از آنها استفاده کند، به مجازات مندرج در ماده فوق محکوم خواهد شد.

مبحث دوم ـ تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی

ماده ۷۳۶ (ماده۸ ق . ج. ر) هر کس به طور غیرمجاز داده‌های دیگری را از سامانه‌های رایانه‌ای یا مخابراتی یا حامل های داده حذف یا تخریب یا مختل یا غیرقابل پردازش کند به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون (۱۰,۰۰۰,۰۰۰)ریال تا چهل میلیون (۴۰,۰۰۰,۰۰۰)ریال یا هر دو مجازات محکوم خواهد شد.

ماده ۷۳۷ (ماده۹ ق . ج. ر) - هر کس به طور غیرمجاز با اعمالی از قبیل وارد کردن، انتقال دادن، پخش، حذف کردن، متوقف کردن، دستکاری یا تخریب داده‌ها یا امواج الکترومغناطیسی یا نوری، سامانه‌های رایانه‌ای یا مخابراتی دیگری را از کار بیندازد یا کارکرد آنها را مختل کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون(۱۰,۰۰۰,۰۰۰)ریال تا چهل میلیون (۴۰,۰۰۰,۰۰۰)ریال یا هر دو مجازات محکوم خواهد شد.

ماده ۷۳۸ (ماده۱۰ ق . ج. ر) هرکس به طور غیرمجاز با اعمالی از قبیل مخفی کردن داده ها، تغییر گذرواژه یا رمزنگاری داده ها مانع دسترسی اشخاص مجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی شود، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون (۵,۰۰۰,۰۰۰)ریال تا بیست میلیون (۲۰,۰۰۰,۰۰۰)ریال یا هردومجازات محکوم خواهدشد.

ماده ۷۳۹ (ماده۱۱ ق . ج. ر) هرکس به قصد به خطر انداختن امنیت، آسایش و امنیت عمومی اعمال مذکور در مواد (۸)، (۹) و (۱۰) این قانون را علیه سامانه های رایانه ای و مخابراتی که برای ارائه خدمات ضروری عمومی به کار می روند، از قبیل خدمات درمانی، آب، برق، گاز، مخابرات، حمل و نقل و بانکداری مرتکب شود، به حبس از سه تا ده سال محکوم خواهد شد.

فصل سوم ـ سرقت و کلاهبرداری مرتبط با رایانه

ماده ۷۴۰ (ماده۱۲ق . ج. ر) هرکس به طور غیرمجاز داده‌های متعلق به دیگری را برباید، چنانچه عین داده ها در اختیار صاحب آن باشد، به جزای نقدی از یک میلیون (۱,۰۰۰,۰۰۰)ریال تا بیست میلیون (۲۰,۰۰۰,۰۰۰)ریال و در غیر این صورت به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون (۵,۰۰۰,۰۰۰)ریال تا بیست میلیون (۲۰,۰۰۰,۰۰۰)ریال یا هر دو مجازات محکوم خواهد شد.

ماده ۷۴۱ (ماده۱۳ق . ج. ر) هرکس به طور غیرمجاز از سامانه های رایانه ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سامانه، وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند علاوه بر رد مال به صاحب آن به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون(۲۰,۰۰۰,۰۰۰)ریال تا یکصد میلیون (۱۰۰,۰۰۰,۰۰۰)ریال یا هر دو مجازات محکوم خواهد شد.

فصل چهارم ـ جرائم علیه عفت و اخلاق عمومی

ماده ۷۴۲ (ماده۱۴ق . ج. ر) هرکس به وسیله سامانه‌های رایانه‌ای یا مخابراتی یا حامل های داده محتویات مستهجن را منتشر، توزیع یا معامله کند یا به قصد تجارت یا افساد تولید یا ذخیره یا نگهداری کند، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون (۵,۰۰۰,۰۰۰)ریال تا چهل میلیون (۴۰,۰۰۰,۰۰۰)ریال یا هر دو مجازات محکوم خواهد شد.

تبصره ۱- ارتکاب اعمال فوق درخصوص محتویات مبتذل موجب محکومیت به حداقل یکی از مجازاتهای فوق می شود.

محتویات و آثار مبتذل به آثاری اطلاق می گردد که دارای صحنه ها و صور قبیحه باشد.

تبصره ۲- هرگاه محتویات مستهجن به کمتر از ده نفر ارسال شود، مرتکب به یک میلیون (۱,۰۰۰,۰۰۰)ریال تا پنج میلیون (۵,۰۰۰,۰۰۰)ریال جزای نقدی محکوم خواهد شد.

تبصره ۳ـ چنانچه مرتکب اعمال مذکور در این ماده را حرفه خود قرار داده باشد یا به طور سازمان یافته مرتکب شود چنانچه مفسد فی الارض شناخته نشود، به حداکثر هر دو مجازات مقرر در این ماده محکوم خواهد شد.

تبصره ۴ـ محتویات مستهجن به تصویر، صوت یا متن واقعی یا غیرواقعی یا متنی اطلاق می‌شود که بیانگر برهنگی کامل زن یا مرد یا اندام تناسلی یا آمیزش یا عمل جنسی انسان است.

ماده ۷۴۳ (ماده۱۵ق . ج. ر) هرکس از طریق سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود، به ترتیب زیر مجازات خواهد شد:

الف) چنانچه به منظور دستیابی افراد به محتویات مستهجن، آنها را تحریک، ترغیب، تهدید یا تطمیع کند یا فریب دهد یا شیوه دستیابی به آنها را تسهیل نموده یا آموزش دهد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون (۵,۰۰۰,۰۰۰)ریال تا بیست میلیون (۲۰,۰۰۰,۰۰۰)ریال یا هردومجازات محکوم خواهدشد.

ارتکاب این اعمال در خصوص محتویات مبتذل موجب جزای نقدی از دومیلیون(۲,۰۰۰,۰۰۰)ریال تا پنج میلیون (۵,۰۰۰,۰۰۰)ریال است

ب) چنانچه افراد را به ارتکاب جرائم منافی عفت یا استعمال مواد مخدر یا روان‌گردان یا خودکشی یا انحرافات جنسی یا اعمال خشونت‌آمیز تحریک یا ترغیب یا تهدید یا دعوت کرده یا فریب دهد یا شیوه ارتکاب یا استعمال آنها را تسهیل کند یا آموزش دهد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون (۵,۰۰۰,۰۰۰)ریال تا بیست میلیون (۲۰,۰۰۰,۰۰۰)ریال یا هر دو مجازات محکوم می شود.

تبصره ـ مفاد این ماده و ماده (۱۴) شامل آن دسته از محتویاتی نخواهد شد که برای مقاصد علمی یا هر مصلحت عقلایی دیگر تهیه یا تولید یا نگهداری یا ارائه یا توزیع یا انتشار یا معامله می شود.

فصل پنجم ـ هتک حیثیت و نشر اکاذیب

ماده ۷۴۴ (ماده۱۶ق . ج. ر) هرکس به وسیله سامانه‌های رایانه‌ای یا مخابراتی، فیلم یا صوت یا تصویر دیگری را تغییر دهد یا تحریف کند و آن را منتشر یا با علم به تغییر یا تحریف منتشر کند، به نحوی که

عرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون(۵,۰۰۰,۰۰۰)ریال تا چهل میلیون (۴۰,۰۰۰,۰۰۰)ریال یا هر دو مجازات محکوم خواهد شد.

تبصره ـ چنانچه تغییر یا تحریف به صورت مستهجن باشد، مرتکب به حداکثر هر دو مجازات مقرر محکوم خواهد شد.

ماده ۷۴۵ (ماده۱۷ق . ج. ر) هرکس به وسیله سامانه‌های رایانه‌ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او جز در موارد قانونی منتشر کند یا در دسترس دیگران قرار دهد، به نحوی که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون(۵,۰۰۰,۰۰۰)ریال تا چهل میلیون (۴۰,۰۰۰,۰۰۰)ریال یا هر دو مجازات محکوم خواهد شد.

ماده ۷۴۶ (ماده۱۸ق . ج. ر) هر کس به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی به وسیله سامانه رایانه ای یا مخابراتی اکاذیبی را منتشر نماید یا در دسترس دیگران قرار دهد یا با همان مقاصد اعمالی را برخلاف حقیقت، رأساً یا به عنوان نقل قول، به شخص حقیقی یا حقوقی به طور صریح یا تلویحی نسبت دهد، اعم از این که از طریق یاد شده به نحوی از انحاء ضرر مادی یا معنوی به دیگری وارد شود یا نشود، افزون بر اعاده حیثیت (درصورت امکان)، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون(۵,۰۰۰,۰۰۰)ریال تا چهل میلیون (۴۰,۰۰۰,۰۰۰)ریال یا هر دو مجازات محکوم خواهد شد.

فصل ششم ـ مسؤولیت کیفری اشخاص

ماده ۷۴۷ (ماده۱۹ق . ج. ر) در موارد زیر، چنانچه جرائم رایانه‌ای به نام شخص حقوقی و در راستای منافع آن ارتکاب یابد، شخص حقوقی دارای مسؤولیت کیفری خواهد بود:

الف) هرگاه مدیر شخص حقوقی مرتکب جرم رایانه‌ای شود.

ب) هرگاه مدیر شخص حقوقی دستور ارتکاب جرم رایانه‌ای را صادر کند و جرم به وقوع بپیوندد.

ج) هرگاه یکی از کارمندان شخص حقوقی با اطلاع مدیر یا در اثر عدم نظارت وی مرتکب جرم رایانه‌ای شود.

د) هرگاه تمام یا قسمتی از فعالیت شخص حقوقی به ارتکاب جرم رایانه‌ای اختصاص یافته باشد.

تبصره ۱ـ منظور از مدیر کسی است که اختیار نمایندگی یا تصمیم‌گیری یا نظارت بر شخص حقوقی را دارد.

تبصره ۲ـ مسؤولیت کیفری شخص حقوقی مانع مجازات مرتکب نخواهد بود و درصورت نبود شرایط صدر ماده و عدم انتساب جرم به شخص خصوصی فقط شخص حقیقی مسؤول خواهد بود.

ماده ۷۴۸ (ماده۲۰ ق . ج. ر) اشخاص حقوقی موضوع ماده فوق، با توجه به شرایط و اوضاع و احوال جرم ارتکابی، میزان درآمد و نتایج حاصله از ارتکاب جرم، علاوه بر سه تا شش برابر حداکثر جزای نقدی جرم ارتکابی، به ترتیب ذیل محکوم خواهند شد:

الف) چنانچه حداکثر مجازات حبس آن جرم تا پنج سال حبس باشد، تعطیلی موقت شخص حقوقی از یک تا نُه ماه و در صورت تکرار جرم تعطیلی موقت شخص حقوقی از یک تا پنج سال.

ب) چنانچه حداکثر مجازات حبس آن جرم بیش از پنج سال حبس باشد، تعطیلی موقت شخص حقوقی از یک تا سه سال و در صورت تکرار جرم، شخص حقوقی منحل خواهد شد.

تبصره ـ مدیر شخص حقوقی که طبق بند «ب» این ماده منحل می‌شود، تا سه سال حق تأسیس یا نمایندگی یا تصمیم‌گیری یا نظارت بر شخص حقوقی دیگری را نخواهد داشت.

ماده ۷۴۹ (ماده۲۱ق . ج. ر) ارائه‌دهندگان خدمات دسترسی موظفند طبق ضوابط فنی و فهرست مقرر از سوی کارگروه(کمیته) تعیین مصادیق موضوع ماده ذیل محتوای مجرمانه که در چهارچوب قانون تنظیم شده است اعم از محتوای ناشی از جرایم رایانه ای و محتوایی که برای ارتکاب جرائم رایانه ای به کار می رود را پالایش (فیلتر) کنند. در صورتی که عمداً از پالایش(فیلتر) محتوای مجرمانه خودداری کنند، منحل خواهند شد و چنانچه از روی بی‌احتیاطی و بی‌مبالاتی زمینه دسترسی به محتوای غیرقانونی را فراهم آورند، در مرتبه نخست به جزای نقدی از بیست میلیون (۲۰,۰۰۰,۰۰۰)ریال تا یکصد میلیون (۱۰۰,۰۰۰,۰۰۰)ریال و در مرتبه دوم به جزای نقدی از یکصد میلیون (۱۰۰,۰۰۰,۰۰۰)ریال تا یک میلیارد (۱,۰۰۰,۰۰۰,۰۰۰)ریال و در مرتبه سوم به یک تا سه سال تعطیلی موقت محکوم خواهند شد.

تبصره ۱- چنانچه محتوای مجرمانه به تارنماهای (وب سایت های) مؤسسات عمومی شامل نهادهای زیرنظر ولی فقیه و قوای سه گانه مقننه، مجریه و قضائیه و مؤسسات عمومی غیردولتی موضوع قانون فهرست نهادها و مؤسسات عمومی غیردولتی مصوب ۱۳۷۳/۴/۱۹ و الحاقات بعدی آن یا به احزاب، جمعیت ها، انجمن های سیاسی و صنفی و انجمن های اسلامی یا اقلیت های دینی شناخته شده یا به سایر اشخاص حقیقی یا حقوقی حاضر در ایران که امکان احراز هویت و ارتباط با آنها وجود دارد تعلق داشته باشد، با دستور مقام قضائی رسیدگی کننده به پرونده و رفع اثر فوری محتوای مجرمانه از سوی دارندگان، تارنما (وب سایت)مزبور تا صدور حکم نهایی پالایش(فیلتر) نخواهدشد.

تبصره ۲- پالایش(فیلتر) محتوای مجرمانه موضوع شکایت خصوصی با دستور مقام قضائی رسیدگی کننده به پرونده انجام خواهد گرفت.

ماده ۷۵۰ (ماده۲۲ ق . ج. ر) قوه قضائیه موظف است ظرف یک ماه از تاریخ تصویب این قانون کارگروه(کمیته)تعیین مصادیق محتوای مجرمانه را در محل دادستانی کل کشور تشکیل دهد. وزیر یا نماینده وزارتخانه‌های آموزش و پرورش، ارتباطات و فناوری اطلاعات، اطلاعات، دادگستری، علوم، تحقیقات و فناوری، فرهنگ و ارشاد اسلامی، رئیس سازمان تبلیغات اسلامی، رئیس سازمان صدا و سیما و فرمانده نیروی انتظامی، یک نفر خبره در فناوری اطلاعات و ارتباطات به انتخاب کمیسیون صنایع و معادن مجلس شورای اسلامی و یک نفر از نمایندگان عضو کمیسیون قضائی و حقوقی به انتخاب کمیسیون قضائی و حقوقی و تأیید مجلس شورای اسلامی اعضای کارگروه(کمیته) را تشکیل خواهند داد. ریاست کارگروه(کمیته) به عهده دادستان کل کشور خواهد بود.

تبصره ۱- جلسات کارگروه(کمیته)حداقل هر پانزده روز یک بار و با حضور هفت نفر عضو رسمیت می یابد وتصمیمات کارگروه(کمیته) با اکثریت نسبی حاضران معتبر خواهد بود.

تبصره ۲- کارگروه(کمیته) موظف است به شکایات راجع به مصادیق پالایش(فیلتر)شده رسیدگی و نسبت به آنها تصمیم گیری کند.

تبصره ۳- کارگروه(کمیته) موظف است هر شش ماه گزارشی در خصوص روند پالایش(فیلتر) محتوای مجرمانه را به رؤسای قوای سه گانه و شورای عالی امنیت ملی تقدیم کند.

ماده ۷۵۱ (ماده ۲۳ ق . ج. ر) ارائه دهندگان خدمات میزبانی موظفند به محض دریافت دستور کارگروه(کمیته) تعیین مصادیق مذکور در ماده فوق یا مقام قضائی رسیدگی کننده به پرونده مبنی بر وجود محتوای مجرمانه در سامانه های رایانه‌ای خود از ادامه دسترسی به آن ممانعت به عمل آورند. چنانچه عمداً از اجرای دستور کارگروه(کمیته) یا مقام قضائی خودداری کنند، منحل خواهند شد. در غیر این صورت، چنانچه در اثر بی احتیاطی و بی مبالاتی زمینه دسترسی به محتوای مجرمانه مزبور را فراهم کنند، در مرتبه نخست به جزای نقدی از بیست میلیون(۲۰,۰۰۰,۰۰۰)ریال تا یکصد میلیون (۱۰۰,۰۰۰,۰۰۰)ریال و در مرتبه دوم به یکصد میلیون(۱۰۰,۰۰۰,۰۰۰)ریال تا یک میلیارد(۱,۰۰۰,۰۰۰,۰۰۰)ریال و در مرتبه سوم به یک تا سه سال تعطیلی موقت محکوم خواهند شد.

تبصره ـ ارائه دهندگان خدمات میزبانی موظفند به محض آگاهی از وجود محتوای مجرمانه مراتب را به کارگروه(کمیته) تعیین مصادیق اطلاع دهند.

ماده ۷۵۲ (ماده ۲۴ ق . ج. ر) هرکس بدون مجوز قانونی از پهنای باند بین‌المللی برای برقراری ارتباطات مخابراتی مبتنی بر پروتکل اینترنتی از خارج ایران به داخل یا برعکس استفاده کند, به حبس از یک تا سه سال یا جزای نقدی از یکصد میلیون(۱۰۰,۰۰۰,۰۰۰)ریال تا یک میلیارد(۱,۰۰۰,۰۰۰,۰۰۰)ریال یا هر دو مجازات محکوم خواهد شد.

فصل هفتم ـ سایر جرائم

ماده ۷۵۳ (ماده ۲۵ ق . ج. ر) هر شخصی که مرتکب اعمال زیر شود، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون(۵,۰۰۰,۰۰۰)ریال تا بیست میلیون (۲۰,۰۰۰,۰۰۰)ریال یا هر دو مجازات محکوم خواهد شد:

الف) تولید یا انتشار یا توزیع و در دسترس قرار دادن یا معامله داده‌ها یا نرم‌افزارها یا هر نوع ابزار الکترونیکی که صرفاً به منظور ارتکاب جرائم رایانه‌ای به کار می‌رود.

ب) فروش یا انتشار یا در دسترس قرار دادن گذرواژه یا هر داده‌ای که امکان دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی متعلق به دیگری را بدون رضایت او فراهم می‌کند.

ج) انتشار یا در دسترس قراردادن محتویات آموزش دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه ای و تخریب و اخلال در داده ها یا سیستم های رایانه ای و مخابراتی.

تبصره ـ چنانچه مرتکب، اعمال یاد شده را حرفه خود قرار داده باشد، به حداکثر هر دو مجازات مقرر در این ماده محکوم خواهد شد.

فصل هشتم ـ تشدید مجازات ها

ماده ۷۵۴ (ماده ۲۶ ق . ج. ر) در موارد زیر، حسب مورد مرتکب به بیش از دوسوم حداکثر یک یا دو مجازات مقرر محکوم خواهد شد:

الف) هر یک از کارمندان و کارکنان اداره ها و سازمان ها یا شوراها و یا شهرداری ها و موسسه ها و شرکت های دولتی و یا وابسته به دولت یا نهادهای انقلابی و بنیادها و مؤسسه هایی که زیر نظر ولی فقیه اداره می شوند و دیوان محاسبات و مؤسسه هایی که با کمک مستمر دولت اداره می شوند و یا دارندگان پایه قضائی و به طور کلی اعضاء و کارکنان قوای سه گانه و همچنین نیروهای مسلح و مأموران به خدمت عمومی اعم از رسمی و غیررسمی به مناسبت انجام وظیفه مرتکب جرم رایانه‌ای شده باشند.

ب) متصدی یا متصرف قانونی شبکه‌های رایانه‌ای یا مخابراتی که به مناسبت شغل خود مرتکب جرم رایانه ای شده باشد.

ج) داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی، متعلق به دولت یا نهادها و مراکز ارائه دهنده خدمات عمومی باشد.

د) جرم به صورت سازمان یافته ارتکاب یافته باشد.

هـ) جرم در سطح گسترده‌ای ارتکاب یافته باشد.

ماده ۷۵۵ (ماده ۲۷ ق . ج. ر) در صورت تکرار جرم برای بیش از دو بار دادگاه می تواند مرتکب را از خدمات الکترونیکی عمومی از قبیل اشتراک اینترنت، تلفن همراه، اخذ نام دامنه مرتبه بالای کشوری و بانکداری الکترونیکی محروم کند:

الف) چنانچه مجازات حبس آن جرم نود و یک روز تا دو سال حبس باشد، محرومیت از یک ماه تا یک سال.

ب) چنانچه مجازات حبس آن جرم دو تا پنج سال حبس باشد، محرومیت از یک تا سه سال.

ج) چنانچه مجازات حبس آن جرم بیش از پنج سال حبس باشد، محرومیت از سه تا پنج سال.

بخش دوم ـ آیین دادرسی

فصل یکم ـ صلاحیت

ماده ۷۵۶ (ماده ۲۸ ق . ج. ر) الی ماده ۷۷۹ (ماده ۵۱ ق.ج.ر) با ماده ۶۸۹ قانون آیین دادرسی کیفری مصوب ۱۳۹۲/۱۲/۰۴ از تاریخ لازم الاجرا شدن قانون آیین دادرسی کیفری مصوب ۱۳۹۴/۰۴/۰۱ صریحاً نسخ شده است [۴۲] .

بخش سوم ـ سایر مقررات

ماده ۷۸۰ (ماده ۵۲ ق . ج. ر) در مواردی که سامانه رایانه‌ای یا مخابراتی به عنوان وسیله ارتکاب جرم به کار رفته و در این قانون برای عمل مزبور مجازاتی پیش‌بینی نشده است، مطابق قوانین جزائی مربوط عمل خواهد شد.

---

[۴۲] ماده ٦٩٨ قانون آیین دادرسی کیفری – از تاریخ لازم‌الاجراء شدن این قانون، ماده واحده قانون راجع به تجویز دادرسی غیابی در امور جنایی مصوب ۲ /۳ /۱۳۳۹، قانون دادرسی نیروهای مسلح جمهوری اسلامی ایران مصوب ۲۲ /۲ /۱۳٦٤ به‌جز مواد (٤)، (۸) و (۹) آن قانون، قانون تشکیل دادگاههای کیفری (یک و دو) و شعب دیوان عالی کشور مصوب ۲۰ /٤ /۱۳٦۸، قانون تجدیدنظر آرای دادگاهها مصوب ١٦ /٥ /۱۳۷۲، **مواد (٧٥٦) الی (٧٧٩) الحاقی مورخ ٥ /٣ /١٣٨٨ به قانون مجازات اسلامی (تعزیرات و مجازاتهای بازدارنده)** و ماده (٥٦٩) قانون آیین‌دادرسی کیفری مصوب ٤ /١٢ /١٣٩٢ و اصلاحات و الحاقات بعدی آنها ملغی است.

تبصره ـ در مواردی که در بخش دوم این قانون برای رسیدگی به جرائم رایانه ای مقررات خاصی از جهت آیین دادرسی پیش بینی نشده است طبق مقررات قانون آیین دادرسی کیفری اقدام خواهد شد.

ماده ۷۸۱ (ماده ۵۳ ق . ج. ر) میزان جزاهای نقدی این قانون بر اساس نرخ رسمی تورم حسب اعلام بانک مرکزی هر سه سال یک بار با پیشنهاد رئیس قوه قضائیه و تصویب هیأت وزیران قابل تغییر است.

ماده ۷۸۲ (ماده ۵۴ ق . ج. ر) آیین نامه های مربوط به جمع آوری و استنادپذیری ادله الکترونیکی ظرف مدت شش ماه از تاریخ تصویب این قانون توسط وزارت دادگستری با همکاری وزارت ارتباطات و فناوری اطلاعات تهیه و به تصویب رئیس قوه قضائیه خواهد رسید.

ماده ۷۸۳ – کلیه قوانین مغایر با این قانون از جمله قانون مجازات عمومی مصوب ۱۳۰۴ و اصلاحات و الحاقات بعدی آن ملغی است .

فهرست مصادیق محتوای مجرمانه

الف) محتوای علیه عفت و اخلاق عمومی

۱ـ اشاعه فحشاء و منکرات (بند ۲ ماده ۶ قانون مطبوعات)

۲ـ تحریک، تشویق، ترغیب، تهدید یا دعوت به فساد و فحشاء و ارتکاب جرایم منافی عفت یا انحرافات جنسی (بند ب ماده ۱۵ قانون جرائم رایانه‌ای و ماده ۶۴۹ قانون مجازات اسلامی)

۳ـ انتشار، توزیع و معامله محتوای خلاف عفت عمومی (مبتذل و مستهجن) (بند ۲ ماده ۶ قانون مطبوعات و ماده ۱۴ قانون جرائم رایانه‌ای)

۴ـ تحریک، تشویق، ترغیب، تهدید یا تطمیع افراد به دستیابی به محتویات مستهجن و مبتذل (ماده ۱۵ قانون جرائم رایانه‌ای)

۵ـ استفاده ابزاری از افراد(اعم از زن و مرد) در تصاویر و محتوی، تحقیر و توهین به جنس زن، تبلیغ تشریفات و تجملات نامشروع و غیر قانونی (بند ۱۰ ماده ۶ قانون مطبوعات)

ب) محتوای علیه مقدسات اسلامی

۱ـ محتوای الحادی و مخالف موازین اسلامی (بند ۱ ماده ۶ قانون مجازات اسلامی)

۲ـ اهانت به دین مبین اسلام و مقدسات آن (ماده ۵۱۳ قانون مجازات اسلامی)

۳ـ اهانت به هر یک از انبیاء عظام یا ائمه طاهرین (ع) یا حضرت صدیقه طاهره (س) (ماده ۵۱۳ قانون مجازات اسلامی)

۴ـ تبلیغ به نفع حزب، گروه یا فرقه منحرف و مخالف اسلام (بند ۹ ماده ۶ قانون مطبوعات)

۵ـ تبلیغ مطالب از نشریات و رسانه‌ها و احزاب و گروه‌های داخلی و خارجی منحرف و مخالف اسلام به نحوی که تبلیغ از آنها باشد (بند ۹ ماده ۶ قانون مطبوعات)

۶ـ اهانت به امام خمینی (ره) و تحریف آثار ایشان (ماده ۵۱۴ قانون مجازات اسلامی)

۷ـ اهانت به مقام معظم رهبری و سایر مراجع مسلم تقلید (بند ۷ ماده ۶ قانون مطبوعات)

ج) محتوای علیه امنیت و آسایش عمومی

۱ـ تشکیل جمعیت، دسته، گروه در فضای مجازی (سایبر) با هدف برهم زدن امنیت کشور(ماده ۴۹۸ قانون مجازات اسلامی)

۲ـ هرگونه تهدید به بمبگذاری (ماده ۵۱۱ قانون مجازات اسلامی)

۳ـ محتوایی که به اساس جمهوری اسلامی ایران لطمه وارد کند (بند ۱ ماده ۶ قانون مطبوعات)

۴ـ انتشار محتوی علیه اصول قانون اساسی (بند ۱۲ ماده ۶ قانون مطبوعات)

۵ـ تبلیغ علیه نظام جمهوری اسلامی ایران (ماده ۵۰۰ قانون مجازات اسلامی)

۶ـ اخلال در وحدت ملی و ایجاد اختلاف ما بین اقشار جامعه به ویژه از طریق طرح مسائل نژادی و قومی (بند ۴ ماده ۶ قانون مطبوعات)

۷ـ تحریک نیروهای رزمنده یا اشخاصی که به نحوی از انحاء در خدمت نیروهای مسلح هستند به عصیان، فرار، تسلیم یا عدم اجرای وظایف نظامی (ماده ۵۰۴ قانون مجازات اسلامی)

۸ـ تحریص و تشویق افراد و گروه‌ها به ارتکاب اعمالی علیه امنیت، حیثیت و منافع جمهوری اسلامی ایران در داخل یا خارج از کشور (بند ۵ ماده ۶ قانون مطبوعات)

۹ ـ تبلیغ به نفع گروه‌ها و سازمان‌های مخالف نظام جمهوری اسلامی ایران (ماده ۵۰۰ قانون مجازات اسلامی)

۱۰ -فاش نمودن و انتشار غیر مجاز اسناد و دستورها و مسایل محرمانه و سری دولتی و عمومی (بند ۶ ماده قانون مطبوعات)

۱۱ـ فاش نمودن و انتشار غیر مجاز اسرار نیروهای مسلح (بند ۶ ماده قانون مطبوعات)

۱۲ـ فاش نمودن و انتشار غیر مجاز نقشه و استحکامات نظامی(بند ۶ ماده ۶ قانون مطبوعات)

۱۳ـ انتشار غیر مجاز مذاکرات غیر علنی مجلس شورای اسلامی (بند ۶ ماده ۶ قانون مطبوعات)

۱۴ـ انتشار بدون مجوز مذاکرات محاکم غیر علنی دادگستری و تحقیقات مراجع قضایی (بند ۶ ماده ۶ قانون مطبوعات)

د) محتوای علیه مقامات و نهادهای دولتی و عمومی

۱ـ اهانت و هجو نسبت به مقامات، نهادها و سازمان حکومتی و عمومی (بند ۸ ماده ۶ قانون مطبوعات و مواد ۶۰۹ و ۷۰۰ قانون مجازات اسلامی)

۲ـ افترا به مقامات، نهادها و سازمان حکومتی و عمومی (بند ۸ ماده ۶ قانون مطبوعات و ۶۹۷ قانون مجازات اسلامی)

۳ـ نشر اکاذیب و تشویش اذهان عمومی علیه مقامات، نهادها و سازمان‌های حکومتی (بند ۱۱ ماده ۶ قانون مطبوعات و ۶۹۸ قانون مجازات اسلامی)

هـ) محتوایی که برای ارتکاب جرایم رایانه‌ای و سایر جرایم بکار می رود

۱ـ انتشار یا توزیع و در دسترس قرار دادن یا معامله داده‌ها یا نرم افزارهای که صرفاً برای ارتکاب جرایم رایانه‌ای به کار می رود (ماده ۲۵ قانون جرائم رایانه‌ای)

۲ـ فروش، انتشار یا در دسترس قرار دادن غیر مجاز گذر واژه‌ها و داده‌هایی که امکان دسترسی غیر مجاز به داده‌ها با سامانه‌های رایانه‌ای یا مخابراتی دولتی یا عمومی را فراهم می کند (ماده ۲۵ قانون جرایم رایانه‌ای)

۳ـ انتشار یا در دسترس قراردادن محتویات آموزش دسترسی غیر مجاز، شنود غیر مجاز، جاسوسی رایانه‌ای، تحریف و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی (ماده ۲۵ قانون جرایم رایانه‌ای)

۴ـ آموزش و تسهیل سایر جرایم رایانه‌ای (ماده ۲۱ قانون جرایم رایانه‌ای)

۵ـ انجام هر گونه فعالیت تجاری و اقتصادی رایانه‌ای مجرمانه مانند شرکت‌های هرمی (قانون اخلال در نظام اقتصادی کشور و سایر قوانین)

۶ـ انتشار ویروس دهی بازی های رایانه‌ای دارای محتوای مجرمانه (مواد مختلف قانون مجازات اسلامی و قانون جرایم رایانه‌ای)

۷ـ انتشار فیلتر شکن ها و آموزش روش های عبور از سامانه های فیلترینگ (بند ج ماده ۲۵ قانون جرایم رایانه‌ای)

۸ـ تبلیغ و ترویج اسراف و تبذیر (بند ۳ ماده ۶ قانون مطبوعات)

۹ـ انتشار محتوای حاوی تحریک، ترغیب یا دعوت به اعمال خشونت آمیز و خودکشی (ماده ۱۵ قانون جرایم رایانه‌ای)

۱۰ـ تبلیغ و ترویج مصرف موادمخدر، مواد روان گردان و سیگار (ماده ۳ قانون جامع کنترل و مبارزه ملی با دخانیات ۱۳۸۵)

۱۱ـ باز انتشار و ارتباط (لینک) به محتوای مجرمانه تارنماها و نشانی های اینترنتی مسدود شده، نشریات توقیف شده و رسانه های وابسته به گروه ها و جریانات منحرف و غیر قانونی

۱۲ـ تشویق، تحریک و تسهیل ارتکاب جرائمی که دارای جنبه عمومی هستند از قبیل اخلال در نظم، تخریب اموال عمومی، ارتشاء، اختلاس، کلاهبرداری، قاچاق موادمخدر، قاچاق مشروبات الکلی و غیره (قانون مجازات اسلامی)

۱۳ـ انتشار محتوایی که از سوی شورای عالی امنیت ملی منع شده باشد.

۱۴ـ تشویق و ترغیب مردم به نقض حقوق مالکیت معنوی (ماده ۱ قانون حمایت از حقوق پدید آورندگان نرم افزارهای رایانه‌ای و ماده ۷۴ قانون تجارت الکترونیکی)

۱۵ـ معرفی آثار سمعی و بصری غیر مجاز به جای آثار مجاز (ماده ۱ قانون نحوه مجازات. اشخاصی که در امور سمعی و بصری فعالیت غیر مجاز دارند)

۱۶ـ عرضه تجاری آثار سمعی و بصری بدون مجوز وزارت فرهنگ و ارشاد اسلامی (ماده ۲ قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت غیر مجاز دارند)

قانون آیین دادرسی کیفری

بخش دهم ــ آیین دادرسی جرائم رایانه‌ای

ماده ۶۶۴ ـ علاوه بر موارد پیش‌بینی شده در دیگر قوانین، دادگاههای ایران صلاحیت رسیدگی به موارد زیر را دارند:

الف ـ داده‌های مجرمانه یا داده‌هایی که برای ارتکاب جرم به‌کار رفته‌اند که به هر نحو در سامانه‌های رایانه‌ای و مخابراتی یا حاملهای داده موجود در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری‌اسلامی‌ایران ذخیره شود.

ب ـ جرم از طریق تارنماهای دارای دامنه مرتبه‌بالای کد کشوری ایران (ir .) ارتکاب یابد.

پ ـ جرم توسط تبعه ایران یا غیرآن در خارج از ایران علیه سامانه‌های رایانه‌ای و مخابراتی و تارنماهای مورد استفاده یا تحت کنترل قوای سه‌گانه یا نهاد رهبری یا نمایندگی‌های رسمی دولت یا هر نهاد یا مؤسسه‌ای که خدمات عمومی ارائه می‌دهد یا علیه تارنماهای دارای دامنه مرتبه بالای کد کشوری ایران در سطح گسترده ارتکاب یابد.

ت ـ جرائم رایانه ای متضمن سوءاستفاده از اشخاص کمتر از هجده سال، اعم از اینکه بزه دیده یا مرتکب ایرانی یا غیرایرانی باشد و مرتکب در ایران یافت شود.

ماده ۶۶۵ ـ چنانچه جرم رایانه ای درصلاحیت دادگاههای ایران در محلی کشف یا گزارش شود، ولی محل وقوع آن معلوم نباشد، دادسرای محل کشف مکلف است تحقیقات مقدماتی را انجام دهد.

درصورتی‌که محل وقوع جرم مشخص نشود، دادسرا پس از اتمام تحقیقات مبادرت به صدور قرار و درصورت اقتضاء صدور کیفرخواست می کند و دادگاه مربوط نیز رأی مقتضی را صادر می‌کند.

ماده ۶۶۶ ـ قوه قضائیه موظف است به تناسب ضرورت، شعبه یا شعبی از دادسراها، دادگاههای کیفری یک، کیفری دو، اطفال و نوجوانان، نظامی و تجدیدنظر را برای رسیدگی به جرائم رایانه ای اختصاص دهد.

تبصره ـ مقامات قضائی دادسراها و دادگاههای مذکور از میان قضاتی که آشنایی لازم به امور رایانه دارند

انتخاب می‌شوند.

ماده ۶۶۷ ـ ارائه دهندگان خدمات دسترسی موظفند داده های ترافیک را حداقل تا شش‌ماه پس از ایجاد حفظ نمایند و اطلاعات کاربران را حداقل تا شش‌ماه پس از خاتمه اشتراک نگهداری کنند.

تبصره ۱ـ داده ترافیک، هرگونه داده ای است که سامانه های رایانه ای در زنجیره ارتباطات رایانه ای و مخابراتی تولید می‌کنند تا امکان ردیابی آنها از مبدأ تا مقصد وجود داشته باشد. این داده ها شامل اطلاعاتی از قبیل مبدأ، مسیر، تاریخ، زمان، مدت و حجم ارتباط و نوع خدمات مربوطه می شود.

تبصره ۲ـ اطلاعات کاربر، هرگونه اطلاعات راجع به کاربر خدمات دسترسی از قبیل نوع خدمات، امکانات فنی مورد استفاده و مدت زمان آن، هویت، نشانی جغرافیایی یا پستی یا قرارداد اینترنت(IP) ، شماره تلفن و سایر مشخصات فردی را شامل می‌شود.

ماده ۶۶۸ ـ ارائه‌دهندگان خدمات میزبانی داخلی موظفند اطلاعات کاربران خود را حداقل تا شش‌ماه پس از خاتمه اشتراک و محتوای ذخیره شده و داده ترافیک حاصل از تغییرات ایجادشده را حداقل تا پانزده روز نگهداری کنند.

ماده ۶۶۹ ـ هرگاه حفظ داده های رایانه ای ذخیره‌شده برای تحقیق یا دادرسی لازم باشد، مقام‌قضائی می تواند دستور حفاظت از آنها را برای اشخاصی که به نحوی تحت تصرف یا کنترل دارند صادر کند. در شرایط فوری، نظیر خطر آسیب دیدن یا تغییر یا از بین رفتن داده ها، ضابطان قضائی می توانند دستور حفاظت را صادر کنند و مراتب را حداکثر تا بیست و چهار ساعت به اطلاع مقام قضائی برسانند. چنانچه هر یک از کارکنان دولت یا ضابطان قضائی یا سایر اشخاص از اجرای این دستور خودداری یا داده های حفاظت شده را افشاء کنند یا اشخاصی که داده های مزبور به آنها مربوط می شود را از مفاد دستور صادره آگاه کنند، ضابطان قضائی و کارکنان دولت به مجازات امتناع از دستور مقام قضائی و سایر اشخاص به حبس از نود و یک روز تا شش‌ماه یا جزای نقدی از پنج تا ده میلیون ریال یا هردو مجازات محکوم می‌شوند.

تبصره ۱ـ حفظ داده ها به منزله ارائه یا افشاء آنها نیست و مستلزم رعایت مقررات مربوط است.

تبصره ۲ـ مدت زمان حفاظت از داده‌ها حداکثر سه‌ماه است و در صورت لزوم با دستور مقام قضائی قابل تمدید است.

ماده ۶۷۰ ـ مقام قضائی می تواند دستور ارائه داده های حفاظت شده مذکور در مواد (۶۶۷)، (۶۶۸) و (۶۶۹) این قانون را به اشخاص یاد شده بدهد تا در اختیار ضابطان قرار گیرد. خودداری از اجرای این دستور و همچنین عدم نگهداری وعدم مواظبت از این داده‌ها موجب مجازات مقرر در ماده (۶۶۹) این قانون می‌شود.

ماده ۶۷۱ ـ تفتیش و توقیف داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی به موجب دستور قضائی و در مواردی به عمل می آید که ظن قوی به کشف جرم یا شناسایی متهم یا ادله جرم وجود دارد.

ماده ۶۷۲ ـ تفتیش و توقیف داده ها یا سامانه های رایانه ای و مخابراتی در حضور متصرفان قانونی یا اشخاصی که به نحوی آنها را تحت کنترل قانونی دارند، نظیر متصدیان سامانه ها انجام می‌شود. درصورت عدم حضور یا امتناع از حضور آنان چنانچه تفتیش یا توقیف ضرورت داشته باشدیا فوریت امر اقتضاء کند، قاضی با ذکر دلایل دستور تفتیش و توقیف بدون حضور اشخاص مذکور را صادر می‌کند.

ماده ۶۷۳ ـ دستور تفتیش و توقیف باید شامل اطلاعاتی از جمله اجرای دستور در محل یا خارج از آن، مشخصات مکان و محدوده تفتیش و توقیف، نوع و میزان داده های مورد نظر، نوع و تعداد سخت افزارها و نرم افزارها، نحوه دستیابی به داده های رمزنگاری یا حذف شده و زمان تقریبی انجام تفتیش و توقیف باشد که به اجرای صحیح آن کمک می کند.

ماده ۶۷۴ ـ تفتیش داده‌ها یا سامانه‌های رایانه ای و مخابراتی شامل اقدامات ذیل می‌شود:

الف ـ دسترسی به تمام یا بخشی از سامانه های رایانه ای یا مخابراتی

ب ـ دسترسی به حاملهای داده از قبیل دیسکت ها یا لوحهای فشرده یا کارتهای حافظه

پ ـ دستیابی به داده های حذف یا رمزنگاری شده

ماده ۶۷۵ ـ در توقیف داده ها، با رعایت تناسب، نوع، اهمیت و نقش آنها در ارتکاب جرم، به روشهایی از قبیل چاپ داده ها، تصویربرداری از تمام یا بخشی از داده ها، غیرقابل دسترس کردن داده ها با

روشهایی از قبیل تغییرگذرواژه یا رمزنگاری و ضبط حاملهای داده عمل می‌شود.

ماده ۶۷۶ ـ در شرایط زیر سامانه های رایانه ای یا مخابراتی توقیف می‌شوند:

الف ـ داده های ذخیره شده به سهولت در دسترس نباشد یا حجم زیادی داشته باشد.

ب ـ تفتیش و تجزیه و تحلیل داده ها بدون سامانه سخت افزاری امکان پذیر نباشد.

پ ـ متصرف قانونی سامانه رضایت داده باشد.

ت ـ تصویربرداری از داده ها به لحاظ فنی امکان پذیر نباشد.

ث ـ تفتیش در محل باعث آسیب داده‌ها شود.

ماده ۶۷۷ ـ توقیف سامانه‌های رایانه‌ای یا مخابراتی متناسب با نوع و اهمیت و نقش آنها در ارتکاب جرم با روشهایی از قبیل تغییر گذرواژه به منظور عدم دسترسی به سامانه، مهر و موم (پلمب) سامانه در محل استقرار و ضبط سامانه صورت می‌گیرد.

ماده ۶۷۸ ـ چنانچه در حین اجرای دستور تفتیش و توقیف، تفتیش داده‌های مرتبط با جرم ارتکابی در سایر سامانه‌های رایانه‌ای یا مخابراتی که تحت کنترل یا تصرف متهم قرار دارند ضروری باشد، ضابطان با دستور مقام قضائی دامنه تفتیش و توقیف را به‌سامانه‌های دیگر گسترش می‌دهند و داده‌های مورد نظر را تفتیش یا توقیف می‌کنند.

ماده ۶۷۹ ـ توقیف داده ها یا سامانه های رایانه ای یا مخابراتی که موجب ایراد لطمه جانی یا خسارات مالی شدید به اشخاص یا اخلال در ارائه خدمات عمومی شود، ممنوع است مگر اینکه توقیف برای اجرای موضوع اهم نظیر حفظ امنیت کشور ضرورت داشته باشد.

ماده ۶۸۰ ـ در جایی که اصل داده ها توقیف می شود، ذی نفع حق دارد پس از پرداخت هزینه از آنها کپی دریافت کند، مشروط به اینکه ارائه داده های توقیف‌شده منافی با ضرورت کشف حقیقت نباشد و به روند تحقیقات لطمه ای وارد نسازد و داده ها مجرمانه نباشد.

ماده ۶۸۱ ـ در مواردی که اصل داده ها یا سامانه های رایانه ای یا مخابراتی توقیف می‌شود، قاضی موظف است با لحاظ نوع و میزان داده ها و نوع و تعداد سخت افزارها و نرم افزارهای مورد نظر و نقش

آنها درجرم ارتکابی، در مهلت متناسب و متعارف برای آنها تعیین تکلیف کند.

ماده ۶۸۲ ـ متضرر می‌تواند در مورد عملیات و اقدامات مأموران در توقیف داده‌ها و سامانه‌های رایانه‌ای و مخابراتی، اعتراض کتبی خود را همراه با دلایل ظرف ده روز به مرجع قضائی دستوردهنده تسلیم نماید. به درخواست یادشده خارج از نوبت رسیدگی می‌شود و قرار صادره قابل اعتراض است.

ماده ۶۸۳ ـ کنترل محتوای در حال انتقال ارتباطات غیرعمومی در سامانه های رایانه ای یا مخابراتی مطابق مقررات راجع به کنترل ارتباطات مخابراتی مقرر در آیین دادرسی کیفری است.

تبصره ـ دسترسی به محتوای ارتباطات غیرعمومی ذخیره شده، نظیر پیام‌نگار (ایمیل) یا پیامک در حکم کنترل و مستلزم رعایت مقررات مربوط است.

ماده ۶۸۴ ـ آیین‌نامه اجرائی نحوه نگهداری و مراقبت از ادله الکترونیکی جمع‌آوری‌شده ظرف شش‌ماه از تاریخ لازم‌الاجراء شدن این قانون توسط وزیر دادگستری با همکاری وزارت ارتباطات و فناوری اطلاعات تهیه می‌شود و به تصویب رئیس قوه قضائیه می‌رسد.

ماده ۶۸۵ ـ چنانچه داده های رایانه ای توسط طرف دعوی یا شخص ثالثی که از دعوی آگاهی ندارد، ایجاد یا پردازش یا ذخیره یا منتقل شود و سامانه رایانه ای یا مخابراتی مربوط به نحوی درست عمل کند که به صحت و تمامیت، اعتبار و انکارناپذیری داده ها خدشه وارد نشود، قابل استناد است.

ماده ۶۸۶ ـ کلیه مقررات مندرج در این بخش، علاوه بر جرائم رایانه ای شامل سایر جرائمی که ادله الکترونیکی در آنها مورد استناد قرار می گیرند نیز می شود.

ماده ۶۸۷ ـ در مواردی که در این بخش برای رسیدگی به جرائم رایانه‌ای مقررات خاصی از جهت آیین‌دادرسی پیش‌بینی نشده است، تابع مقررات‌عمومی آیین دادرسی کیفری است.