مجله حقوقی دادگستری

سال ۷۴/ شماره‌ی ۶۹/ بهار ۱۳۸۹/ صفحه ۳۷ تا ۷۹

جرایم مخابراتی

احسان زررخ[۱]

چکیده

بـا رشـد فزاینده‌ی تکنولوژی در عصـر اخیر، هر روز تغییرات شـگرفی در زندگی بشـر به وقـوع می‌پیوندد که دارای جنبه‌های مثبت و منفی اسـت؛ از جمله مهم‌ترین دسـتاوردها، پیشـرفت‌های مخابراتی و ارتباطی اسـت که طی چند دهه، بشـر را از مرحلـه‌ی تلگرام، تلگـراف و تلفن‌های اولیه خارج نمـوده و به مرحله‌ی تلفن‌های اینترنتی رسانیده است. این پیشرفت‌ها، ارتکاب جرایم بسیاری و از جمله جرایم مخابراتی را موجب شده است؛ جرایمی که می‌توان آن‌ها را در دو گروه جرایم مخابراتـی محض و جرایم مرتبط با مخابرات جـای داد؛ هر یک از این‌ها، خود طیف وسیعی از جرایم را در بر می‌گیرد.

جرایم نخست، مشـتمل بر جرایم ارتکابی به وسیله‌ی ابزارهای مخابراتی و نیز جرایم علیه سیسـتم‌های مخابراتی اسـت؛ اما، جرایم گروه دوم، جرایمی سنتی هستند که که ارتکاب آن‌ها با دستگاه‌های مخابراتی- ارتباطی دگرگون شده است.

در نظام حقوقی ایران، با وجود تلاش برای برای شـمول مصادیق این جرایم، برخی قانون‌گذاری‌های مصداقـی و محدود و تعدادی جرم‌انگاری‌های ناقص صورت گرفته اسـت؛ امری که نیازمند تغییر رویه قانون‌گذار و انجام اصلاحات ساختاری در این حوزه است.

واژگان کلیدی

دسـتگاه‌های مخابراتی، جرایم مخابراتی محض، جرایم مرتبط با مخابرات، قانون جرایم رایانه‌ای.

---

۱ کارشناسی ارشد حقوق کیفری و جرم‌شناسی.

۱. درآمد

مبنای زندگی جمعی انسـان‌ها بر ارتباطات و تعاملات میان آن‌ها اسـت؛ در حقیقت، اساس شکل‌گیری جوامع بشری بر روابط میان آن‌ها مستقر شده است. ایجاد ارتباط با دیگران خود نیازمند ابزارها و روش‌هایی است؛ که از ابتدایی‌ترین نوع آن در جوامع اولیه که شامل تصاویر و نقاشی‌های خالی از ظرافت و زیبایی بوده، شروع شده و به ابزارهای اعجاب‌برانگیز دوران ما رسیده است.

در عصر حاضر، رشد فزاینده‌ی فن‌آوری‌های ارتباطی[1] مخابراتی به شکل‌گیری فضای نوینی منجر شده است که تمامی یافته‌های سنتی در خصوص تعامل و ارتباط میان افراد را دسـتخوش تغییر کرده است. به راستی دیگر نمی‌توان با تفکرات سنتی و بـدون لحاظ جایگاه این فن‌آوری‌ها به بررسـی روابط میان افـراد و حتی جوامع با یکدیگر پرداخت.

این تحول عظیم با گسـترش ابزارهای مخابراتی که همچون تارهای عنکبوت افـراد و جوامـع را به هم متصل نموده‌اند، ایجاد شـده و به مرحله‌ای رسـیده اسـت کـه نمی‌توان نقش این وسـایل را انکار کـرد؛ خصوصاً از هنگامی‌کـه اینترنت پا به عرصه‌ی وجود گذاشـته است.[2] هرچند افرادی چون نایلور[3] این اظهارنظر را اغراق‌آمیز دانسته و این‌گونه استدلال می‌کنند: «مباحث اغراق‌آمیزی در خصوص نقش فن‌آوری صورت گرفته اسـت، از ابتدا تا اواسـط قرن نوزدهم اثر راه‌آهن، کشتی بخار و تلگراف

1. Information Technology

۲. نقش رایانه‌ها و اینترنت در شکل‌گیری نسل جدید مخابرات و ارتباطات به‌گونه‌ای است که نمی‌توان این دو را در بررسی جرایم مخابراتی نادیده گرفت؛ گرایش سیستم‌های مخابراتی موجود به سوی سیستم‌های هوشمند و به تعبیری رایانه‌ای شـدن سیستم‌های مخابراتی نیز موجب شده تا به سختی بتوان میان جرایم رایانه‌ای و مخابراتی قائـل به تفکیک شـد، اما در مجمـوع باید به کلیت جرایم خارج از فضای واقعـی و فیزیکی اذعان کرد. ناتوانی از طبقه‌بندی این دسـته از جرایم موجب شده تا اصطلاحات گوناگونی نسبت به جرایم خارج از فضای واقعی به کار گرفته شـود، که از جمله آن‌ها می‌توان به این موارد اشـاره کرد: جرم سـایبر (Cyber Crime)، جرم فن‌آوری بالا (High Tech Crime)، جرم رایانه‌ای (Computer Crime)، جرم فن‌آوری (Technology Crime)، جرم دیجیتالـی (Digital Crime)، جرم فن‌آوری اطلاعات (IT Crime)، جرم مجازی (Virtual Crime)، جرم شبکه (Net Crime) و جرم مخابراتی (Telecommunication Crime).

3. Naylor

بسیار انقلابی‌تر و تحول‌آمیزتر از نقش اینترنت و سفر با هواپیما بوده است. در واقع هر نوع جرمی‌که توسط ارتباطات الکترونیکی مدرن و فن‌آوری‌های ارتباطی نوین انجام می‌شود، مشابه چیزی در عصر تلگراف است، عصری که ... شرکت‌های تلگراف خودشان را با موارد نقض امنیت به وسیله تهدیدهای هکری مخصوصاً نقل و انتقال پول تلگرافی مواجه می‌دیدند.»[1]

به نظر می‌رسد باید این اظهارنظر را با دید خاصی تعدیل کرد و آن را مورد بررسی قرار داد؛ چه آن‌که ایشان تنها به نقش برخی از فن‌آوری‌های نوین ارتباطی چون اینترنت متعرض شده‌اند، نه به کلیت جایگاه فن‌آوری‌های ارتباطی - مخابراتی در جوامع؛ ایشان با پذیرش نقش ابزارهایی چون تلگراف که از نخستین ابزارهای مخابراتی غیرمستقیم است، به‌طور ضمنی به اهمیت جایگاه فن‌آوری‌های ارتباطی اذعان نموده‌اند.

در مقابل این نگرش، عده‌ی دیگری از حقوق‌دانان، با توجه به نقش فن‌آوری (اعم از مخابراتی و غیرمخابراتی) در تحقق جرایم، نظری مخالف داشته و جایگاه مهمی را برای آن در تحقق جرم ترسیم می‌کنند. در این میان نظرات زیتراین[2] و گرابوسکی[3] و اسمیت[4] معقول‌تر به نظر می‌رسد. زیتراین بیان می‌دارد که: «هرگونه رشد و توسعه‌ی فن‌آوری در درجات مختلف با طیف وسیع منبع باید فرصت مجرمانه‌ای به شمار آید. اعم از آن‌که هدف جرم، تسهیل‌کننده‌ی فعالیت‌های جنایی یا با سوءنیت باشد. به هرحال فرصت‌های ارتکاب جرم در چهارچوب فن‌آوری، به‌طور فزاینده‌ای افزایش یافته است.» (Schiek)

در این میان گرابوسکی و اسمیت، این‌گونه استدلال می‌کنندکه: «پیشرفت‌های فن‌آوری بیش از هر زمان دیگر توسعه یافته و مستحق بررسی و

1. See: http://www.rcmp-grc.gc.ca/html/cpu-cri.htm
2. Zittrain
3. Grabosky
4. Russel G. Smith

کنکاش ویژه‌ای هســتند؛ زیرا، خود فرصت جزایی ارتکاب جرم را به وجود آورده‌اند.» (Naylor,2002, p.1)

هدف این نوشــتار از مباحث مخابراتی، تنها بررســی فن‌آوری‌های مخابراتی دیجیتال اســت و به همین منظور از پرداختن به سایر ابزارهای مخابراتی چون پست، خودداری می‌شــود. البته شایان ذکر است که شیوه‌های پستی دیجیتالی مانند پست الکترونیک[1] و پیامک[2] مورد بررســی قــرار خواهند گرفت، چه آن‌که آن‌ها در مقوله‌ی وسایل مخابراتی دیجیتال قرار می‌گیرند.

این نوشــتار در دو قسمت نگارش یافته است؛ در ابتدا جرایم مخابراتی محض که تنها به وسیله‌ی ابزارهای ارتباطی - مخابراتی نوین قابلیت ارتکاب دارند، با تأکید بر قانون تجارت الکترونیکی و قانون جرایم رایانه‌ای بررســی می‌شــود. ســپس جرایم مرتبط با سیستم‌های مخابراتی بررسی می‌شود؛ جرایمی که این سیستم‌ها در تحقق آن‌ها نقش سازنده‌ای دارند و با قوانین موجود نیز قابل جرم‌انگاری و مجازات هستند.

پیش از ورود به بحث اصلی، به بیان دیدگاه‌ها و تعاریف ارائه شده در خصوص محیط‌ها و جرایم مخابراتی می‌پردازیم.

کانینگهــام در تعریف محیط‌های مخابراتی بیان مــی‌دارد: «محیط مخابراتی فضایی اســت که توســعه‌ی فن‌آوری ارتباطی الکترونیکی در اوایل قرن نوزدهم را در برگرفته، از تلگرام شــروع شده و به سیستم‌های بی‌سیم ختم می‌شود.» (Denning, p.42)

این تعریف در بردارنده‌ی ویژگی‌های اصلی فضاهای مخابراتی است، لکن این حدود و ثُغور در تعریف محیط‌های مخابراتی، با توجه به از میان رفتن‌کاربری بسیاری از ابزارهای آن از جمله تگراف و تلگرام، از محدوده‌ی بحث ما خارج می‌شــود. فضای مخابراتی مورد نظر در این نوشتار فضایی محدودتر است و به ابزارهایی می‌پردازد که

1. Electronic Mail (E-mail)
2. Short Message System (SMS)

در جهان امروز کاربرد دارند.

در رابطه با تعریف جرایم مخابراتی نیز دیدگاه‌های متفاوتی ارائه شـده است؛ در اینجا به دو مورد از آن‌ها شـاره می‌شـود که تقریباً سایر تعاریف و دیدگاه‌ها را نیز دربرمی‌گیرند.

نخسـتین تعریف از سوی «دِنینگ» ارائه شده است که بیان می‌دارد: «طیف فعالیت‌هـای مجرمانه کـه با نظام‌های مخابراتـی یا علیه نظام‌هـای مخابراتی صورت می‌گیرند، به نحو عجیبی گسترده است.»

(Grabosky, 1996, p.323; Grabosky, 1997, p.326)

تعریف دیگر که از سوی گرابوسکی و اسمیت ارائه شده، بدین مضمون است: «برخی از این فعالیت‌های مجرمانه حقیقتاً از نظر ماهیت بدیع نیسـتند، بلکه از نظر میانجی بودن بدیع هسـتند. در مجموع فعالیت‌های مجرمانه‌ی دیگر، معرف اشـکال جدیدی از کارهای نامشـروع هستند: اشـکال منحصر به فردی چون سرقت خدمات مخابراتی، دسترسـی نامشروع و... فعالیت‌های مجرمانه‌ی متضمن نظام‌های مخابراتی بـه عنـوان ابزار یا اهداف این موارد، الزاماً ... سـیاهه‌ی کاملی را تشـکیل نمی‌دهند، برعکس آن‌ها معرف پهنه‌های اولیه‌ی نگرانی‌های سیاست‌گذاران هستند.»[1]

از این تعاریف برمی‌آید که جرایم مخابراتی، شامل جرایم ارتکابی به وسیله‌ی ابزارهای مخابراتی و نیز جرایم ارتکابی علیه سیستم‌های مخابراتی است. از این رو به نظر می‌رسـد جرایم مخابراتی باید این‌گونه تعریف شود: فعل یا ترک فعل مجرمانه که با استفاده از وسایل و شبکه‌های ارتباطی - مخابراتی و یا علیه آن‌ها روی دهد و در قانون نیز برای آن مجازات تعیین شده باشد.

۲. جرایم مخابراتی محض

در این بخش با توجه به آنچه پیش‌تر گفته شـد، به بررسـی صُور خاص جرایم

1. See: http://www.itu.int/ti

مخابراتـــی که تنها با سیســـتم‌های مخابراتـــی یا علیه آن‌ها محقق می‌شـــوند، خواهیم پرداخـــت؛ در ایـــن میان به موارد مصرحه در قانون تجـــارت الکترونیکی و قانون جرایم رایانه‌ای و بررســـی قواعد حاکم بر آن‌ها خواهیم پرداخت. لذا، تلاش شـــده است تا حد امکان دسته‌بندی مطالب این بخش بر مبنای طبقه‌بندی صورت گرفته در قانون جرایم رایانه‌ای باشد.

۱-۲. جرایم علیه محرمانگی داده‌ها و سیستم‌های رایانه‌ای و مخابراتی

۱-۱-۲. دسترسی غیرمجاز

بـــه نظر می‌رســـد این عمل مجرمانه کـــه در ماده‌ی ۱ قانـــون جرایم رایانه‌ای نیز مورد اشـــاره قرار گرفته اســـت، در زمره‌ی جرایم خاص مخابراتی باشد. چه آن‌که، دسترسی غیرمجاز به محتویات سیستم‌های مخابراتی - رایانه‌ای تنها از طریق همین سیســـتم‌ها میسر است. به نظر می‌رسد این دسترسی به صورت مستقیم و با استفاده از سیستم‌هایی که فرد حق دسترسی به آن‌ها را ندارد و همچنین به نحو غیرمستقیم محقـــق می‌شـــود، به این صورت کـــه فرد از طریق سیســـتم دیگری و با اســـتفاده از شـــبکه‌های ارتباطی چون اینترنت یا بلوتوث، به آن سیســـتم وارد می‌شود. در هر دو فرض دسترسی غیرمجاز به سیستم‌های مخابراتی محقق شده است.

به نظر می‌رسد عنصر مادی این جرم، شامل اعمالی باشد که موجب اشراف و احاطـــه‌ی فرد بـــر داده‌هایی خارج از حیطه‌ی صلاحیت شـــود؛ ایـــن مهم باید به وســـیله‌ی ابزارهای مخابراتی- رایانه‌ای و علیه این سیســـتم‌ها صورت گرفته باشـــد. به‌نحوی‌که، سیستم مورد استفاده، همان سیستم هدف[1] (سیستم مورد حمله) بوده، که فرد صلاحیت دسترســـی به آن را نداشـــته یا این‌که این صلاحیت از وی ســـلب شده باشد.

پرسشـــی که ممکن اســـت مطرح شـــود، آن اســـت که اگر فرد در ابتدا مجوز

1. Target System

دسترســی به سیســتم را داشــته و به طور موقت این مجوز از وی سلب شده باشد و در مدت فقدان مجوز، اقدام به دسترســی نماید، آیا مشمول عنوان جزایی دسترسی غیرمجاز است؟ با توجه به ماهیت این جرم و این‌که صرف عدم اجاره، هرچند به طور موقت، برای تحقق آن کفایت می‌کند، عمل فرد مذکور منطبق با این عنوان مجرمانه است.

پــس از طــرح این مقدمات، به بررســی مــاده‌ی ۱ قانون جرایــم رایانه‌ای [۱]، می‌پردازیم؛ قید «هرکس» که در این ماده بدان اشاره شده، کلیت دارد و تمامی افراد را شــامل می‌شود، اما پرسشی که مطرح می‌شــود، آن است که اگر عملیات منجر به دسترسی غیرمجاز توسط چند نفر صورت گرفته باشد، بدین‌نحو که، هر یک بخشی از عملیات ورود به سیســتم را انجام داده، و این افراد زیرمجموعه‌ی یک شخص حقوقی باشــند، (فرضاً متخصصان یک شــرکت رایانه‌ای یا مخابراتی که برای شرکت و با نام شرکت اقدام به ورود به سیستم‌های رایانه‌ای می‌کنند)، آیا می‌توان مسؤولیت شخص حقوقی را مطرح کرد، یا این‌که باید به مسؤولیت افراد قائل شد؟

با توجه به نحوه‌ی نگارش این ماده و با رعایت شرایط ماده‌ی ۱۹ این قانون[۲]، به نظر می‌رســد شــخص حقوقی را بتوان مســؤول قلمداد کرد؛ افزون بر آن‌که، باید مسؤولیت فردی افراد دخیل در فعل مجرمانه دسترسی غیرمجاز را نیز جداگانه لحاظ نمود؛ هر چند قواعد مشــارکت و معاونت در جرم با توجه به نحوه‌ی دخالت آن‌ها در

---

۱. «هرکس به‌طور غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی که به‌وسیله تدابیر امنیتی حفاظت شده اســت دسترســی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.»

۲. «در موارد زیر چنان‌چه جرایم 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 ۱: منظور از مدیر کسی است که اختیار نمایندگی یا تصمیم‌گیری یا نظارت بر شخص حقوقی را دارد.

تبصره ۲: مسؤولیت کیفری شخص حقوقی مانع مجازات مرتکب نخواهد شد.»

عنصر مادی نیز متصور اســت. ضمن آن‌که، به نظر می‌رسد شخص حقوقی که حسب شرایط ماده‌ی ۱۹، عمل مجرمانه برای وی انجام شده باشد، را می‌توان از باب ضمان قهری به تأدیه‌ی ضرر و زیان‌های ناشی از فعل اعضایش، محکوم کرد.

پرسش دیگر این است که آیا دسترسی به داده‌ها بدون دسترسی به سیستم‌های رایانه‌ای و مخابراتی متصور است؟ برای پاسخ، ابتدا باید به تعریف داده‌پیام[1] در قانون تجارت الکترونیکی رجوع کرده، سپس تعاریف سیستم‌های رایانه‌ای و مخابراتی و نیز سیستم اطلاعاتی حفاظت شده (مطمئن)[2] را مورد بررسی قرار داد.

مطابق بند «الف» ماده‌ی ۲ قانون تجارت الکترونیکی، داده‌پیام، «هر نمادی از واقعه، اطلاعات یا مفهوم اســت که با وسایل الکترونیکی، نوری و یا فناوری‌های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود.»

در بند «و» ماده‌ی ۲ این قانون سیســتم رایانه‌ای[3] را نیز بدین شــکل تعریف کرده اســت: «هر نوع دســتگاه یا مجموعه‌ای از دســتگاه‌های متصل ســخت‌افزاری- نرم‌افزاری اســت که از طریق اجــرای برنامه‌های پردازش خــودکار «داده‌پیام» عمل می‌کند.»

بند «ح» ماده‌ی ۲ این قانون سیســتم اطلاعاتی حفاظت شــده را بدین‌شکل تعریف نموده اســت که «سیســتم اطلاعاتی اســت که: ۱- به نحوی معقول در برابر سوءاســتفاده و نفوذ محفوظ باشــد. ۲- ســطح معقولی از قابلیت دسترسی و تصدی صحیح را دارا باشــد. ۳- به نحوی معقول متناســب با اهمیت کاری که انجام می‌دهد پیکربندی و سازماندهی شده باشد. ۴- موافق با رویه ایمن باشد.»

در قانون تجارت الکترونیکی از سیســتم مخابراتی، تعریفی ارائه نشــده است، بــا توجــه به ماهیت آن قانــون، چنین امری منطقــی به نظر می‌رســد؛ بهتر آن بود

1. Data Message
2. Secure Information System
3. Computer System

تدوین‌کننـدگان قانون جرایم رایانـه‌ای حداقل به ارائه‌ی تعریف سیسـتم مخابراتی مطابق دیدگاه‌های خود اقدام می‌کردند.

با وجود این خلاء به نظر می‌رسـد سیسـتم مخابراتی را باید این‌گونه تعریف کرد: «هر نوع دسـتگاه با مجموعه‌ای از دستگاه‌های متصل الکترونیکی سخت‌افزاری- نرم‌افزاری، که کارکرد اصلی آن‌ها مخابره‌ی پیام و داده باشد.»

این تعریف اولاً، سیسـتم‌های سـنتی غیرالکترونیکی را با قید «الکترونیکی» از شـمول خود خارج می‌کند؛ ثانیاً، دسـتگاه‌های رایانـه‌ای را که کارکرد اصلی آن‌ها مخابره‌ی پیام نیسـت، با قید «کارکرد اصلی مخابره‌ی پیام» از شـمول دسـتگاه‌های مخابراتـی خـارج می‌کند؛ هر چند در حال حاضر سیسـتم‌های رایانـه‌ای با توجه به امکاناتی که شبکه‌ی جهانی اینترنت بدان‌ها داده است، کارکرد مخابراتی نیز یافته‌اند، ایـن روند به گونه‌ای اسـت کـه دسـتگاه‌های مخابراتی در حال کسـب ویژگی‌های دستگاه‌های رایانه‌ای هستند.

با این پیش‌زمینه‌ها، پاسـخ به پرسـش اخیر و سـایر سـؤالات مرتبط میسر خواهد بود؛ با توجه به تعریف داده‌پیام، پاسـخ، مثبت است؛ امکان دسترسی غیرمجاز به داده‌ها بدون نفوذ به سیسـتم‌های رایانه‌ای - مخابراتی میسـر اسـت، زیرا، مطابق تعریف مذکور هر نماد ذخیره شـده بر روی دسـتگاه‌های حامل داده چون کارت‌های حافظه‌ی موبایل‌ها، حامل‌های داده[1] و...، مشـمول عنوان داده‌پیام شـده و به اسـتناد ماده‌ی ۱ قانون جرایم رایانه‌ای دسترسـی غیرمجاز به این داده‌ها نیز مشـمول عنوان جزایی دسترسی غیرمجاز می‌شود.

موضوع دیگری که مطرح می‌شـود، آن اسـت که مقصود قانون‌گذار از عبارت «... که به وسـیله تدابیر امنیتی حفاظت شـده است» چیست؟ آیا همان شاخص‌های سیسـتم اطلاعاتی حفاظت شـده موضوع قانون تجارت الکترونیکی، مدنظر است؟ آیا این حفاظت تنها حفاظت نرم‌افزاری را شـامل می‌شـود و یا اعم از حفاظت نرم‌افزاری

1. Cool Disk

و سخت‌افزاری است؟

بـا توجـه به نوع نگارش مـاده‌ی ۱ قانـون جرایم رایانه‌ای به نظر می‌رسـد، معیارهای تدابیر امنیتی ارائه شده در آن، همان معیارهای ارائه شده در قانون تجارت الکترونیکی باشد؛ از سوی دیگر، به نظر می‌رسد هر دو نوع حفاظت مادی و غیرمادی (سـخت‌افزاری و نرم‌افزاری) مورد نظر قانون‌گذاران بوده باشـد، زیرا، اصطلاح تدابیر امنیتی عمومیت داشته و هر دو قسم را در برمی‌گیرد.

نکته‌ی دیگر در خصوص دسترسـی غیرمجاز، با تلفیق آن با بند «ب» ماده‌ی ۲۵ قانون جرایم رایانه‌ای[1] به دست می‌آید؛ پرسش این است که آیا قرار دادن گذرواژه یـا هر داده‌ای که امکان دسترسـی غیرمجاز را فراهم کنـد، عملی جز معاونت در بزه دسترسـی غیرمجاز است؟ پاسخ منفی است. لکن، قانون‌گذار برای مباشرت و معاونت مجازاتی واحد (نود و یک روز تا یک سـال حبس و پنج تا بیسـت میلیون ریال جزای نقدی و یا هر دو مجازات) مقرر نموده اسـت؛ از دید جرم‌شناسـی این عمل منطقی به نظر نمی‌رسـد و با اصول قانون‌نویسـی نیز در تضاد اسـت؛ بهتـر آن بود مجازات سنگین‌تری برای مباشر تعیین می‌شد.

آخریـن نکته آن‌که، در سـاختار موجـود و با توجه به ویژگی‌های سـاختار مخابراتی کشـور و نیز بی‌اطلاعی افراد، تبهکاران می‌توانند با در اختیار داشـتن خط تلفن (سیم‌کارت) افراد، حساب‌کابری خط خاصی را به حساب آن شخص وارد کنند؛ این عمل با استفاده از کدهای مخصوص و در ادامه، اضافه نمودن شماره‌ی مورد نظر قابل تحقق اسـت؛ پـس از آن کارکرد خط مورد نظر به خط قربانی اضافه می‌شـود، بـه این ترتیب وی باید آن مبلغ را نیز پرداخت کند؛ باتوجه به ویژگی‌های سـرقت و کلاهبرداری مخابراتی و سـایر جرایم مرتبط کـه در ادامه خواهد آمد، این موضوع با

---

۱. «هرکس مرتکب اعمال زیر شود، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شـد: ... ب) فروش یا انتشـار یا در دسترس قرار دادن گذرواژه یا هر داده‌ای که امکان دسترسی غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی متعلق به دیگری را فراهم می‌کند.»

هیچ یک از این جرایم منطبق نیســت؛ به نظر می‌رسد در وضعیت موجود تنها بتوان آن‌را در زمــره‌ی دسترســی غیرمجــاز قلمداد کرد، هر چند بهتر بــود به جای جرایم خُــردی که به طور مجزا به آن‌ها پرداخته شــده اســت، از عناویــن مجرمانه‌ای چون سوءاستفاده‌ی مالی از سیستم‌های مخابراتی- ارتباطی استفاده می‌شد.

۲-۱-۲. شنود غیرمجاز سیستم‌های مخابراتی

گســترش دســتگاه‌های ارتباطی از قبیل تلفن‌های ثابــت و همراه، تلفن‌های اینترنتی و غیره، به توسعه‌ی ارتباطات انجامیده است؛ این خود سبب توسعه‌ی جرایم مرتبط با آن‌ها شده است؛ جرایم شنود غیرمجاز از این جمله است.

این شــیوه‌ی تجاوز به محرمانگی داده‌ها، به وســیله‌ی سیستم‌های رایانه‌ای و همچنین با سیستم‌های مخابراتی محقق می‌شود. این عنوان مجرمانه در ماده‌ی ۲ قانون جرایم رایانه‌ای[۱] موردتوجه قانون‌گذار قرار گرفته اســت. به نظر می‌رسد امکان شنود به دو روش باشد: نخست آن‌که، نرم‌افزارهای ضبط مکالمات بر روی دستگاه‌های مخابراتی نصــب شــده و آن نرم‌افزارها بدون اطلاع فرد اقدام بــه ضبط تماس‌های وی می‌کنند.[۲] روش دوم شــنود مکالمات به وسیله‌ی دســتگاه‌هایی مجزا است که با ورود به فرکانس یا خط مورد اســتفاده‌ی فرد خاص، مکالمات وی را ضبط می‌کنند؛ به نظر می‌رسد هر دو روش را بتــوان بــا این ماده منطبق کرد. در خصــوص مکالمات اینترنتی نیز این دو شیوه کاربرد دارند، با این تفاوت‌که، در روش دوم به جای ورود به فرکانس یا خط مورد اســتفاده‌ی فرد خاص، به پایگاه ارائه‌دهنده‌ی این خدمت رجوع می‌شود و از طریق آن، مکالمات فرد مورد تعرض قرار می‌گیرد.

---

۱. «هرکس به طور غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی در سیســتم‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری را شنود کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.»

۲. برای آگاهی بیشــتر در خصوص این قســم از نرم‌افزارها و شیوه‌ی عملکرد آن‌ها، به پایگاه الکترونیکی شرکت killer mobile به آدرس www.killermobile.com رجوع کنید.

پرسشـــی که در این خصوص مطرح می‌شـــود، آن اســـت که آیا دسترسی به پیامک‌هـــای فرد را نیز می‌توان مشـــمول عنوان جزایی شـــنود غیرمجاز دانســـت؟ با توجـــه به نص این ماده پاســـخ منفی خواهد بود؛ دایره‌ی شـــمول ایـــن ماده پیام‌ها را در برنمی‌گیرد، اما، با توجه به پیشـــرفت ابزارهای مخابراتی و توانایی ارسال پیام‌های چندرسانه‌ای[1] به نظر می‌رســـد این ماده شنود پیام‌های چندرسانه‌ای را نیز در گرفته و به اســـتناد آن می‌توان این اعمال را جرم‌انگاری کرد؛ افزون بر این، به نظر می‌رســـد شنود پیام‌های صوتی در اتاق‌های گفت‌وگو[2] نیز مشمول عنوان شنود غیرمجاز باشد، ضمن آن‌که، شنود بی‌سیم‌های شخصی را نیز می‌توان مشمول حکم این ماده دانست؛ زیرا، این دستگاه‌ها که در زمره‌ی دستگاه‌های مخابراتی هستند، در ماده‌ی اخیر مورد حمایت قانون‌گذار قرار گرفته‌اند.

نکتـــه‌ی آخر آن‌که، به نظر می‌رســـد شـــنود محتـــوای ارتباطـــات از راه دور چندرســـانه‌ای کـــه نمونه‌ی بارز آن ویدیو کنفرانس‌ها هســـتند، را نیـــز بتوان با حکم مـــاده‌ی اخیر تطبیـــق داد؛ زیرا، این سیســـتم‌های ارتباطی مصداق بـــارز امواج نوری هســـتند که در ماده بدان‌ها اشـــاره شده است. البته پرســـش قابل طرح که به جرایم مخابراتی موضوع این نوشـــتار، ارتباط چندانی ندارد، آن است‌که سیستم‌های نوری و الکترومغناطیسی، در بردارنده‌ی امواج ماهواره‌ای و شبکه‌های ماکروویو نیز می‌شوند؛ چنین ابزارهایی نیز مشمول حکم این ماده قرار می‌گیرند.

البته شـــایان ذکر اســـت که در تمامی این فروض، جرایـــم ارتکابی باید علیه داده‌هـــای غیرعمومی صورت گیرنـــد، چه آن‌که، در غیر این صورت مشـــمول عنوان جزایی جاسوسی خواهند شد.

۳-۱-۲. جاسوسی مخابراتی

در جاسوســـی مخابراتی، افراد با مقاصد غیرشـــخصی و به سود یا علیه دولت

1. Multimedia Message
2. Chat Rooms

خاصی نسبت به وسایل عمومی به منظور به دست آوردن اطلاعات اقدام می‌کنند. در این صورت خاص بزهکاری، ممکن است فرد مرتکب سایر اَشکال جرایم مخابراتی و رایانه‌ای نیز بشود. این مهم در مواد ۳، ۴ و ۵ قانون جرایم رایانه‌ای مورد اشاره قرار گرفته و شرایطی نیز برای آن در ماده‌ی ۳ پیش‌بینی شده است.[۱]

نکته‌ی دیگر در خصوص جرم جاسوسی مخابراتی - رایانه‌ای، آن است که در ماده‌ی ۴ قانون یاد شده شروع به جاسوسی جرم‌انگاری شده است.[۲] این امر از اهمیت آن ناشی می‌شود؛ زیرا، این تأسیس را در جرایمی چون دسترسی یا شنود غیرمجاز نمی‌بینیم.

نکته‌ی دیگر در خصوص جاسوسی مخابراتی با توجه به ماده‌ی ۵ قانون مذکور [۳] آن است‌که قانون‌گذار برخلاف قانون مجازات اسلامی، افشای اطلاعات بر اثر بی‌احتیاطی، بی‌مبالاتی یا عدم رعایت تدابیر امنیتی را مستوجب مجازات دانسته است.

افزون بر این، با توجه به آن‌چه پیشتر در خصوص شنود غیرمجاز، گفته شد، به نظر می‌رسد آن مصادیق در صورتی‌که علیه داده‌های سری و عمومی باشد، مصداق این ماده خواهد بود. نکته‌ی دیگری آن‌که، اگر اشخاص از دستگاه‌های مخابراتی برای جاسوسی استفاده کنند، مشمول این ماده نخواهند بود؛ این موضوعی است که در بحث

---

۱. «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 تا شصت میلیون ریال یا هر دو مجازات. ب) در دسترس قرار دادن داده‌های مذکور برای اشخاص فاقد صلاحیت، به حبس از دو تا ده سال. ج) افشا یا در دسترس قرار دادن داده‌های مذکور برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آن‌ها، به حبس از پنج تا پانزده سال.»

۲. «هرکس به قصد دسترسی به داده‌های سری موضوع ماده (۳) این قانون، تدابیر امنیتی سیستم‌های رایانه‌ای یا مخابراتی را نقض کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.»

۳. «چنان‌چه مأموران دولتی که مسؤول حفظ داده‌های سری مقرر در ماده (۳) این قانون یا سیستم‌های مربوط هستند و به آن‌ها آموزش لازم داده شده است یا داده‌ها یا سیستم‌های مذکور در اختیار آن‌ها قرار گرفته است بر اثر بی‌احتیاطی، بی‌مبالاتی یا عدم رعایت تدابیر امنیتی موجب دسترسی اشخاص فاقد صلاحیت به داده‌ها، حامل‌های داده یا سیستم‌های مذکور شوند، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات و انفصال از خدمت از شش ماه تا دو سال محکوم خواهند شد.»

جرایم مرتبط با دستگاه‌های مخابراتی، بدان اشاره خواهد شد.

۲-۲. جرایم علیه صحت و تمامیت داده‌ها و سیستم‌های رایانه‌ای و مخابراتی

۱-۲-۲. جعل رایانه‌ای - مخابراتی

عنصر مادی جرم جعل رایانه‌ای و مخابراتی در تغییر، ایجاد، وارد کردن و حذف کردن تمام یا قسمتی از داده‌ها است. مطابق قواعد کلی حاکم بر جعل در قانون مجازات اسلامی و قواعد پذیرفته شده‌ی حقوق جزا، جعل بر دو قسم مادی و معنوی است، به نظر می‌رسد هر دو نوع جعل به یکی از طرق یاد شده قابلیت تحقق دارند. این دسته‌بندی در ماده‌ی ۶ قانون جرایم رایانه‌ای[۱] پیش‌بینی شده است، صُور خاص فوق نیز مدنظر قانون‌گذار بوده است.

علاوه بر این، قانون‌گذار در ماده‌ی ۷ قانون مذکور[۲] به استفاده از داده‌های مجعول اشاره کرده و این مورد را نیز جرم‌انگاری کرده است. شایان ذکر است که با توجه به قواعد کلی حاکم بر تعدد و نیز متفاوت بودن جعل از استفاده، جعل مخابراتی و استفاده از آن دو جرم مختلف بوده و مشمول قاعده‌ی تعدد مادی و جمع مجازات‌ها است.

لازم به ذکر است که در قانون یاد شده، تفاوت‌هایی که در قانون مجازات اسلامی، میان اسناد وجود دارد، لحاظ نشده و داده‌ها به طور مطلق مورد حمایت یکسان قرار گرفته‌اند؛ اعم از آن‌که داده‌ای رسمی باشد و یا غیررسمی.

در این میان چند پرسش مطرح می‌شود؛ نخست آن‌که، این قانون هرگونه

---

۱. «هرکس به طور غیرمجاز مرتکب اعمال زیر شود، جاعل محسوب و به حبس از یک تا پنج سال یا جزای نقدی از بیست تا یکصد میلیون ریال یا هر دو مجازات محکوم خواهد شد: الف) تغییر داده‌های قابل استناد یا ایجاد یا وارد کردن متقلبانه‌ی داده‌ها، ب) تغییر داده‌ها یا علایم موجود در کارت‌های حافظه یا قابل پردازش در سیستم‌های رایانه‌ای یا مخابراتی یا تراشه‌ها یا ایجاد یا وارد کردن متقلبانه داده‌ها یا علایم به آن‌ها.»

۲. «هرکس با علم به مجعول بودن داده‌ها یا کارت‌ها یا تراشه‌ها از آن‌ها استفاده کند، به مجازات مندرج در ماده فوق محکوم خواهد شد.»

تغییر در داده‌ها را مشـــمول عنوان جعل دانســـته اســـت و این در حالی است که داده شامل تمامی فایل‌های متنی، تصویری، صوتی و... می‌شود؛ حال اگر شخصی با استفاده از سیســـتم‌های رایانه‌ای - مخابراتی اقدام به تغییر صدای دیگری کند و سیستم‌های شناسایی صوتی را فریب دهد، مورد از مصادیق این نوع جعل خواهد بود؟ با توجه به عام‌الشمول بودن حکم ماده‌ی ۶ قانون جرایم رایانه‌ای این مورد از مصادیق بارز تغییر در داده‌ها بوده و مشمول عنوان جزایی جعل رایانه‌ای است.

اکنون این پرسش مطرح می‌شود که اگر «الف» با این روش سیستم شناسایی صوتی را فریب دهد و به جای «ب» وارد محلی شود که حق ورود به آن را ندارد، این عمل علاوه بر جعل رایانه‌ای عنوان دیگری نیز محسوب می‌شود که از آن به «سرقت هویـــت»[1] یـــاد کرده‌اند. البته این عمـــل مجرمانه تنها به این روش محقق نمی‌شـــود؛ سوءاستفاده از سایر داده‌ها، برای استفاده از نام و عنوان دیگری نیز مشمول این عنوان جزایی خواهد بود. قانون‌گذار می‌بایست به صراحت نسبت به جرم‌انگاری این عمل در قانون جرایم رایانه‌ای، اقدام می‌کرد.

۲-۲-۲. تخریب و اخلال در داده‌ها یا سیستم‌های رایانه‌ای - مخابراتی

نخســـتین تصوری که پس از شنیدن این واژه به ذهن متبادر می‌شود، از بین بردن و نابودی مادی و فیزیکی اجســـام و اشیاء اســـت، درحالی‌که، تخریب در فضای غیرمادی و در وسایل مخابراتی نیز متصور بوده و با آنچه در دنیای واقعی مطرح است و قواعد آن نیز در قوانین جزایی آمده، متفاوت است.

قانون‌گـــذار در قانون جرایم رایانه‌ای، عناویـــن مجرمانه‌ی تخریب و اخلال در داده‌ها یا سیستم‌های رایانه‌ای - مخابراتی را در یک مبحث آورده و مواد ۸ تا ۱۱ این قانون را به آن‌ها اختصاص داده است.

1. Identity Theft

از حکم مطروحه در ماده‌ی ۸ [۱] این قانون چنین استنباط می‌شود که حکم این ماده موارد غیرعمدی را در بر نمی‌گیرد. دیگر آن‌که نحوه‌ی نگارش ماده به‌گونه‌ای است که داده‌های متعلق به دیگری را هرچند در سیستمی غیر از سیستم دارنده‌ی آن‌ها باشد، نیز در بر می‌گیرد. در این خصوص چند نکته قابل توجه است؛ نخست آن‌که، در این ماده قانون‌گذار میان حذف قابل بازگشت و بدون بازگشت داده‌ها تفاوتی قائل نشده و هر دو نوع را مشمول یک میزان مجازات دانسته است. نکته‌ی دیگر آن که، در پیش‌نویس‌های سابق به واژه‌ی «ضرر» اشاره شده، حال آن‌که در نسخه‌ی اخیر که به تصویب کمیسیون رسیده است، این واژه حذف شده است. به نظر می‌رسد اگر فعل شخص موجب ایراد ضرر به دیگری شود، فرد زیان‌زننده از باب مسؤولیت مدنی، مسؤول جبران خسارت خواهد بود؛ اطلاق ماده‌ی ۸ و نیز مواد ۹ [۲] و ۱۰ [۳] قانون می‌تواند مؤید این تفسیر باشد؛ افزون این معلوم نیست که آیا صرفاً ضرر مادی می‌توان مطالبه کرد یا ضرر معنوی هم قابل مطالبه است؟ زیرا، ممکن است «الف» وارد سیستم «ب» شده و عکس‌های غیرحرفه‌ای وی را به یکی از روش‌های مذکور در مواد ۸ یا ۹ قانون جرایم رایانه‌ای تخریب کند، در این حالت ضرر مالی به «ب» وارد نشده، بلکه موجب ضرر معنوی شده است. به نظر می‌رسد تفاوت عمده مواد ۸ و ۹ این قانون در مصادیق و نیز ابزارهایی است که در جرایم تخریب و اخلال ممکن است، رخ دهد.

۱. «هرکس به‌طور غیرمجاز داده‌های دیگری را از سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده حذف یا تخریب یا مختل یا غیرقابل پردازش کند به حبس از شش ماه تا دو سال یا جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.»

۲. «هرکس به طور غیرمجاز با انجام اعمالی از قبیل وارد کردن، انتقال دادن، پخش، حذف کردن، متوقف کردن، دستکاری یا تخریب داده‌ها یا امواج الکترومغناطیسی یا نوری، سیستم‌های 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 تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.»

۳. «هرکس به طور غیرمجاز با انجام اعمالی از قبیل مخفی‌کردن داده‌ها، تغییر گذرواژه یا رمزنگاری داده‌ها مانع دسترسی اشخاص مجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی شود، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.»

۳-۲. سرقت رایانه‌ای - مخابراتی

تحقق سرقت رایانه‌ای، مستلزم آن است که داده‌های رایانه‌ای، مال تلقی شود. تا به تبع آن سرقت نیز قابل تحقق باشد؛ به عبارت دیگر، مقدمه‌ی تحقق بزه سرقت رایانه‌ای آن است که داده‌های رایانه‌ای، مال محسوب شوند. با توجه به خرید و فروش نرم‌افـزار، نام‌هـای دامنه و... در عصر حاضر و پرداخت مبالـغ هنگفتی در ازای آن‌ها، تردیدی نیست که این امور در زمره‌ی اموال هستند.

نخستین نکته آن‌که در قانون جرایم رایانه‌ای از سرقت و کلاهبرداری مرتبط با رایانه یاد شـده، اما، تمامی مصادیق مطروحه در آن سرقت و کلاهبرداری رایانه‌ای است.

دومین نکته آن‌که محروم کردن فرد از مال خویش، یکی از مهم‌ترین سرقت است؛ حال آن‌که، فرض مطروحه در ماده‌ی ۱۲ قانون جرایم رایانه‌ای[۱]، هنگامی است که «عین داده‌ها در اختیار صاحب آن باشد»، لذا، اصولاً به علت عدم تحقق این شرط بنیادین ربایشی صورت نگرفته تا مشمول عنوان جزایی سرقت باشد؛ بنابراین، به نظر می‌رسـد، صحیح آن است که این عمل مشـمول عنوان جزایی دسترسی غیرمجاز به داده‌ها تلقی شـود و نه سـرقت، زیرا، در این فرض محرومیت از مال هرچند به طور موقت نیز محقق نشده است.

با توجه به سـاختار موجود درخصوص این بزه به نظر می‌رسـد عنصر مادی سرقت رایانه‌ای - مخابراتی بدین نحو باشد که فرد خاطی با ورود به داده‌های سیستم قربانـی، اطلاعات او را بردارد (به نوعی مقدمه‌ی تحقق جرم سـرقت، ورود غیرقانونی اسـت)؛ این عمل به دو صورت محقق می‌شـود، نخسـت آن‌که، فرد عین داده‌ها را از سیسـتم قربانی به سیسـتم خود منتقل کرده و قربانی را از داده‌های موجود بر روی سیسـتمش محروم کند، دیگر آن‌که، یک نسـخه از داده‌های موجود بر روی سیستم

۱. «هرکس به طور غیرمجاز داده‌های متعلق به دیگری را برباید، چنان‌چه عین داده‌ها در اختیار صاحب آن باشد، به جزای نقدی از یک تا بیست میلیون ریال و در غیر این صورت به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.»

قربانی را بر روی سیستم خویش کپی کرده و از فروش آن‌ها منفعت کسب کند. به نظر می‌رسد روش نخست را بتوان با توضیحات پیش گفته، با عنوان جزایی سرقت منطبق نمود، اما، شیوه‌ی دوم به بزه تحصیل نامشروع نزدیک‌تر است تا سرقت؛ زیرا، مبنای اساسی سرقت محروم نمودن فرد از اموالش می‌باشد؛ حا آن‌که، در این فرض چنین نبوده و صرفاً امکان بهره‌برداری از آن‌ها برای فرد دیگری محقق شده است.

۴-۲. کلاهبرداری رایانه‌ای - مخابراتی

به طور کلی عنصر مادی بزه کلاهبرداری مشتمل بر سه رکن مانور متقلبانه، فریب و تحصیل مال است؛ این عناصر در تحقق کلاهبرداری رایانه‌ای - مخابراتی نیز باید لحاظ شوند. البته به نظر می‌رسد عده‌ای بر این اساس که در کلاهبرداری رایانه‌ای نیازی به تحقق عنصر فریب نیست، میان کلاهبرداری رایانه‌ای و کلاهبرداری کلاسیک که با رایانه صورت می‌گیرد، قائل به تفکیک شده‌اند، (میرمحمد صادقی، ۱۳۸۶، صص ۹۲-۹۱) حال آن‌که در ماده‌ی ۶۷ قانون تجارت الکترونیکی[1] فریب دیگران و یا گمراهی سیستم‌های رایانه‌ای - مخابراتی مورد توجه قرار گرفته است؛ این درحالی است که در ماده‌ی ۱۳ قانون جرایم رایانه‌ای[2] شرط فریب مطرح نشده و طراحان آن به تبعیت از ماده‌ی ۸ کنوانسیون جرایم سایبری این قید را بیان نکرده‌اند، البته به استناد ماده‌ی ۵۷ قانون مذکور تمام قوانین مغایر این قانون ملغی است.

---

۱. «هر کس در بستر مبادلات الکترونیکی، با سوءاستفاده و یا استفاده غیرمجاز از داده پیام‌ها، برنامه‌ها و سیستم‌های رایانه‌ای و وسایل ارتباط از راه دور و ارتکاب افعالی نظیر ورود، محو، توقف داده پیام مداخله در عملکرد برنامه یا سیستم رایانه‌ای و غیره دیگران را بفریبد و یا سبب گمراهی سیستم‌های پردازش خودکار و نظایر آن شود و از این طریق برای خود یا دیگری وجوه، اموال یا امتیازات مالی تحصیل کند و اموال دیگران را ببرد مجرم محسوب و علاوه بر رد مال به صاحبان اموال به حبس از یک تا سه سال و پرداخت جزای نقدی معادل مال مأخوذه محکوم می‌شود. تبصره: شروع به این جرم نیز جرم محسوب و مجازات آن حداقل مجازات مقرر در این ماده می‌باشد.»

۲. «هرکس به طور غیرمجاز از سیستم‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل‌کردن سیستم، 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 تا یکصد میلیون ریال یا هر دو مجازات محکوم خواهد شد.»

نکته‌ی حائز اهمیت آن‌که اســتفاده از سیستم‌های رایانه‌ای - مخابراتی برای کلاهبــرداری و بــردن مال افراد با روش‌های خاصی متصور اســت، در مواد اخیر، این روش‌ها لحاظ شــده‌اند. ایــن دیدگاه در خصوص نیاز یا عدم نیــاز به عنصر فریب در کلاهبرداری رایانه‌ای در مواردی ایجاد شبهه می‌کند، برای مثال «الف» ارسال پیامکی برای «ب» که دارای خط ارائه‌کننده‌ی خدمات به وی اســت، نموده و خود را متولی سیســتم اعتبارات شــبکه معرفی کرده و بیان می‌دارد که وی در قرعه‌کشــی شرکت ایرانســل برنده‌ی کد اعتباری شــده و از «ب» می‌خواهد کد شارژ فعلی خود را برای وی ارسال کند تا کد شارژ با اعتبار بیشتر برای او ارسال شود، «ب» که فریب خورده است اقدام به این کار می‌کند و «الف» تمامی اعتبار او را مصرف می‌کند. طبق تعریف مقرر در ماده‌ی ۱۳ قانون جرایم رایانه‌ای این مثال را نمی‌توان کلاهبرداری دانســت؛ ضمن آن‌که، مطابق عمومات راجع به ســرقت نمی‌توان آن را ســرقت نامید، زیرا، در تحقق بزه سرقت، بردن مال فرد بدون رضایت وی شرط است، حال آن‌که در این مثال این‌گونه نیســت. به نظر می‌رسد در کلاهبرداری رایانه‌ای - مخابراتی، اعم از آن‌که بر روی سیســتم‌ها و یا اشخاص صورت گیرد، وجود عنصر فریب ضروری است؛ زیرا، در غیر این صورت با خلاء قانونی در تفکیک جرایم سرقت و کلاهبرداری رایانه‌ای مواجه خواهیم شــد. جرایمی مشــابه مثال فوق را نمی‌توانیم در قالــب اصولی که در قانون جرایم رایانه‌ای تبیین کرده‌ایم، قرار دهیم؛ بنابر این، باید آن‌ها را در قالب جرم دیگری به نام فیشینگ[1] بررسی کنیم.

۵-۲. فیشینگ

در قلمرو امنیت رایانه‌ای، حملات فیشــینگ عبارت اســت از ترغیب کاربران به افشــای اطلاعات محرمانه‌ی شخصی با استفاده از هویت‌های قلابی و ساختگی. در تجارت الکترونیکی، فیشینگ به تلاش برای دستیابی به اطلاعات حساس افراد مانند

1. Phishing

نـام کاربری، کلمه‌ی عبور و اطلاعات کارت‌های اعتباری، به‌وسـیله‌ی معرفی خود به عنوان یک سایت مورد اطمینان، اطلاق می‌شود.[۱]

فیشـینگ در عمـل به صـورت کپی دقیق رابـط گرافیکی یک وب سـایت معتبر مانند بانک‌های آن‌لاین اسـت که دربردارنده‌ی بانک‌های موجود در شـبکه‌ی جهانی اینترنت و شـبکه‌های اعتباری موجود در سیسـتم‌های مخابراتی نیز می‌شود. در فیشـینگ آن‌لاین ابتدا کاربر از طریق ایمیل و یا آگهی‌های تبلیغاتی سـایت‌های دیگر به یک صفحه‌ی قلابی راهنمایی می‌شـود، سپس از کاربر درخواست می‌شود تا اطلاعاتی را مانند اطلاعات کارت اعتباری که می‌تواند مهم و حساس باشد، وارد کند. در صورت گمراه شـدن کاربر و وارد کردن اطلاعات، فیشرها به اطلاعات شخصی وی دسترسی می‌یابند. نخستین مورد گزارش شده‌ی فیشینگ مربوط به دوم ژانویه سال ۱۹۹۶ میلادی است که بر روی گروه خبری یوزنت[۲] انجام شد. با توجه به اهمیت بزه فیشـینگ در جرایم مخابراتی و لزوم آشـنایی با عناصر متشکله‌ی آن، در این قسمت به اجزای این جرم و خصوصاً فیشینگ تلفنی پرداخته می‌شود.

الف) دسـتکاری پیونـد: در این تکنیک بـرای گمراه کردن کاربر از اسـامی معتبری در آدرس اسـتفاده می‌شـود، مانند اسـتفاده از زیردامنه‌ی آشنای Gmail در www.gmail.Phisher.com، کـه در واقع کاربر را به سـایت Phisher هدایت می‌کند.

ب) گریز از فیلترها: فیشـرها برای جلوگیری از شناسـایی متن‌های متداول فیشـینگ در ایمیل توسط فیلترهای ضد فیشینگ، به جای نوشته، از عکس استفاده می‌کنند.

ج) جعل وب سـایت: برخی از فیشرها از جاوا اسکریپت برای تغییر آدرس در نوار آدرس مرورگر استفاده می‌کنند تا هیچ جای شکی برای قربانی باقی نماند. مهاجم

---

۱. به نقل از تعریف ارائه شده در دانشنامه‌ی آزاد ویکیپدیا، آدرس:
http://en.wikipedia.org/wiki/Phishing
2. Usenet

حتی می‌تواند از ایرادهای موجود در اسکریپت‌های یک سایت معتبر نیز علیه خودش استفاده کند؛ به این نوع حمله Cross-Site Scripting گفته می‌شود؛ در این مورد از کاربر خواسته می‌شود تا در بانک خودش لاگین کند.

ظاهراً همه چیز عادی است؛ از آدرس وب سایت گرفته تا گواهی‌نامه‌ی امنیتی[1]؛ اما، در واقع، پیوند به آن وب سایت دستکاری می‌شود تا با استفاده از عیب‌های موجود در اسکریپت‌های آن وب سایت، حمله انجام شود. از این روش در سال ۲۰۰۶ برای حمله به وب سایت PayPal [2] استفاده شد.

د) فیشینگ تلفنی: تمام حملات فیشینگ نیازمند وب سایت قلابی نیست. پیام‌هایی‌که ظاهراً از طرف بانک فرستاده شده و از کاربر می‌خواهد تا مثلاً به دلیل وجود ایراد در حسابشان، شماره‌ی خاصی را شماره‌گیری کنند، نیز می‌تواند حمله‌ی فیشینگ باشد؛ پس از گرفتن شماره (که متعلق به فیشر است و با سرویس صدا از طریق IP مهیا شده است)، از کاربر خواسته می‌شود تا شماره حساب و پین[3] خود را وارد کند. مثالی که پیش‌تر در خصوص تخلیه‌ی اعتبار خطوط اعتباری آورده شد، نیز از همین نوع است.

۶-۲. ترمینیشن[4] و اورجینیشن[5]

ترمینیشن به معنای مکالمات از خارج به داخل و اورجینیشن به معنای مکالمات از داخل به خارج است. در این میان جرم مهمی‌که ممکن است به وقوع بپیوندد، قاچاق مخابرات است، که از سوی شرکت‌های ارائه‌کننده‌ی خدمات مخابراتی اینترنتی صورت می‌گیرد؛ زیرا، همان‌گونه که می‌دانیم این دو، جزئی از VOIP [6] یا

1. Security Certificates

۲. یک وب سایت پرداخت آن‌لاین که کابران با مراجعه به آن می‌توانند از سیستم پرداخت بین‌المللی آن استفاده کنند؛ کاربر باید نام‌کاربری و کلمه‌ی ورود خویش را وارد کند.

3. PIN

4.Termination

5. Origination

6. Voice over Internet Protocol

همان انتقال صدا از طریق پروتکل اینترنتی هستند. البته شایان ذکر است که این شاخه از فن‌آوری ارتباطی شامل شبکه‌ی جهانی اینترنت و سایر شبکه‌های سوئیچ بین بسته‌های داده[1] است و از این رو دربردارنده‌ی تلفن آی پی،[2] تلفن اینترنتی،[3] صدا از ورای پهن باند[4] و تلفن پهن باند[5] می‌شود.

این دو فرایند به دو طریق قابل اعمال است؛ [1] نخست، با استفاده از دستگاه‌های ارسال و دریافت ماهواره‌ای؛ این امر نیازمند استفاده از خطوط تلفنی است تا مشترکان با استفاده از آن خطوط به شبکه‌ی ماهواره‌ای شرکت ارائه‌دهنده‌ی این خدمات متصل شده و سپس از طریق آن به مکالمه‌ی اینترنتی بپردازند؛ [2] شیوه‌ی دوم، عبارت است از استفاده از سیستم‌های اینترنتی پرسرعت که توسط شرکت مخابرات ارائه شده است؛ شرکت‌ها یا افراد می‌توانند بدین طریق و با استفاده از یک خط تلفن به افراد خدمات ارائه نمایند؛ هر دو نوع با استفاده از کارت‌های تلفن اینترنتی صورت می‌گیرد.

تفاوت این دو روش در آن است که در قسم نخست، بدون استفاده از درگاه‌های ارتباطی مخابرات با شبکه‌ی جهانی اینترنت این اقدام صورت می‌گیرد و افراد یا شرکت‌ها از زیرساخت‌های مخابراتی برای اتصال مشترکان خود استفاده می‌کنند؛ در حالی که در روش دوم، از زیرساخت‌های مخابرات برای اتصال به اینترنت و نیز اتصال مشترکان از شبکه‌ی ایجاد شده توسط آن شرکت استفاده می‌شود. روش نخست که با استفاده از سیستم‌های ماهواره‌ای است، در هر دو وجه ترمینیشن و اورجینیشن بدون مجوز و به صورت قاچاق است.

شیوه‌ی دوم، بیشتر مورد استفاده‌ی شرکت‌های ارائه‌کننده‌ی خدمات اینترنتی[6] (ISP) است؛ به نحوی‌که، با بهره‌گیری از ساختارهای مخابراتی شرکت

1. Packet-switches Networks
2. IP Telephony
3. Internet Telephony
4. Voice over Broadband (VOBB)
5. Broadband Telephony
6. Internet Service Provider

زیرســاخت و ارائــه‌ی کارت‌های تلفن اینترنتــی، خدمات مکالمــه‌ی اینترنتی ارائه می‌کنند، این روش از دو منظر قابل بررسی است؛ نخست آن‌که، برای این شرکت‌ها صرفاً امکان اورجینیشــن وجود دارد و مجوزی برای ترمینیشــن به آن‌ها داده نشده اســت؛ لذا، عمل آن‌ها در این قســمت غیرقانونی و به صورت قاچاق اســت؛ ضمن آن‌کــه، این شــرکت‌ها با بازفروشــی[1] امکانی که حق فــروش آن را ندارند، اقدام به کســب درآمد می‌کنند، این مورد نیز خلاف قوانین موجود اســت، به‌گونه‌ای‌که، در حال حاضر عمده‌ی قاچاق مخابرات در ایران به صورت ترمینیشــن و از ســوی ISP ها اســت؛ «تقریباً ۱۲۰ تــا ۱۵۰ میلیون دقیقه مکالمه تلفــن در ماه به این صورت قاچاق می‌شــود.»[2]

این جرم مخابراتی که در حال گســترش اســت، در ماده‌ی ۲۴ قانون جرایم رایانــه‌ای[3] موردتوجه قانون‌گذار قرار گرفته اســت. این ماده بــه طور عام تمامی صُور اســتفاده‌ی بــدون مجوز از پهنــای باند بین‌المللــی را به منظور برقــراری ارتباطات مخابراتی قابل مجازات دانسته است؛ عنصر مادی آن، فعل مادی مثبت در بهره‌برداری بدون مجوز از این پهن‌باندها اســت؛ مرتکب نیز هر شــخص حقیقی یا حقوقی اســت که به این پهن‌باندها دسترســی دارد. به نظر می‌رســد همان‌گونه‌که پیش‌تر نیز اشاره شد، اســتفاده از سیستم‌های ماهواره‌ای به منظور ارائه‌ی خدمات مکالماتی قاچاق، با توجه به صراحت این ماده در اســتفاده از پهنای باند بین‌المللی قابل مجازات نباشد و این خلاء قانونی، که نیازمند بازنگری مقنن است؛ زیرا، در این فرض امکان اتصال به شــرکت‌های ارائه‌کننده‌ی خدمات مخابراتی در سایر کشورها از طریق ماهواره میسر می‌شود و نیازی به استفاده از پهنای باند بین‌المللی نیست.

---

1. Reseller

۲. به نقل از مصاحبه‌ی عضو هیأت‌مدیره‌ی سازمان نظام صنفی رایانه‌ای با سایت اخبار ارتباطات ایران.

۳. «هرکــس بــدون مجوز قانونــی از پهنای باند بین‌المللی بــرای برقراری ارتباطات مخابراتــی مبتنی بر پروتکل اینترنتی از خارج ایران به داخل یا برعکس اســتفاده کند، به حبس از یک تا ســه ســال یا جزای نقدی از یکصد میلیون تا یک میلیارد ریال یا هر دو مجازات محکوم خواهد شد.»

عنصر معنوی این جـرم، علم و عمد مرتکب به غیرقانونی بودن عمل خویش اسـت؛ به‌نحوی‌که شخص باید سوءنیت عام در فعل مجرمانه و نیز سوءنیت خاص در نتیجه‌ی حاصله را دارا باشد.

۳. جرایم مرتبط با سیستم‌های مخابراتی

در این قسـمت از نوشـتار به بررسی جرایم سـنتی موجود که ارتکاب آن‌ها با دسـتگاه‌های مخابراتی - ارتباطی دگرگون شـده، می‌پردازیـم؛ ماهیت این جرایم به‌گونه‌ای اسـت که صرفاً بر سیستم‌های مخابراتی مبتنی نیستند، اما، این سیستم‌ها تحقق آن‌ها را دسـتخوش تغییر نموده و گاه به عنوان ابزاری در ارتکاب این قسـم از جرایم بدل شده و یا خود قربانی این جرایم هستند.

۳-۱. آسیب رساندن به دستگاه‌ها و سیستم‌های مخابراتی

صیانـت از تمامیت فیزیکی سیسـتم‌ها و دسـتگاه‌های مخابراتی عمومی، در قوانین کیفری ایران از پیشـینه‌ی طولانی برخوردار اسـت. در ابتدا در سـال ۱۳۳۳ لایحه‌ی مجازات قطع و تخریب وسایل مخابرات و برق به تصویب رسیدکه به موجب آن هر کس به وسـایل مخابراتی کشـور اعم از تلگراف، تلفن و دستگاه‌های فرستنده و گیرنده خبر دولتی آسـیب رسـاند، مستوجب دو تا پنج سـال حبس مجرد بوده و در صورتی که کسـی طی آن کشته می‌شـد، مرتکب به اعدام محکوم می‌شده است؛ ایـن مجازات‌ها در فرضی بود که هدف مرتکـب اخلال در نظم و آرامش عمومی و یا پیشرفت مقاصد سیاسی باشد.

ایـن لایحه در سـال ۱۳۳۷ جای خـود را به قانون راجع بـه مجازات قطع و تخریب وسایل مخابرات و برق داد که در آن، بار دیگر بر مجازات‌های پیش‌بینی شده در لایحـه‌ی مصـوب ۱۳۳۳ تصریح، اما، تبانی در ارتکاب آن نیز مطرح شـده بود. به موجـب ماده‌ی ۲ ایـن قانون، مجازات مرتکبان از دو تا پنج سـال حبس بود. مطابق

ماده‌ی ۳ نیز در صورتی که مرتکب از کارمندان دولت بود، به حداکثر مجازات محکوم می‌شد. این قانون به موجب لایحه‌ی سال ۱۳۳۳ ملغی شد.

در سال ۱۳۵۱ قانون مجازات اخلال‌کنندگان در تأسیسات آب و برق و گاز و مخابرات کشور جایگزین قانون راجع به مجازات قطع و تخریب وسایل مخابرات و برق ۱۳۳۷ شد؛ در این قانون اخلال در این تأسیسات جرم‌انگاری شد و برخلاف قوانین پیشین، دستگاه‌های مخابراتی و ارتباطات مملکتی از قبیل تلفن، تلگراف، رادیو، تلویزیون، ماکروویو و وسایل مربوط مورد حمایت قرار گرفته با توجه به تمثیلی بودن دستگاه‌های موضوع این قانون، دیگر دستگاه‌ها و سیستم‌های مخابراتی که در ماده‌ی ۱ به صراحت به آن‌ها اشاره نشده است، نیز مشمول این ماده هستند، مشروط بر آن‌که کارکردی مشابه موارد مطروحه در این ماده داشته و جزء وسایلی باشند که به طور عمومی مورد استفاده قرار گیرند. لذا، به وسایل مخابراتی که استفاده‌ی عمومی ندارد، اشاره‌ای نشده و آسیب رساندن به آن‌ها مشمول عنوان کلی تخریب اموال شده است. در این قانون مجازات مرتکبان به سه تا ده سال حبس افزایش یافت و در صورتی که اقدامات مذکور به مرگ شخص یا اشخاصی منتهی شود، برای مرتکب مجازات اعدام پیش‌بینی شده است. طبق ماده‌ی ۲ این قانون رسیدگی به این جرایم در صلاحیت دادگاه نظامی بود.

قانون‌گذار در سال ۱۳۷۵ با تصویب قانون تعزیرات و مجازات‌های بازدارنده، ماده‌ی ۶۸۷ این قانون[۱]، به بیان جرایم علیه تأسیسات آب و... مخابرات پرداخته و

۱. «هر کس در وسایل و تأسیسات مورد استفاده عمومی از قبیل شبکه‌های آب و فاضلاب، برق، نفت، گاز، پست و تلگراف و تلفن و مراکز فرکانس و ماکروویو (مخابرات) و رادیو و تلویزیون و متعلقات مربوط به آن‌ها اعم از سد و کانال و انشعاب لوله‌کشی و نیروگاه‌های برق و خطوط انتقال نیرو و مخابرات (کانال‌های هوایی یا زمینی یا نوری) و دستگاه‌های تولید و توزیع و انتقال آن‌ها ... مرتکب تخریب یا ایجاد حریق یا از کار انداختن یا هر نوع خرابکاری دیگر شود بدون آن‌که منظور او اخلال در نظم و امنیت عمومی باشد، به حبس از سه تا ده سال محکوم خواهد شد.

تبصره ۱: در صورتی‌که اعمال مذکور به منظور اخلال در نظم و امنیت جامعه و مقابله با حکومت اسلامی باشد مجازات محارب را خواهد داشت.

تبصره ۲: مجازات شروع به جرایم فوق یک تا سه سال حبس است.»

مفاهیم مندرج در قانون سال ۱۳۵۱ را لحاظ نموده است با این تفاوت که صلاحیت رسیدگی را از محاکم نظامی سلب نمود و از سوی دیگر به جای مجازات اعدام، مجازات محارب را تعیین و شروع به این جرایم را نیز جرم‌انگاری نمود. از آن‌جا که به موجب ماده‌ی ۷۲۹ این قانون، کلیه‌ی قوانین مغایر این قانون ملغی هستند، به نظر می‌رسد جایگاهی برای اعمال قانون مجازات اخلال‌کنندگان در تأسیسات آب و برق و گاز و مخابرات کشور مصوب ۱۳۵۱ وجود ندارد؛ لذا، باید ماده‌ی ۶۸۷ یاد شده، ملاک عمل قرار گیرد.

البته ماده‌ی اخیر با توجه به سیاق نگارشی آن، تنها در بردارنده‌ی صدمات فیزیکی است و صدمات غیرفیزیکی که در فضاهای غیرمادی ممکن است به این دستگاه ها وارد شود، را شامل نمی‌شود. این موضوعی است که در قانون جرایم رایانه‌ای، مورد توجه قانون‌گذار قرار گرفته است. این ماده از قانون مجازات اسلامی، تنها ابزارهایی را دربرمی‌گیرد که کاربری عمومی دارند، لذا، به نظر می‌رسد تخریب دستگاه‌های مخابراتی شخصی که کاربرد عمومی ندارند، مشمول عمومات تخریب در قانون مجازات اسلامی است.

۲-۳. استفاده‌ی غیرمجاز از خدمات مخابراتی

در قوانین کیفری ایران، استفاده‌ی غیرمجاز از خدمات مخابراتی، به عنوان جرمی مستقل پیش‌بینی نشده است، به‌نحوی‌که، صرفاً موضوع استفاده‌ی غیرمجاز از انشعاب تلفن در ماده‌ی ۶۶۰ قانون مجازات اسلامی[1] مطرح شده است؛ زیرا، شمول خدمات مخابراتی امری گسترده‌تر از یک انشعاب ساده‌ی تلفن است. به این جهت که انشعاب تلفن تنها راه بهره‌مندی از خدمات مخابراتی است، به نظر می‌رسد مقنن

۱. «هرکس بدون پرداخت حق انشعاب آب و فاضلاب و برق و گاز و تلفن مبادرت به استفاده غیرمجاز از آب و برق و تلفن و گاز شبکه فاضلاب نماید علاوه بر جبران خسارت وارده به پرداخت جزای نقدی از یک تا دو برابر خسارت وارده محکوم خواهد شد. چنان‌چه مرتکب از مأمورین شرکت‌های مذکور باشد به حداکثر مجازات محکوم خواهد شد. اصلاحی ۱۳۸۷/۹/۱۳.»

در ماده‌ی اخیر به بیان مجازات اســتفاده‌ی غیرمجاز از انشــعاب تلفن پرداخته است و مجازاتی را برای اســتفاده‌ی غیرمجاز از خدمات مخابراتــی قرار نداده و مرتکب را تنها به جبران خســاراتی‌که از این طریق وارد کرده، محکوم نموده اســت؛ این نیز مجازات محسوب نمی‌شود.

در قانون جرایم رایانه‌ای، به اســتفاده‌ی غیرمجاز از خدمات مخابراتی و حتی سرقت آن‌ها نیز اشاره‌ای نشده و تنها به سرقت داده‌ها بسنده شده است.[1] بحث سرقت خدمات نیز بنابر دکترین غالب در نظام حقوقی ایران پذیرفته نیست؛ زیرا، نویسندگان حقوق خدمات را مال نمی‌دانند.(میرمحمدصادقی، ۱۳۸۶، ص ۲۰۵) همچنین به نظر می‌رسد اصل بزه‌ای که در ماده‌ی ۶۶۰ قانون مجازات اسلامی بدان اشاره شده است، در خصوص تلفن قابل اعمال نیست؛ زیرا، امکان بهره‌مندی از تلفن بدون اخذ انشعاب میسر نیســت، تنها بهره‌برداری غیرمجاز از انشعاب دیگری قابل تحقق است؛ این امر نیز به دولت ارتباطی ندارد؛ هنگامی که مخابرات از کُنتور شــخصی عبور می‌کند، در مایملک او وارد شده و چگونگی استفاده‌ی آن به دولت مربوط نشده و حق شکایت از سوءاستفاده‌کنندگان از آن تنها برای آن شخص محرز می‌شود. (آزمایش، ۷۹-۱۳۷۸، ص ۴۳)

۳-۳. جعل بر روی سیستم‌های مخابراتی

از جمله مصادیق تحقق جعل علیه دســتگاه‌های مخابراتی، هنگامی است که افراد یا شــرکت‌هایی، گوشــی‌های تلفن همراه یا ثابت یا سایر محصولات مخابراتی را مشــابه و هم مارک یک شــرکت معتبر تولید کننــد؛ (Collins, 2000, p.143) در این فرض جرم جعل بر روی دســتگاه‌های مخابراتی تحقق یافته است که با عمومات

۱. ر.ک: ماده‌ی ۱۲ قانون جرایم رایانه‌ای.

قانون مجازات اسلامی و به‌ویژه ماده‌ی ۵۳۰ این قانون[۱] قابل مجازات است. پرسشی که مطرح می‌شود آن است که اگر فرد یا شرکتی گوشی‌ها یا سایر ادوات مخابراتی مشابه تولیدات شرکت معروفی را بدون آرم و علامت آن شرکت تولید کند، برای مثال، گوشی تلفن همراه مشابه یک مدل معروف شرکت «Samsung» را با نام «Samsong» تولید نمایند و خریداران نیز به تصور آن‌که کالای اصلی است، آن را خریداری نمایند، وصف مجرمانه‌ی آن چیست؟ با توجه به آن‌که جعل مارک صورت نگرفته است، به نظر می‌رسد با توجه به قوانین فعلی نمی‌توان این مورد را مشمول عنوان مجرمانه‌ای دانست؛ زیرا، با هیچ‌یک از موارد مصرحه قانونی منطبق نیست.

۴-۳. جرایم علیه تمامیت جسمانی اشخاص

با توجه به ساختار سیستم‌ها و دستگاه‌های مخابراتی، از آن‌ها بیش‌تر در جرایم علیه شخصیت معنوی افراد استفاده می‌شود تا جرایم علیه تمامیت جسمانی اشخاص به نظر می‌رسد استفاده از آن‌ها در صُور خاصی از جرایم علیه تمامیت جسمانی اشخاص نیز متصور باشد.

هرگاه فرد «الف» با آگاهی از بیماری قلبی فرد «ب»، برای وی پیامک ارسال و یا تماس بی‌موقعی با شماره‌ی وی برقرار نماید و این صدای نابه‌هنگام منجر به سکته و فوت شخص «ب» بشود، آیا می‌توان مورد را از مصادیق بند «ج» ماده‌ی ۲۰۶ قانون مجازات اسلامی دانست و آن را قتل عمد فرض نمود؟ آیا با توجه به این‌که ابزارهای مخابراتی در حکم وسیله هستند، امکان قتل به وسیله‌ی آن‌ها متصور است؟ و این‌که آیا میان فعل استفاده‌کننده از آن‌ها و عمل رخ داده، رابطه‌ی سببیت برقرار است؟ این‌ها پرسش‌هایی هستند که با توجه به نوع عمل و اوضاع و احوالی که فعل

---

۱. «هرکس مهر یا تمبر یا علامت ادارات یا شرکت‌ها یا تجارتخانه‌های مذکور در مواد قبل را بدون مجوز به دست آورد و به طریقی که به حقوق و منافع آن‌ها ضرر وارد آورد استعمال کند یا سبب استعمال آن گردد، علاوه بر جبران خسارت وارده به دو ماه تا دو سال حبس محکوم خواهد شد.»

ارتکابی در آن به وقوع پیوسته، قابل بررسی است، از این رو امکان آن‌که چنین اعمالی حتی منجر به قتل عمدی موضوع بند «ج» ماده‌ی ۲۰۶ قانون مذکور شـوند، دور از ذهن نیسـت. افزون بر این، به نظر می‌رسـد فرضی که استفاده از امواج فرستنده‌های موجـود در دسـتگاه‌های موبایل، موجب آسـیب قلب مصنوعی بیماری شـود که در حوزه‌ی تشعشـعات آن قرار دارد، را بتوان موجب انتساب قتل غیرعمد به مرتکب آن دانسـت. همچنین هرگاه اسـتفاده از تلفن‌ها یا دستگاه‌های مخابراتی در هواپیماهای معمولی منجر به ایجاد اختلال و یا احیاناً سـقوط آن‌ها بشـود، به نظر می‌رسد بتوان استفاده‌کننده از این ابزار را به عنوان قتل غیرعمدی مورد تعقیب قرار داد.

۵-۳. ایجاد مزاحمت مخابراتی

در مورد ایجاد مزاحمت به وسـیله‌ی دستگاه‌های مخابراتی از جمله تلفن، در قوانین جزایی پیش از انقلاب اسلامی حکم صریحی وجود نداشت؛ در این‌گونه موارد بـه عمومات مقررات جزایی مراجعه می‌شـد. صرف‌نظر از مـاده‌ی ۳ آیین‌نامه‌ی امور خلافـی مصوب ۲۲ مرداد ۱۳۲۴ که در ادامه‌ی ماده‌ی ۲۷۶ قانون مجازات اسـلامی مصـوب ۱۳۰۴ و مـاده‌ی ۱۱ اصلاحی قانون کیفر عمومی مصـوب مرداد ماه ۱۳۲۲ تصویب شده بود و در آن به مواردی همچون «دست زدن به جعبه تلفن یا سیم‌های تلفن و تلگراف به منظور تخریب یا تولید خطر» اشاره شده بود، در تبصره‌ی ۲ ماده‌ی ۱۴ قانون تأسـیس شـرکت مخابرات ایران مصوب ۱۳۵۰، اعمـال مجرمانه‌ای تحت عناوین «وسـیله مزاحمت دیگری قرار دادن دستگاه مخابراتی در اختیار خود» و نیز «مختل کردن ارتباط دیگری با عمد و سوءنیت» مقرر شده بود که بعداً در سال ۱۳۶۶ تبصره‌ی یاد شده طی ماده واحده‌ای اصلاح گردید. غیر از مصوبات یادشده، در قوانین و مقررات جزایی قبل از انقلاب اسلامی مصوبه‌ی دیگری پیش‌بینی نشده است.

پس از پیروزی انقلاب اسلامی نیز تا سال ۱۳۷۵ در مجموعه‌ی قوانین جزایی، در مـورد مزاحمت تلفنی، مقرره‌ای وجود نداشـت، به نحوی‌که دادگاه‌ها که به کرات

بـا این عمـل ناهنجار اجتماعی مواجه بودنـد، مطابق عمومات قوانیـن جزایی اقدام می‌کردند. همچنان‌که اداره‌ی حقوقی قوه قضاییه در پاسخ به این پرسش که آیا برای مزاحمت تلفنی در قانون تعزیرات مجازاتی تعیین شـده یا خیر؟ آورده است: «غیر از آنچه که در تبصره ۲ ماده‌ی ۱۴ قانون تأسـیس شرکت مخابرات مصوب ۱۳۵۰ آمده است، در قانون تعزیرات کیفر علی‌حده‌ای برای مزاحمت تلفنی تعیین نشده است»[۱].

تبصره‌ی ۲ ماده‌ی ۱۴ قانون مذکور نیز در نهم تیرماه ۱۳۶۶ بدین نحو اصلاح شد که «هرکس وسیله مخابراتی در اختیار خود را وسیله مزاحمت دیگری قرار دهد یا با عمد و سـوءنیت ارتباط دیگری را مختل کند، برای بار اول پس از کشف، ارتباط تلفنـی او به مـدت یک هفته همراه با اخطـار کتبی قطع و تجدید ارتباط مسـتلزم پرداخت هزینه‌های مربوطه خواهد بود. برای بار دوم، پس از کشـف، ارتباط تلفنی او به مدت سه ماه همراه با اخطار کتبی قطع و تجدید ارتباط مستلزم تقاضای مشترک و پرداخت هزینه‌های مربوطه خواهد بود و برای بار سوم، شرکت ارتباط تلفنی وی را به طور دائم قطع و اقدام به جمع‌آوری منصوبات تلفن کرده و ودیعه مربوط به مشـترک را پس از تسویه حساب مسترد خواهد کرد».

در سـال ۱۳۷۵، قانون‌گذار با تصویب کتاب پنجم قانون مجازات اسـلامی با عنـوان تعزیرات و مجازات‌های بازدارنده و به‌موجب مـاده‌ی ۶۴۱، ایجاد مزاحمت از طریق تلفن یا سایر دستگاه‌های مخابراتی را جرم‌انگاری نمود. مطابق این ماده «هرگاه کسـی به وسـیله تلفن یا دستگاه‌های مخابراتی دیگر برای اشـخاص ایجاد مزاحمت نماید، علاوه بر اجرای مقررات خاص شـرکت مخابرات به حبس از یک تا شـش ماه محکوم خواهد شد».

اصطلاح مزاحمت در این ماده معنای روشـنی ندارد؛ این امر موجب می‌شود معنای ایجاد مزاحمت نیز مبهم شـود. به ویژه آن‌که، تلفن معمولاً وسـیله‌ی ارتکاب جرایـم دیگـری نیز قرار می‌گیرد. بـرای مثال به نظر می‌رسـد در مواردی که فردی

۱. نظریه‌ی مشورتی شماره‌ی ۷/۵۹۳۳ مورخ ۱۳۶۸/۱۰/۱۹

به‌وسیله‌ی تلفن به دیگری توهین کند، مقصود از مزاحمت، مجموعه‌ی اعمالی است که به واسطه‌ی یک دستگاه مخابراتی، به اذیت کردن و به زحمت افتادن دیگری منجر شود. به عبارت دیگر، مقصود قانون‌گذار از مزاحمت، حالتی است که عنوان جرم دیگری بر آن صدق نکند؛ مانند این‌که کسی بعد از نیمه شب با دیگری تماس گرفته و او را از خواب بیدار کند یا آسایش او را سلب کند. (جلالی فراهانی، ۱۳۸۷، ص ۶۴)

در مزاحمت تلفنی، عمل مرتکب فقط به صورت یک عمل مثبت خارجی بروز می‌یابد و صرفاً فعل مثبت مطرح است. لذا، ترک فعل نمی‌تواند در رکن مادی این جرم مصداق پیدا کند.

با توجه به قید «کسی» در ماده‌ی مذکور، مرتکب جرم، شخص حقیقی است و اشخاص حقوقی تنها می‌توانند بزه‌دیده این جرایم تلقی شوند. این نوع مزاحمت با ارسال پیامک نیز محقق شده و با حکم این ماده منطبق است؛ حال پرسشی که مطرح می‌شود آن است که آیا ارسال پیامک توسط سیستم‌های هوشمند رایانه‌ای به یک سری شماره را می‌توان از مصادیق این ماده دانست؟ در چنین مواردی، مرتکب بزه مزاحمت، سیستم هوشمندی است که به صورت خودکار اقدام به ارسال پیام می‌کند. در پاسخ باید به دو نکته توجه نمود؛ نخست آن‌که، مزاحمت صرفاً ارتکاب یک عمل غیرمباح نیست و ممکن است ارتکاب عمل جایزی در زمان یا مکان غیرمجاز باشد و دیگر آن‌که، این گونه سیستم‌ها غالباً با یک برنامه‌ی از پیش تعیین شده اقدام به قبول و ارسال پیام می‌کنند و افراد در آن‌ها نقش مستقیم ندارند. بنابراین، به نظر می‌رسد اگر پیام ارسالی، پیامی غیرمجاز نبوده و ارسال آن در زمان غیرمجاز صورت نگرفته باشد و خود سیستم نیز صرفاً با برنامه‌ی قبلی که غیرمجرمانه طرح‌ریزی شده است، اقدام به ارسال پیام کرده باشد، عمل از شمول ماده‌ی ۶۴۱ قانون مجازات اسلامی خارج است.

در خصوص وسیله‌ی ارتکاب جرم نیز با توجه به ماده‌ی اخیر و شیوه‌ی نگارش آن به نظر می‌رسد مقصود از دستگاه‌های مخابراتی دیگر موضوع این ماده،

آن دســتگاه‌هایی اســت که علاوه بر اطلاق عنوان مخابراتی بر آن‌ها در عرف خاص، استفاده از آن‌ها نیازمند اخذ امتیاز و اشتراک از مراجع رسمی و متعاقب آن کنترل و نظارت مراجع مزبور در استفاده از این دستگاه‌ها است. همچنان‌که اطلاق قید «اجرای مقررات خاص شرکت مخابرات» در متن ماده مؤید این مطلب است. (همان، ص۸۱) حــال آن‌که علاوه بر این به نظر می‌رســد برای تحقق بــزه مزاحمت باید خصوصیت دیگری نیز در دستگاه‌های مخابراتی مورد توجه قرار گیرد و آن بلاواسطه بودن است؛ بدین معنا که، ابزارهای مخابراتی مانند تلگراف که با واسطه‌ی شخص دیگری قابلیت استفاده دارند، را نمی‌توان از مصادیق ماده‌ی اخیر دانست. (آقایی‌نیا، ۱۳۸۶، ص۲۴۰)

در مــورد این‌که آیا جرم مزاحمت موضوع ماده‌ی ۶۴۱ قانون مذکور از لحاظ عنصر مادی، از جمله جرایم مقید است یا مطلق، اختلاف نظر بوده و رویه‌ی یکسانی در این زمینه حاکم نیست. عده‌ای با این اعتقاد که در جرم مزاحمت تلفنی احتیاجی بــه حصــول نتیجه‌ی مجرمانه نبوده و همین که شــخص ایجــاد مزاحمت کند، جرم مزاحمت تلفنی تحقق یافته است و نیز به این دلیل که این جرم، مقید به ایجاد وضع خاصی در شــخص مقابل نیســت، آن را از جمله جرایم مطلق می‌دانند. لیکن برخی دیگــر، آن را جــرم مقید می‌دانند، بدین معنی که وقــوع جرم مزبور منوط به حصول نتیجه‌ی مجرمانه ایجاد مزاحمت اســت؛ (همــان، ص۲۴۱) همان‌گونه که قید «ایجاد مزاحمت نماید»، در متن ماده همین معنا را می‌رســاند؛ به نظر می‌رسد دیدگاه اخیر صحیح‌تر باشــد. افزون بر این، این جرم، مستلزم سوءنیت خاص مرتکب، دائر بر عمد در فعل و نتیجه‌ی مجرمانه بوده و در زمره‌ی جرایم عمدی است.(همان‌جا)

بــا توجه به مطالب فــوق در خصوص مزاحمت مخابراتــی چند موضوع دیگر شایان توجه است که بدان‌ها پرداخته می‌شود:

نخســت آن‌که، در رابطه با ارســال پیامــک و با توجه به آنچــه که پیش‌تر در خصوص مزاحمت گفته شد، هرگاه پیامک در زمان نامتعارف نیز ارسال شود، از مصادیق مزاحمت اســت؛ حال آن‌که، در پاره‌ای اوقات زمان ارســال پیامک از سوی فرستنده و

زمان دریافت آن از سوی گیرنده تفاوت بسیار دارد، به‌گونه‌ای‌که امکان رسیدن پیام در زمانی نامناسب وجود دارد؛ این مشکل از خطوط ارتباطی شرکت مخابرات ناشی شده و از مصادیق ماده‌ی ۶۴۱ قانون مجازات اسلامی خارج است.

دیگر آن‌که، با توجه به ویژگی‌های جدید خطوط مخابراتی سیار و نیز خطوط هوشمند ثابت در رابطه با انتقال خطوط بر روی یکدیگر، ایجاد مزاحمت موضوع ماده‌ی فوق نیز با صُور جدیدی مواجه شده است. برای مثال، فرض کنید «الف» از تماس‌ها و پیام‌های شخص «ب» بیزار شده و به این جهت شماره‌ی خویش را بر روی خط شخص دیگری «ج» منتقل می‌کند. این اقدام موجب می‌شود که پیام‌های «الف» به جای «ب» برای «ج» ارسال شود. در این فرض چند پرسش ممکن است مطرح شود: «الف» قصد مزاحمت برای «ج» را نداشته، اما، به‌طور ناخواسته و به واسطه‌ی اقدام «ب» این امر پیش آمده است. آیا اقدام «الف» از سوی «ج»، قابل شکایت است؟ آیا در صورت دادن پاسخ توهین‌آمیز از سوی «ج»، «الف» می‌تواند از وی شکایت کند؟ آیا با توجه به آن‌که «الف» در فعل ارتکابی خویش نسبت به «ب» قصد مجرمانه داشته و نه نسبت به «ج»، در صورت شکایت «ج»، «الف» قابل تعقیب کیفری است؟ آیا در صورت شکایت «الف» از «ج» امکان محکومیت وی وجود دارد؟

به نظر می‌رسد فروضی که در این پرسش‌ها مطرح شد، قابلیت تحقق در فضای واقعی را دارند. در این فروض شخص «الف» دارای سوءنیت نسبت به «ج» بوده و «ب» نیز ممکن است نسبت به «الف» دارای سوءنیت بوده باشد، بدین‌جهت «ب» در برابر «الف» دارای مسؤولیت است و «الف» نیز در برابر «ج» دارای مسؤولیت کیفری است؛ به‌رغم آن‌که مباشرتاً اقدام به مزاحمت برای «ج» نکرده است، مسؤولیت این مورد از مصادیق اقوی بودن سبب از مباشر است.

۶-۳. جرایم علیه عفت و اخلاق

در جرایم علیه عفت و اخلاق عمومی که به شیوه‌های مختلفی متصور است،

ابزارهای مخابراتی نقش وسیله را دارند؛ لذا، به نظر می‌رسد این اعمال در گروه جرایم خاص مخابراتی قرار نمی‌گیرند، هر چند در مواد ۱۴ [۱] و ۱۵ [۲] قانون جرایم رایانه‌ای به آن‌ها اشاره شده است. در واقع ابزارهای مخابراتی و رایانه‌ای تنها در خلق (در نوع انیمیشن)، تهیه و انتشار تصاویر و اصوات جرایم علیه عفت، نقش دارند.

با توجه به ساختارهای ابزارهای مخابراتی که موضوع این نوشتار هستند، عمدتاً فروض تهیه و انتشار با این دستگاه‌ها قابل تحقق است. به نظر می‌رسد تهیه‌ی تصاویر و اصوات این جرایم تنها با گوشی‌های تلفن همراه نسل سوم که به دوربین‌های ثبت تصاویر و سیستم‌های ضبط صدا مجهز هستند، قابل تحقق باشد، البته ساختن فایل‌های متنی مستهجن نیز توسط نرم‌افزارهای قابل اجرا در این گوشی‌ها قابل تحقق است، حال آن‌که این ابزارها مخابراتی بوده و همچنین قابلیت انجام چنین کارهایی را دارند. اما، مورد شایع‌تر در میان دستگاه‌های مخابراتی، توزیع و انتشار

---

۱. «هرکس به وسیله سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده محتویات مستهجن را تولید، ارسال، منتشر، توزیع یا معامله کند یا به قصد ارسال یا انتشار یا تجارت تولید یا ذخیره یا نگهداری کند، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

تبصره ۱: ارتکاب اعمال فوق در خصوص محتویات مبتذل موجب محکومیت به حداقل یکی از مجازات‌های فوق می‌شود. محتویات و آثار مبتذل به آثاری اطلاق می‌گردد که دارای صحنه‌ها و صور قبیحه باشد.

تبصره ۲: هرگاه محتویات مستهجن به کمتر از ده نفر ارسال شود، مرتکب به یک تا پنج میلیون ریال جزای نقدی محکوم خواهد شد.

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

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

۲. «هرکس از طریق سیستم‌های 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 یا ترغیب یا تهدید یا تطمیع کند یا فریب دهد یا شیوه دستیابی به آن‌ها را تسهیل کند یا آموزش دهد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات. ارتکاب این اعمال در خصوص محتویات مبتذل موجب جزای نقدی از دو تا پنج میلیون ریال است.

ب) چنان‌چه افراد را به ارتکاب جرایم منافی عفت یا استعمال مواد مخدر یا روان‌گردان یا خودکشی یا انحرافات جنسی یا اعمال خشونت‌آمیز تحریک یا ترغیب یا تهدید یا دعوت کند 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 تا بیست میلیون ریال یا هر دو مجازات.

تبصره 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 می‌شود.»

داده‌های خلاف عفت و اخلاق اســت، زیرا، این دســتگاه‌ها در انتشار داده‌های خلاف عفت توانایی بالایی دارند.

ارســال فایل‌های متنی خلاف عفــت به دو صورت عمده قابل تحقق اســت: نخست، ارسال داده توسط دستگاه‌های ارسال متن، مانند دورنگار که می‌توان از طریق آن‌ها داده‌های متنی مســتهجن را توزیع کرد و دوم، ارسال داده‌های متنی مستهجن از طریق فن‌آوری پیام‌رســان که در تلفن‌های همراه و تلفن‌های هوشمند ثابت وجود دارد.

افزون بر این، ارســال فایل‌های چندرسانه‌ای خلاف عفت توسط دستگاه‌های مخابراتی به چند طریق قابل تصور است:

الف) ارســال این داده‌ها از طریق سیستم پیام‌رسان چندرسانه‌ای که طی آن مرتکب با استفاده از این امکان، فایل‌های صوتی و تصویری خلاف عفت را به خطوط تلفنی موردنظر خویش ارسال می‌کند.

ب) اســتفاده از سیســتم‌های ارتباطــی مادون قرمز موجود در دســتگاه‌های مخابراتــی (اینفــرارد)[1]، در این روش با گوشــی‌ها و دســتگاه‌های مخابراتی مجهز به این فن‌آوری که بُرد بســیار کوتاهی (بین بیســت تا سی ســانتیمتر) دارد، فایل‌های غیراخلاقی ارسال می‌کنند.

ج) اســتفاده از سیســتم‌های ارتباطی بی‌ســیم با بُرد بیشــتر که از آن‌ها به بلوتوث[2] یاد می‌شــود؛ این فن‌آوری که به سرعت جای خویش را در ارتباطات بی‌سیم

---

1. Infrared

برای اطلاعات بیشتر در خصوص این فن‌آوری به آدرس ذیل مراجعه فرمایید:
http://aftab.ir/articles/computer_internet_infortmation_technology/mobil/c14c1227357037_infrared_p1.php

۲. در ســال ۱۹۹۸ شــرکت اریکســون و چهار شــرکت دیگر (آی بی ام، اینتل، نوکیا و توشیبا) یک گروه تشکیل دادند تا اســتانداردی بی‌ســیم را برای اتصال ابزارهای مخابراتی / رایانه‌ای و ابزارهای جانبی آن‌ها طراحی کنند؛ اســتانداردی که بُرد کوتاه، مصرف انرژی پایین و قیمتی ارزان داشــته باشد. نام این پروژه، بلوتوث انتخاب شد که از نام یک پادشــاه دانمارکی به نام Harald Blaatand گرفته شــده است. کلمه‌ی Blaatand پس از انتقال به زبان انگلیسی به شکل Bluetooth تلفظ شد که به معنی دندان آبی است.

باز کرده اســت، به روشــی برای تبادل اطلاعاتی که بعضاً خلاف عفت هستند، تبدیل شده است. دشواری در شناسایی فرستنده و نیز سهولت ارسال، معضلات اصلی مبارزه با این روش اشاعه‌ی منکر است.

د) ارســال فایل‌های صوتی مســتهجن و خلاف اخلاق از طریق دســتگاه‌های فرســتنده مخابراتی، که بر روی گوشی‌های تلفن همراه جدید نیز مشاهده می‌شود و امکان ارسال اصوات منافی عفت را دارند.

اســتفاده از دستگاه‌های مخابراتی در انتشــار فایل‌های خلاف عفت به شدت رواج یافته و نگرانی‌های بســیاری را موجب شــده اســت؛ در این میان امکان مجازات مرتکبان این اعمال به موضوعی بحث‌برانگیز بدل گشــته اســت. هر چند رکن قانونی نسبتاً جامعی در مواد ۱۴ و ۱۵ قانون جرایم رایانه‌ای که پیش‌تر از آن یاد شد، وجود دارد، اما، قانون دیگری با نام قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیرمجاز می‌نمایند، نیز شایان توجه است.

به نظر می‌رسد قانون اخیر همان‌گونه‌که از نام آن پیدا است، تنها به مجازات فعالان غیرمجاز امور سمعی و بصری می‌پردازد و افرادی را که در غیر این موارد اقدام به توزیع آثار مستهجن می‌کنند، در بر نمی‌گیرد. در این قانون تنها به توزیع «نوارها و لوح‌های فشرده صوتی و تصویری» اشاره شده و به وسایلی که در بالا از آن‌ها یاد شد، تصریحی ندارد؛ این قانون نسب به این موارد نیازمند نص صریح است.

به نظر می‌رســد تنها رکن قانونی موجود در خصوص مجازات انتشاردهندگان تصاویر و اصوات منافی عفت با دستگاه‌های مخابراتی، بند ۳ ماده‌ی ۶۴۰ قانون جرایم رایانه‌ای[1] است، که در آن قید «به نحوی از انحاء» آمده است؛ از این رو به نظر می‌رسد

---

۱. «اشخاص ذیل به حبس از سه ماه تا یک سال و جزای نقدی از یک میلیون و پانصد هزار ریال تا شش میلیون ریال و تا (۷۴) ضربه شلاق یا به یک یا دو مجازات مذکور محکوم خواهند شد:

۱. هرکس نوشته یا طرح، گراور، نقاشی، تصاویر، مطبوعات، اعلانات، علایم، فیلم، نوار سینما و یا به طور کلی هر چیز که عفت و اخلاق عمومی را جریحه‌دار نماید برای تجارت یا توزیع به نمایش و معرض انظار عمومی می‌گذارد یا بسازد یا برای تجارت و توزیع نگاه دارد...

۲. هرکس اشیاء فوق را به نحوی از انحاء منتشر کند یا آن‌ها را به معرض انظار عمومی بگذارد.

ابزارهـای فوق الذکر را نیـز در بر گیرد؛ هرچند نمی‌توان صـرف نگهداری فایل‌های مسـتهجن در دسـتگاه‌های مخابراتی و خصوصاً گوشی‌های تلفن همراه را بدون قصد انتشار، جرم محسوب کرد.

موضـوع دیگر آن‌که، در تبصره‌هـای ماده‌ی ۱۴ قانون جرایـم رایانه‌ای، آثار مبتذل و نیز آثار مسـتهجن تعریف شـده است؛ به موجب تبصره‌ی ۱ این ماده، «آثار مبتـذل به آثاری اطلاق می‌گـردد که دارای صحنه‌ها و صور قبیحه باشـد.»؛ مطابق تبصـره‌ی ۴ این مـاده نیز «محتویات مسـتهجن به تصویر، صوت یـا متن واقعی یا غیرواقعی اطلاق می‌شود که بیانگر برهنگی کامل زن یا مرد یا اندام تناسلی یا آمیزش یا عمل جنسـی انسان است.» لذا، به نظر می‌رسـد قانون‌گذار در این ماده میان آثار مبتذل و مسـتهجن قائل به تفکیک شده اسـت؛ بنابراین، تصاویر آمیزش حیوانات را باید مشـمول عنوان مبتذل دانسـت؛ زیرا، با تعریفی که از اصطلاح مستهجن در این ماده ارائه شده است، مطابقت ندارد.

۷-۳. هتک حیثیت و نشر اکاذیب

عمده جرایم این مبحث، توهین، افتراء قولی، قذف و نشر اکاذیب است که به تفکیک بدان‌ها پرداخته خواهد شد. شایان ذکر است که این اعمال، جرایم علیحده‌ای بوده و ابزارهای مخابراتی تنها نقش وسـیله را در ارتکاب آن‌ها ایفاء می‌کنند. لذا، این قسم از جرایم را در زمره‌ی جرایم خاص مخابراتی ذکر نکردیم.

۱-۷-۳. توهین و قذف

ارتـکاب بـزه توهین به وسـیله‌ی دسـتگاه‌های مخابراتی نیز متصور اسـت؛

---

۳. هرکس برای تشویق به معامله اشیای مذکور در فوق یا ترویج آن اشیاء به نحوی از انحاء اعلان یا فاعل یکی از اعمال ممنوعه فوق یا محل به دست آوردن آن را معرفی نماید...»

به‌نحوی‌که، این دستگاه‌ها به ابزارهایی برای ارتکاب بزه توهین بدل گشته‌اند. در مواد ۱۶[۱]، ۱۷[۲] و ۱۸[۳] قانون جرایم رایانه‌ای به صراحت عناوین مجرمانه‌ای چون توهین ذکر نشده و به طور عام هتک حیثیت افراد به هر نحو مورد اشاره قرار گرفته است. به نظر می‌رسد بزه توهین با عمومات ماده‌ی ۶۰۸ قانون مجازات اسلامی[۴] نیز قابل مجازات باشد. برای مثال، اقداماتی چون توهین از طریق تلفن و یا ارسال نوشته‌ی توهین‌آمیز به‌وسیله‌ی دستگاه دورنگار، ارسال مطالب توهین‌آمیز از طریق پیامک‌های صوتی، تصویری و تلفنی و یا از طریق پست الکترونیکی، می‌تواند مصداق این جرم باشد؛ به‌نحوی‌که، همه‌ی این مصادیق با ماده‌ی اخیر قابل مجازات باشد. قانون استفساریه نسبت به کلمه‌ی اهانت، توهین و یا هتک حرمت... مصوب ۱۳۷۹ نیز استدلال بر شمول این ماده نسبت به مصادیق مذکور را تقویت می‌کند.

در رابطه با ایجاد مزاحمت از طریق پیامک، موضوع شایان توجه آن است که در این موارد اصولاً شخص صاحب خط ارسال‌کننده‌ی پیامک توهین‌آمیز مسؤول است؛ مگر آن‌که، ارتکاب جرم توسط دیگری را اثبات نماید؛ در خصوص پیامک‌های ارسالی از طریق سایت‌های اینترنتی نیز با توجه به این‌که برای ایجاد حساب‌های ارسال پیام، ثبت یک شماره و دریافت کد تأییدیه توسط آن شماره ضروری است،

---

۱. «هرکس به وسیله سیستم‌های 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 منتشرکند، به نحوی که عرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد. تبصره: چنان‌چه تغییر یا تحریف به صورت مستهجن باشد، مرتکب به حداکثر هر دو مجازات مقرر محکوم خواهد شد.»

۲. «هرکس به وسیله سیستم‌های رایانه‌ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او 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 تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.»

۳. «هرکس به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی به وسیله سیستم رایانه یا مخابراتی اکاذیبی را منتشر نماید یا در دسترس دیگران قرار دهد یا با همان مقاصد اعمالی را بر خلاف حقیقت، رأساً یا به عنوان نقل قول، به شخص حقیقی یا حقوقی یا مقام‌های رسمی 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 به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.»

۴. «توهین به افراد از قبیل فحاشی و استعمال الفاظ رکیک چنان‌چه موجب حد قذف نباشد به مجازات شلاق تا (۷۴) ضربه و یا پنجاه هزار تا یک میلیون ریال جزای نقدی خواهد بود.»

باید صاحب آن خط را که حساب به نام وی تأیید شده، مسؤول دانست، مگر آن‌که بتواند سوءاستفاده‌ی دیگری از خط خویش را ثابت نماید.

در رابطه با قذف که به نظر نوع خاصی از توهین است و بنا بر شرایط خاصی، مجازات ویژه‌ای در شرع برای آن پیش‌بینی شده است، نیز می‌توان بر این باور بود که امکان تحقق قذف از طریق دستگاه‌های مخابراتی وجود دارد، هرچند، اثبات آن با توجه به شرایط ویژه‌ای که در شرع برای آن وجود دارد، بسیار دشوار و تا حدودی محال است؛ به‌نحوی‌که، صرفاً در صورتی‌که پیام صوتی به صورت مستقیم و از طریق بلندگو به وسیله چهار مرد عادل شنیده شده باشد، می‌توان قائل به اثبات حد قذف شد.

۳-۷-۳. افترای قولی

بزه افترای قولی در مقابل بزه افترای فعلی قرار دارد؛ همان‌گونه‌که در ماده‌ی ۶۹۷ قانون مجازات اسلامی[۱] بدان تصریح شده است، عنوان قولی، مبین لفظی بودن این بزه نیست؛ بزه افترای قولی با انتساب صریح عملی مجرمانه به دیگری تحقق می‌یابد، با توجه به نص ماده‌ی اخیر و قید «به هر وسیله‌ای» در این ماده، بزه مذکور با هر وسیله‌ای و از جمله دستگاه‌های مخابراتی قابل تحقق است. نکته‌ی قابل توجه آن‌که با بررسی مواد ۱۶، ۱۷ و ۱۸ قانون جرایم رایانه‌ای، نصی حاکی از جرم‌انگاری بزه افترا در آن‌ها یافت نمی‌شود؛ به نظر می‌رسد این عمل تنها با مبانی ماده‌ی ۶۹۷ قانون مجازات اسلامی قابل مجازات است.

عنصر مادی این جرم از طریق ارسال پیام متنی با دستگاه‌های دورنگار و سیستم‌های ارسال پیام و نیز دستگاه‌های مکالمه‌ی صوتی و تصویری قابل تحقق

---

۱. «هرکس به وسیله اوراق چاپی یا خطی یا به وسیله درج در روزنامه و جراید یا نطق در مجامع یا به هر وسیله دیگر به کسی امری را صریحاً نسبت دهد یا آن‌ها را منتشر نماید که مطابق قانون آن امر جرم محسوب می‌شود و نتواند صحت آن اسناد را ثابت نماید جز در مواردی که موجب حد است به یک ماه تا یک سال حبس و تا (هفتاد و چهار) ضربه شلاق یا یکی از آن‌ها حسب مورد محکوم خواهد شد.»

باشد؛ مرتکب آن با توجه به قید «هرکس» تنها می‌تواند شخص حقیقی باشد.

۳-۷-۳. نشر اکاذیب

بزه نشـــر اکاذیب در ماده‌ی ۱۸ قانون جرایم رایانه‌ای مورد اشاره قرار گرفته اســـت؛ با توجه به واژه‌ی «هرکس» که در این ماده به‌کار رفته اســـت، مرتکب این جرم، تنها شـــخص حقیقی اســـت، اما، بزه‌دیده می‌تواند شـــخص حقیقی یا حقوقی باشـــد. همچنین به نظر می‌رســـد این جرم در زمره‌ی جرایم مطلق اســـت و اعم از آن‌کـــه به ایراد ضرر مادی و یا معنوی منجر شـــود و یا چنین نباشـــد، مســـؤولیت مرتکب آن را به همراه خواهد داشت.

بزه نشر اکاذیب در ماده‌ی ۶۹۸ قانون مجازات اسلامی[۱] مورد اشاره قرار گرفته اســـت؛ در این ماده، تنها وســـایل خاصی برای ارتکاب این جرم مطرح شـــده است که همگی در زمره‌ی وسایل چاپی هستند؛ لذا، به نظر می‌رسد در دستگاه‌های مخابراتی تنهـــا دورنـــگار و ایمیل را بتوان با این ماده منطبق دانســـت؛ زیرا، دورنگار، دســـتگاه ارسال فایل‌های متنی و چاپی است و ایمیل یا همان پست الکترونیکی نیز نامه‌نگاری الکترونیکی است؛ با توجه به عبارت «مراسلات»[۲] در این ماده، می‌توان نشر اکاذیب از طریق این ابزار را مشمول حکم این ماده دانست.

۴. برآیند

جرایـــم مخابراتی محـــض و جرایم مرتبط با دســـتگاه‌های مخابراتی موضوعات

---

۱. «هرکس به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی به وسیله نامه یا شکواییه یا مراسلات یا عرایض یا گزارش یا توزیع هرگونه اوراق چاپی یا خطی با امضاء یا بدون امضاء اکاذیبی را اظهار نماید یا با همان مقاصد اعمالی را بر خلاف حقیقت راساً یا به عنوان نقل قول به شخص حقیقی یا حقوقی یا مقامات رسمی تصریحاً یا تلویحاً نسبت دهد اعم از این‌که از طریق مزبور به نحوی از انحاء ضرر مادی یا معنوی به غیر وارد شود یا نه علاوه بر اعاده حیثیت در صورت امکان، باید به حبس از دو ماه تا دو سال و یا شلاق تا (هفتاد و چهار) ضربه محکوم شود.»

۲. در فرهنـــگ دهخدا، «مراســـله» به معنی نامه‌نگاری و مکاتبه‌کردن آمده و به نظر هر نوع نامه‌نگاری را شـــامل می‌شود.

عمده‌ی این نوشـــتار بودند که در دو بخش مســـتقل به آن‌ها پرداخته شد؛ حال آن‌که، مباحث مطرح شده تنها بخشی از جرایم این عرصه را در بر می‌گیرد و موضوعات بسیار دیگری باقی می‌ماند که می‌بایست به تفصیل در نوشتاری دیگر به آن‌ها پرداخته شود.

در حال حاضر، دستگاه‌های مخابراتی در حال گرویدن به دستگاه‌های رایانه‌ای هســـتند؛ شاید در آینده‌ای نزدیک میان این دو، فاصله‌ای نباشد و دستگاه‌هایی با هر دو ویژگی رایانه‌ای و مخابراتی جای دســـتگاه‌های صرفاً مخابراتی امروز را بگیرند، اما، به نظر می‌رسد جایگاه جرایم مخابراتی همواره ثابت باشد.

باید متذکر شد قانون‌گذاری‌های مصداقی و محدود و نیز جرم‌انگاری‌های ناقص در چنین جرایمی با مشـــکل مواجه بوده و به ســـرعت آن‌ها را به قوانین متروک بدل خواهد کرد؛ همان‌گونه‌که، «گرابوســـکی» در این مورد اشاره کرده است: «راه‌حل‌های ظاهری و بدون مطالعه و پشـــتوانه‌ی علمی چون شمشـــیری دو لبه می‌مانند که آثار ســـوء آن‌ها ممکن است بسیار مخرب‌تر از خود مشکل باشد.» (Grabosky, Smith, 1998, pp.347-369)

فهرست منابع

الف) فارسی

۱. آزمایـــش، علی؛ **تقریرات جزای اختصاصی (جرایم علیه اشـــخاص و اموال)**، مقطع کارشناسی ارشد، دانشگاه تهران، ۱۳۷۹-۱۳۷۸.

۲. آقایی‌نیا، حســـین؛ **جرایم علیه اشخاص (شـــخصیت معنوی)**، انتشارات میزان، تهران، ۱۳۸۶.

۳. جلالی فراهانی، امیرحسین؛ **بررسی قوانین و مقررات راجع به مزاحمت علیه امـــوال و اشـــخاص**، مجله‌ی کانون وکلای دادگستری مرکز کرمانشاه، شماره‌ی ۲۱-۲۰، پائیز و زمستان ۱۳۸۷.

۴. میرمحمدصادقی، حســـین؛ **جرایم علیه اشـــخاص**، چاپ اول، نشر میزان، تهران، ۱۳۸۶.

۵. میرمحمدصادقی، حســـین؛ **جرایم علیه اموال و مالکیت: کلاهبرداری، خیانت در امانت، ســـرقت و صدور چک پرداخت نشدنی (مطالعه تطبیقی)**، انتشارات میزان، تهران، ۱۳۸۶.

ب) لاتین

3. Collins, Michael, **Telecommunication crime (3),** Computers & Security Journal, Vol. 19, No. 2, Elsevier Science Ltd, 2000.

4. Cradduck, Lucy; Mccullagh, Adrian, **Identifying the Identity Thief: Is it time for a (smart) Australia Card?**, International Journal of Law and Information Technology, Vol. 16, No. 2, Oxford University Press, 2007.

5. Cross, Michael, **Threat of Cyber Sabotage Increase**, Science Direct, 1999.

6. Cunningham, J. Lawrence, **Cutting Cell Fraud Frequently**, Security Management, 40.

7. Denning, D, **Crime and Crypto on the Information Super-highway**, Journal of Criminal Justice Education, Vol. 6.

8. Grabosky, P.N; Smith, Russell G; Wright, Paul, **Crime and Telecommunication**, Australian Criminology Institute, 1996.

9. Grabosky P.N; Smith, Russel G., **Telecommunications and**

Crime: Regulatory Dilemmas, Law & Policy, VOL. 19, No. 3, July 1997.
10. Grabosky, P.N; Smith, Russell g., **Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities**, Federation Press, Sydney, 1998.
11. International Telecommunication Union (ITU) 2001, '**Telecommunications Indicators,** http://www.itu.int/ti.
12. Karl Seger, David; Von Storch, William, **Computer Crime: A Crime Fighter's Handbook**, Sebastopol, Calif. O'Reilly and Associates.
13. Naylor, R. T. (2000). **Expert Panel on Emerging Crimes**: 4, Research and Statistics Division, Department of Justice: http://www.justice.gc.ca/en/ps/rs/rep/2002/expertpanel.pdf.
14. Royal Canadian Mounted Police (RCMP) 2001, '**What is Computer and Telecommunication Crime?**, http://www.rcmp-grc.gc.ca/html/cpu-cri.html
15. Schiek, Michael, **Combating Fraud in Cable and Telecommunications**, IIC Communications Topics, No. 13, London, International Institute of Communications.
16. Smith, Russell G, **Stealing Telecommunications Services**, Trends and Issues in Crime and Criminal Justice, No. 54, Canbera, Australian Institute of Criminology.
17. Zittrain, J. L. (2006). **The Generative Internet**, Harvard Law Review (119:7) http://www.harvardlawreview.org/issues/119/may06/may06.shtml.