

جرایم مخابراتی

احسان زرخ^۱

چکیده

با رشد فزاینده‌ی تکنولوژی در عصر اخیر، هر روز تغییرات شگرفی در زندگی بشر به وقوع می‌پیوندد که دارای جنبه‌های مثبت و منفی است؛ از جمله مهم‌ترین دستاوردها، پیشرفت‌های مخابراتی و ارتباطی است که طی چند دهه، بشر را از مرحله‌ی تلگرام، تلگراف و تلفن‌های اولیه خارج نموده 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 مخابراتی محض و جرایم مرتبط با مخابرات جای داد؛ هر یک از این‌ها، خود طیف وسیعی از جرایم را در بر می‌گیرد.

جرایم نخست، مشتمل بر جرایم ارتكابی به وسیله‌ی ابزارهای مخابراتی و نیز جرایم علیه سیستم‌های مخابراتی است؛ 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 شمول مصادیق این جرایم، برخی قانون‌گذاری‌های مصدق‌ی و محدود و تعدادی جرم‌انگاری‌های ناقص صورت گرفته است؛ امری که نیازمند تغییر رویه قانون‌گذار و انجام اصلاحات ساختاری در این حوزه است.

واژگان کلیدی

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

۱ کارشناسی ارشد حقوق کیفری و جرم‌شناسی.

۱. درآمد

مبنای زندگی جمعی انسان‌ها بر ارتباطات و تعاملات میان آن‌ها است؛ 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^۱ مخابراتی به شکل‌گیری فضای نوینی منجر شده است که تمامی یافته‌های سنتی در خصوص تعامل و ارتباط میان افراد را دستخوش تغییر کرده است. به راستی دیگر نمی‌توان با تفکرات سنتی و بدون لحاظ جایگاه این فن‌آوری‌ها به بررسی روابط میان افراد و حتی جوامع با یکدیگر پرداخت.

این تحول عظیم با گسترش ابزارهای مخابراتی که همچون تارهای عنکبوت افراد و جوامع را به هم متصل نموده‌اند، ایجاد شده و به مرحله‌ای رسیده است که نمی‌توان نقش این وسایل را انکار کرد؛ خصوصاً از هنگامی که اینترنت پا به عرصه‌ی وجود گذاشته است.^۲ هرچند افرادی چون نایلور^۳ این اظهارنظر را اغراق‌آمیز دانسته و این‌گونه استدلال می‌کنند: «مباحث اغراق‌آمیزی در خصوص نقش فن‌آوری صورت گرفته است، از ابتدا تا اواسط 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 شدن سیستم‌های مخابراتی نیز موجب شده تا به سختی بتوان میان جرایم رایانه‌ای و مخابراتی قائل به تفکیک شد، اما در مجموع باید به کلیت جرایم خارج از فضای واقعی و فیزیکی اذعان کرد. ناتوانی از طبقه‌بندی این دسته از جرایم موجب شده تا اصطلاحات گوناگونی نسبت به جرایم خارج از فضای واقعی به کار گرفته شود، که از جمله آن‌ها می‌توان به این موارد اشاره کرد: جرم سایبر (Cyber Crime)، جرم فن‌آوری بالا (High Tech Crime)، جرم رایانه‌ای (Computer Crime)، جرم فن‌آوری (Technology Crime)، جرم دیجیتال (Digital Crime)، جرم فن‌آوری اطلاعات (IT Crime)، جرم مجازی (Virtual Crime)، جرم شبکه (Net Crime) و جرم مخابراتی (Telecommunication Crime).

3. Naylor

بسیار انقلابی تر و تحول آمیزتر از نقش اینترنت و سفر با هواپیما بوده است. در واقع هر نوع جرمی که توسط ارتباطات الکترونیکی مدین و فن آوری های ارتباطی نوین انجام می شود، مشابه چیزی در عصر تلگراف است، عصری که ... شرکت های تلگراف خودشان را با موارد نقض امنیت به وسیله تهدیدهای هکری مخصوصاً نقل و انتقال پول تلگرافی مواجه می دیدند.^۱

به نظر می رسد باید این اظهار نظر را با دید خاصی تعدیل کرد و آن را مورد بررسی قرار داد؛ چه آن که ایشان تنها به نقش برخی از فن آوری های نوین ارتباطی چون اینترنت متعرض شده اند، نه به کلیت جایگاه فن آوری های ارتباطی - مخابراتی در جوامع؛ ایشان با پذیرش نقش ابزارهایی چون تلگراف که از نخستین ابزارهای مخابراتی غیرمستقیم است، به طور ضمنی به اهمیت جایگاه فن آوری های ارتباطی اذعان نموده اند.

در مقابل این نگرش، عده ای دیگری از حقوق دانان، با توجه به نقش فن آوری (اعم از مخابراتی و غیرمخابراتی) در تحقق جرایم، نظری مخالف داشته و جایگاه مهمی را برای آن در تحقق جرم ترسیم می کنند. در این میان نظرات زیتراین^۲ و گرابوسکی^۳ و اسمیت^۴ معقول تر به نظر می رسد. زیتراین بیان می دارد که: «هرگونه رشد و توسعه فن آوری در درجات مختلف با طیف وسیع منبع باید فرصت مجرمانه ای به شمار آید. اعم از آن که هدف جرم، تسهیل کننده فعالیت های جنایی یا با سوءنیت باشد. به هر حال فرصت های ارتکاب جرم در چهارچوب فن آوری، به طور فزاینده ای افزایش یافته است.» (Schiek)

در این میان گرابوسکی و اسمیت، این گونه استدلال می کنند که: «پیشرفت های فن آوری 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 هستند؛ زیرا، خود فرصت جزایی ارتکاب جرم را به وجود آورده‌اند.»
(Naylor, 2002, p.1)

هدف این نوشتار از مباحث مخابراتی، تنها بررسی فن‌آوری‌های مخابراتی دیجیتال است و به همین منظور از پرداختن به سایر ابزارهای مخابراتی چون پست خودداری می‌شود. البته شایان ذکر است که شیوه‌های پستی دیجیتالی مانند پست الکترونیک^۱ و پیامک^۲ مورد بررسی قرار خواهند گرفت، چه آن‌ها در مقوله‌ی وسایل مخابراتی دیجیتال قرار می‌گیرند.

این نوشتار 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 بررسی می‌شود. سپس جرایم مرتبط با سیستم‌های مخابراتی بررسی می‌شود؛ جرایمی که این سیستم‌ها در تحقق آن‌ها نقش سازه‌ای 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.

کانینگهام در تعریف محیط‌های مخابراتی بیان می‌دارد: «محیط مخابراتی فضایی است که توسعه‌ی فن‌آوری ارتباطی الکترونیکی در اوایل قرن نوزدهم را در بر گرفته، از تلگرام شروع شده و به سیستم‌های بی‌سیم ختم می‌شود.» (Denning, p.42)

این تعریف در بردارنده‌ی ویژگی‌های اصلی فضاهای مخابراتی است، لکن این حدود و ثغور در تعریف محیط‌های مخابراتی، با توجه به از میان رفتن کاربری بسیاری از ابزارهای آن از جمله تگراف و تلگرام، از محدوده‌ی بحث ما خارج می‌شود. 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 شده است؛ در اینجا به دو مورد از آن‌ها اشاره می‌شود که تقریباً سایر تعاریف و دیدگاه‌ها را نیز دربرمی‌گیرند.

نخستین تعریف از سوی «دنینگ» ارائه شده است که بیان می‌دارد: «طیف فعالیت‌های مجرمانه که با نظام‌های مخابراتی یا علیه نظام‌های 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 نیستند، بلکه از نظر میانجی بودن بدیع هستند. در مجموع فعالیت‌های مجرمانه‌ی دیگر، معرف اشکال جدیدی از کارهای نامشروع هستند: اشکال منحصر به فردی چون سرقت خدمات مخابراتی، دسترسی نامشروع و... فعالیت‌های مجرمانه‌ی متضمن نظام‌های مخابراتی به عنوان ابزار یا اهداف این موارد، الزاماً... سیاهه‌ی کاملی را تشکیل نمی‌دهند، برعکس آن‌ها معرف پهنه‌های اولیه‌ی نگرانی‌های سیاست‌گذاران هستند.»^۱

از این تعاریف برمی‌آید که جرایم مخابراتی، شامل جرایم ارتكابی به وسیله‌ی ابزارهای مخابراتی و نیز جرایم ارتكابی علیه سیستم‌های مخابراتی است. از این رو به نظر می‌رسد 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 شد، به بررسی صور خاص جرایم

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

مخابراتی که تنها با سیستم‌های مخابراتی یا علیه آن‌ها محقق می‌شوند، خواهیم پرداخت؛ در این میان به موارد مصرحه در قانون تجارت الکترونیکی و قانون جرایم رایانه‌ای و بررسی قواعد حاکم بر آن‌ها خواهیم پرداخت. لذا، تلاش شده است تا حد امکان دسته‌بندی مطالب این بخش بر مبنای طبقه‌بندی صورت گرفته در قانون جرایم رایانه‌ای باشد.

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

۲-۱-۱. دسترسی غیرمجاز

به نظر می‌رسد این عمل مجرمانه که در ماده‌ی ۱ قانون جرایم رایانه‌ای نیز مورد اشاره قرار گرفته است، در زمره‌ی جرایم خاص مخابراتی باشد. چه آن‌که، دسترسی غیرمجاز به محتویات سیستم‌های مخابراتی - رایانه‌ای تنها از طریق همین سیستم‌ها 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 محقق می‌شود، به این صورت که فرد از طریق سیستم دیگری و با استفاده از شبکه‌های ارتباطی چون اینترنت یا بلوتوث، به آن سیستم 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 اشراق و احاطه‌ی فرد بر داده‌هایی خارج از حیطه‌ی صلاحیت شود؛ این مهم باید به وسیله‌ی ابزارهای مخابراتی - رایانه‌ای و علیه این سیستم‌ها صورت گرفته باشد. به نحوی که، سیستم مورد استفاده، همان سیستم هدف^۱ (سیستم مورد حمله) بوده، که فرد صلاحیت دسترسی به آن را نداشته یا این‌که این صلاحیت از وی سلب شده باشد.

پرسشی که ممکن است مطرح شود، آن است که اگر فرد در ابتدا مجوز

1. Target System

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

پس از طرح این مقدمات، به بررسی ماده‌ی ۱ قانون جرایم رایانه‌ای^۱، می‌پردازیم؛ قید «هرکس» که در این ماده بدان اشاره شده، کلیت دارد و تمامی افراد را شامل می‌شود، اما پرسشی که مطرح می‌شود، آن است که اگر عملیات منجر به دسترسی غیرمجاز توسط چند نفر صورت گرفته باشد، بدین نحو که، هر یک بخشی از عملیات ورود به سیستم را انجام داده، و این افراد زیرمجموعه‌ی یک شخص حقوقی باشند، (فرضاً متخصصان یک شرکت 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 این که باید به مسؤولیت افراد قائل شد؟

با توجه به نحوه‌ی نگارش این ماده و با رعایت شرایط ماده‌ی ۱۹ این قانون^۲، به نظر می‌رسد شخص حقوقی را بتوان مسؤول قلمداد کرد؛ افزون بر آن که، باید مسؤولیت فردی افراد دخیل در فعل مجرمانه دسترسی غیرمجاز را نیز جداگانه لحاظ نمود؛ هر چند قواعد مشارکت 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 است دسترسی 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 است. ضمن آن که، 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^۱ در قانون تجارت الکترونیکی رجوع کرده، سپس تعاریف سیستم‌های رایانه‌ای و مخابراتی و نیز سیستم اطلاعاتی حفاظت شده (مطمئن)^۲ را مورد بررسی قرار داد.

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

در بند «و» ماده‌ی ۲ این قانون سیستم رایانه‌ای^۳ را نیز بدین شکل تعریف کرده است: «هر نوع دستگاه یا مجموعه‌ای از دستگاه‌های متصل سخت‌افزاری- نرم‌افزاری است که از طریق اجرای برنامه‌های پردازش خودکار «داده‌پیام» عمل می‌کند.»

بند «ح» ماده‌ی ۲ این قانون سیستم اطلاعاتی حفاظت شده را بدین شکل تعریف نموده است که «سیستم اطلاعاتی است که: ۱- به نحوی معقول در برابر سوءاستفاده و نفوذ محفوظ باشد. ۲- سطح معقولی از قابلیت دسترسی و تصدی صحیح را دارا باشد. ۳- به نحوی معقول متناسب با اهمیت کاری که انجام می‌دهد پیکربندی و سازماندهی شده باشد. ۴- موافق با رویه ایمن باشد.»

در قانون تجارت الکترونیکی از سیستم مخابراتی، تعریفی ارائه نشده است، با توجه به ماهیت آن قانون، چنین امری منطقی به نظر می‌رسد؛ بهتر آن بود

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

تدوین کنندگان قانون جرایم رایانه‌ای حداقل به ارائه‌ی تعریف سیستم مخابراتی مطابق دیدگاه‌های خود اقدام می‌کردند.

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

این تعریف اولاً، سیستم‌های سنتی غیرالکترونیکی را با قید «الکترونیکی» از شمول خود خارج می‌کند؛ ثانیاً، دستگاه‌های رایانه‌ای را که کارکرد اصلی آن‌ها مخابره‌ی پیام نیست، با قید «کارکرد اصلی مخابره‌ی پیام» از شمول دستگاه‌های مخابراتی خارج می‌کند؛ هر چند در حال حاضر سیستم‌های رایانه‌ای با توجه به امکاناتی که شبکه‌ی جهانی اینترنت بدان‌ها داده است، کارکرد مخابراتی نیز یافته‌اند، این روند به گونه‌ای است که دستگاه‌های مخابراتی در حال کسب ویژگی‌های دستگاه‌های رایانه‌ای هستند.

با این پیش‌زمینه‌ها، پاسخ به پرسش اخیر و سایر سؤالات مرتبط میسر خواهد بود؛ با توجه به تعریف داده‌پیام، پاسخ، مثبت است؛ امکان دسترسی غیرمجاز به داده‌ها بدون نفوذ به سیستم‌های رایانه‌ای - مخابراتی میسر است، زیرا، مطابق تعریف مذکور هر نماد ذخیره شده بر روی دستگاه‌های حامل داده چون کارت‌های حافظه‌ی موبایل‌ها، حامل‌های داده^۱ و...، مشمول عنوان داده‌پیام شده و به استناد ماده‌ی ۱ قانون جرایم رایانه‌ای دسترسی غیرمجاز به این داده‌ها نیز مشمول عنوان جزایی دسترسی غیرمجاز می‌شود.

موضوع دیگری که مطرح می‌شود، آن است که مقصود قانون‌گذار از عبارت «... که به وسیله تدابیر امنیتی حفاظت شده است» چیست؟ آیا همان شاخص‌های سیستم اطلاعاتی حفاظت شده موضوع قانون تجارت الکترونیکی، مدنظر است؟ آیا این حفاظت تنها حفاظت نرم‌افزاری را شامل می‌شود و یا اعم از حفاظت نرم‌افزاری

و سخت‌افزاری است؟

با توجه به نوع نگارش ماده‌ی ۱ قانون جرایم رایانه‌ای به نظر می‌رسد، 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 (سخت‌افزاری و نرم‌افزاری) مورد نظر قانون‌گذاران بوده باشد، زیرا، اصطلاح تدابیر امنیتی عمومیت داشته و هر دو قسم را در برمی‌گیرد.

نکته‌ی دیگر در خصوص دسترسی غیرمجاز، با تلفیق آن با بند «ب» ماده‌ی ۲۵ قانون جرایم رایانه‌ای^۱ به دست می‌آید؛ پرسش این است که آیا قرار دادن گذرواژه یا هر داده‌ای که امکان دسترسی غیرمجاز را فراهم کند، عملی جز معاونت در بزه دسترسی غیرمجاز است؟ پاسخ منفی است. لکن، قانون‌گذار برای مباشرت و معاونت مجازاتی واحد (نود و یک روز تا یک سال حبس و پنج تا بیست میلیون ریال جزای نقدی و یا هر دو مجازات) مقرر نموده است؛ از دید جرم‌شناسی این عمل منطقی به نظر نمی‌رسد و با اصول قانون‌نویسی نیز در تضاد است؛ بهتر آن بود مجازات سنگین‌تری برای مباشر تعیین می‌شد.

آخرین نکته آن‌که، در ساختار موجود و با توجه به ویژگی‌های ساختار مخابراتی کشور و نیز بی‌اطلاعی افراد، تبه‌کاران می‌توانند با در اختیار داشتن 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 است؛ پس از آن کارکرد خط مورد نظر به خط قربانی اضافه می‌شود، به این ترتیب وی باید آن مبلغ را نیز پرداخت کند؛ باتوجه به ویژگی‌های سرقت و کلاهبرداری مخابراتی و سایر جرایم مرتبط که 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 شد: ... ب) فروش یا انتشار 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 نیست؛ به نظر می‌رسد در وضعیت موجود تنها بتوان آن را در زمره‌ی دسترسی غیرمجاز قلمداد کرد، هر چند بهتر بود به جای جرایم خُردی که به طور مجزا به آن‌ها پرداخته شده است، از عناوین مجرمانه‌ای چون سوءاستفاده‌ی مالی از سیستم‌های مخابراتی - ارتباطی استفاده می‌شد.

۲-۱-۲. شنود غیرمجاز سیستم‌های مخابراتی

گسترش دستگاه‌های ارتباطی از قبیل تلفن‌های ثابت 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 شیوه‌ی تجاوز به محرمانگی داده‌ها، به وسیله‌ی سیستم‌های رایانه‌ای و همچنین با سیستم‌های مخابراتی محقق می‌شود. این عنوان مجرمانه در ماده‌ی ۲ قانون جرایم رایانه‌ای^۱ مورد توجه قانون‌گذار قرار گرفته است. به نظر می‌رسد امکان شنود به دو روش باشد: نخست آن‌که، نرم‌افزارهای ضبط مکالمات بر روی دستگاه‌های مخابراتی نصب شده و آن نرم‌افزارها بدون اطلاع فرد اقدام به ضبط تماس‌های وی می‌کنند.^۲ روش دوم شنود مکالمات به وسیله‌ی دستگاه‌هایی مجزا است که با ورود به فرکانس یا خط مورد استفاده‌ی فرد خاص، مکالمات وی را ضبط می‌کنند؛ به نظر می‌رسد هر دو روش را بتوان با این ماده منطبق کرد. در خصوص مکالمات اینترنتی نیز این دو شیوه کاربرد دارند، با این تفاوت که، در روش دوم به جای ورود به فرکانس یا خط مورد استفاده‌ی 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 سیستم‌های 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 بیشتر در خصوص این قسم از نرم‌افزارها و شیوه‌ی عملکرد آن‌ها، به پایگاه الکترونیکی شرکت killer mobile به آدرس www.killermobile.com رجوع کنید.

پرسشی که در این خصوص مطرح می‌شود، آن است که آیا دسترسی به پیام‌های فرد را نیز می‌توان مشمول عنوان جزایی شنود غیرمجاز دانست؟ با توجه به نص این ماده پاسخ منفی خواهد بود؛ دایره‌ی شمول این ماده پیام‌ها را در بر نمی‌گیرد، اما، با توجه به پیشرفت ابزارهای مخابراتی و توانایی ارسال پیام‌های چندرسانه‌ای^۱ به نظر می‌رسد این ماده شنود پیام‌های چندرسانه‌ای را نیز در گرفته و به استناد آن می‌توان این اعمال را جرم‌انگاری کرد؛ افزون بر این، به نظر می‌رسد شنود پیام‌های صوتی در اتاق‌های گفت‌وگو^۲ 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.

نکته‌ی آخر آن‌که، به نظر می‌رسد شنود محتوای ارتباطات از راه دور چندرسانه‌ای که نمونه‌ی بارز آن ویدیو کنفرانس‌ها هستند، را نیز بتوان با حکم ماده‌ی اخیر تطبیق داد؛ زیرا، این سیستم‌های ارتباطی مصداق بارز امواج نوری هستند که در ماده بدان‌ها اشاره شده است. البته پرسش قابل طرح که به جرایم مخابراتی موضوع این نوشتار، ارتباط چندانی ندارد، آن است که سیستم‌های نوری و الکترومغناطیسی، در بردارنده‌ی امواج ماهواره‌ای و شبکه‌های ماکروویو نیز می‌شوند؛ چنین ابزارهایی نیز مشمول حکم این ماده قرار می‌گیرند.

البته شایان ذکر است که در تمامی این فروض، جرایم ارتكابی باید علیه داده‌های غیرعمومی صورت گیرند، چه آن‌که، در غیر این صورت مشمول عنوان جزایی جاسوسی خواهند شد.

۳-۱-۲. جاسوسی مخابراتی

در جاسوسی مخابراتی، افراد با مقاصد غیرشخصی 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 اشکال 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 است که 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 صورتی که 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 مسئول 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 مخبراتی، بدان اشاره خواهد شد.

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

مخبراتی

۱-۲-۲. جعل رایانه‌ای - مخبراتی

عنصر مادی جرم جعل رایانه‌ای و مخبراتی 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، صور 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 مخبراتی 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 مخبراتی 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 مشمول عنوان جعل دانسته است و این در حالی است که داده شامل تمامی فایل‌های متنی، تصویری، صوتی و... می‌شود؛ حال اگر شخصی با استفاده از سیستم‌های 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 هویت»^۱ یاد کرده‌اند. البته این عمل مجرمانه تنها به این روش محقق نمی‌شود؛ 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

نخستین تصویری که پس از شنیدن این واژه به ذهن متبادر می‌شود، از بین بردن و نابودی مادی و فیزیکی اجسام و اشیاء است، 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.

قانون‌گذار در قانون جرایم رایانه‌ای، عناوین 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.

از حکم مطروحه در ماده‌ی ۸^۱ این قانون چنین استنباط می‌شود که حکم این ماده موارد غیر عمدی را در بر نمی‌گیرد. دیگر آن که نحوه‌ی نگارش ماده به گونه‌ای است که داده‌های متعلق به دیگری را هر چند 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 ۲۹ و ۳۰ 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 غیر حرفه‌ای 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 به‌طور 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 به‌طور غیرمجاز با انجام اعمالی از قبیل مخفی کردن 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.»

۲-۳. 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 نرم‌افزار، نام‌های دامنه و... در عصر حاضر و پرداخت مبالغ هنگفتی در ازای آن‌ها، تردیدی نیست که این امور در زمره‌ی اموال هستند. نخستین نکته آن که در قانون جرایم رایانه‌ای از سرقت و کلاهبرداری مرتبط با رایانه یاد شده، اما، تمامی مصادیق مطروحه در آن سرقت و کلاهبرداری رایانه‌ای است.

دومین نکته آن که محروم کردن فرد از مال خویش، یکی از مهم‌ترین سرقت است؛ حال آن که، 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 می‌رسد، صحیح آن است که این عمل مشمول عنوان جزایی دسترسی غیرمجاز به داده‌ها تلقی نشود و نه سرقت، زیرا، در این فرض محرومیت از مال هرچند به طور موقت نیز محقق نشده است.

با توجه به ساختار موجود درخصوص این بزه به نظر می‌رسد عنصر مادی سرقت رایانه‌ای - مخابراتی بدین نحو باشد که فرد خاطی با ورود به داده‌های سیستم قربانی، اطلاعات او را بردارد (به نوعی مقدمه‌ی تحقق جرم سرقت، ورود غیرقانونی است)؛ این عمل به دو صورت محقق می‌شود، نخست آن که، فرد عین داده‌ها را از سیستم قربانی به سیستم خود منتقل کرده و قربانی را از داده‌های موجود بر روی سیستمش محروم کند، دیگر آن که، یک نسخه از داده‌های موجود بر روی سیستم

۱. «هرکس به طور غیرمجاز داده‌های متعلق به دیگری را برآید، 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 متقابلانه، 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^۱ فریب دیگران و یا گمراهی سیستم‌های رایانه‌ای - مخابراتی مورد توجه قرار گرفته است؛ این درحالی است که در ماده‌ی ۱۳ قانون جرایم رایانه‌ای^۲ 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 معایر 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. «هر کس به طور غیرمجاز از سیستم‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن 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 آن که استفاده از سیستم‌های رایانه‌ای - مخابراتی برای کلاهبرداری و بردن مال افراد با روش‌های خاصی متصور است، در مواد اخیر، این روش‌ها لحاظ شده‌اند. این دیدگاه در خصوص نیاز یا عدم نیاز 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 است، نموده و خود را متولی سیستم اعتبارات شبکه معرفی کرده و بیان می‌دارد که وی در قرعه‌کشی شرکت ایرانسسل برنده‌ی کد اعتباری شده 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 دانست؛ ضمن آن که، مطابق عموماً راجع به سرقت نمی‌توان آن را سرقت نامید، زیرا، در تحقق بزه سرقت، بردن مال فرد بدون رضایت وی شرط است، حال آن که در این مثال این‌گونه نیست. به نظر می‌رسد در کلاهبرداری رایانه‌ای - مخابراتی، اعم از آن که بر روی سیستم‌ها 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 شد. جرایمی مشابه مثال فوق را نمی‌توانیم در قالب اصولی که در قانون جرایم رایانه‌ای تبیین کرده‌ایم، قرار دهیم؛ بنابراین، باید آن‌ها را در قالب جرم دیگری به نام فیشینگ^۱ بررسی کنیم.

۵-۲. فیشینگ

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

1. Phishing

نام کاربری، کلمه‌ی عبور و اطلاعات کارت‌های اعتباری، به‌وسیله‌ی معرفی خود به عنوان یک سایت مورد اطمینان، اطلاق می‌شود.^۱

فیشینگ در عمل به صورت کپی دقیق رابط گرافیکی یک وب سایت معتبر مانند بانک‌های آن لاین است که دربردارنده‌ی بانک‌های موجود در شبکه‌ی جهانی اینترنت و شبکه‌های اعتباری موجود در سیستم‌های مخابراتی نیز می‌شود. در فیشینگ آن لاین ابتدا کاربر از طریق ایمیل و یا آگهی‌های تبلیغاتی سایت‌های دیگر به یک صفحه‌ی قلابی راهنمایی می‌شود، سپس از کاربر درخواست می‌شود تا اطلاعاتی را مانند اطلاعات کارت اعتباری که می‌تواند مهم و حساس باشد، وارد کند. در صورت گمراه شدن 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 فیشینگ در جرایم مخابراتی و لزوم آشنایی با عناصر متشکله‌ی آن، در این قسمت به اجزای این جرم و خصوصاً فیشینگ تلفنی پرداخته می‌شود.

الف) دستکاری پیوند: در این تکنیک برای گمراه کردن کاربر از اسامی معتبری در آدرس استفاده می‌شود، مانند استفاده از زیردامنه‌ی آشنای Gmail در www.gmail.phisher.com، که در واقع کاربر را به سایت Phisher هدایت می‌کند.

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

ج) جعل وب سایت: 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^۱؛ 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^۲ استفاده شد.

د) فیشینگ تلفنی: تمام حملات فیشینگ نیازمند وب سایت فلاپی نیست. پیام‌هایی که 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^۳ خود را وارد کند. مثالی که پیش‌تر در خصوص تخلیه‌ی اعتبار خطوط اعتباری آورده شد، نیز از همین نوع است.

۴-۶. ترمینیشن^۴ و اورجینیشن^۵

ترمینیشن به معنای مکالمات از خارج به داخل و اورجینیشن به معنای مکالمات از داخل به خارج است. در این میان جرم مهمی که 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^۶ یا

1. Security Certificates

۲. یک وب سایت پرداخت آن‌لاین که کاربران 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^۱ است و از این رو دربردارنده‌ی تلفن آی پی^۲، تلفن اینترنتی^۳، صدا از ورای پهن باند^۴ و تلفن پهن باند^۵ می‌شود.

این دو فرایند به دو طریق قابل اعمال است؛^۱ 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؛^۲ 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^۶ (ISP) است؛ به نحوی که، 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

زیرساخت و ارائه‌ی کارت‌های تلفن اینترنتی، خدمات مکالمه‌ی اینترنتی ارائه می‌کنند، این روش از دو منظر قابل بررسی است؛ نخست آن‌که، برای این شرکت‌ها صرفاً امکان اورجینیشن وجود دارد و مجوزی برای ترمینیشن به آن‌ها داده نشده است؛ لذا، عمل آن‌ها در این قسمت غیرقانونی و به صورت قاچاق است؛ ضمن آن‌که، این شرکت‌ها با بازروشی^۱ امکانی که حق فروش آن را ندارند، اقدام به کسب درآمد می‌کنند، این مورد نیز خلاف قوانین موجود است، به‌گونه‌ای که، در حال حاضر عمده‌ی قاچاق مخابرات در ایران به صورت ترمینیشن و از سوی ISP ها است؛ «تقریباً ۱۲۰ تا ۱۵۰ میلیون دقیقه مکالمه تلفن در ماه به این صورت قاچاق می‌شود.»^۲

این جرم مخابراتی که در حال گسترش است، در ماده‌ی ۲۴ قانون جرایم رایانه‌ای^۳ مورد توجه قانون‌گذار قرار گرفته است. این ماده به طور عام تمامی صور استفاده‌ی بدون مجوز از پهنای باند بین‌المللی را به منظور برقراری ارتباطات مخابراتی قابل مجازات دانسته است؛ عنصر مادی آن، فعل مادی مثبت در بهره‌برداری بدون مجوز از این پهناندها است؛ مرتکب نیز هر شخص حقیقی یا حقوقی است که به این پهناندها دسترسی دارد. به نظر می‌رسد همان‌گونه که پیش‌تر نیز اشاره شد، استفاده از سیستم‌های ماهواره‌ای به منظور ارائه‌ی خدمات مکالماتی قاچاق، با توجه به صراحت این ماده در استفاده از پهنای باند بین‌المللی قابل مجازات نباشد و این خلاء قانونی، که نیازمند بازنگری مقنن است؛ زیرا، در این فرض امکان اتصال به شرکت‌های 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. «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 تا یک میلیارد ریال یا هر دو مجازات محکوم خواهد شد.»

عنصر معنوی این جرم، علم و عمد مرتکب به غیرقانونی بودن عمل خویش است؛ به نحوی که 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 قسمت از نوشتار به بررسی جرایم سنتی موجود که ارتکاب آن‌ها با دستگاه‌های مخابراتی - ارتباطی دگرگون شده، می‌پردازیم؛ ماهیت این جرایم به گونه‌ای است که صرفاً بر سیستم‌های مخابراتی مبتنی نیستند، اما، این سیستم‌ها تحقق آن‌ها را دستخوش تغییر نموده و گاه به عنوان ابزاری در ارتکاب این قسم از جرایم بدل شده و یا خود قربانی این جرایم هستند.

۳-۱. آسیب رساندن به دستگاه‌ها و سیستم‌های مخابراتی

صیانت از تمامیت فیزیکی سیستم‌ها و دستگاه‌های مخابراتی عمومی، در قوانین کیفری ایران از پیشینه‌ی طولانی برخوردار است. در ابتدا در سال ۱۳۳۳ لایحه‌ی مجازات قطع و تخریب وسایل مخابرات و برق به تصویب رسید که به موجب آن هر کس به وسایل مخابراتی کشور اعم از تلگراف، تلفن و دستگاه‌های فرستنده و گیرنده خبر دولتی آسیب رساند، مستوجب دو تا پنج سال حبس مجرد بوده و در صورتی که کسی طی آن کشته می‌شد، مرتکب به اعدام محکوم می‌شده است؛ این مجازات‌ها در فرضی بود که هدف مرتکب اخلال در نظم و آرامش عمومی و یا پیشرفت مقاصد سیاسی باشد.

این لایحه در سال ۱۳۳۷ جای خود را به قانون راجع به مجازات قطع و تخریب وسایل مخابرات و برق داد که در آن، بار دیگر بر مجازات‌های پیش‌بینی شده در لایحه‌ی مصوب ۱۳۳۳ تصریح، اما، تبانی در ارتکاب آن نیز مطرح شده بود. به موجب ماده‌ی ۲ این قانون، مجازات مرتکبان از دو تا پنج سال حبس بود. مطابق

ماده 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 ماده 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، اشاره‌ی 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 ماده ۲ این قانون رسیدگی به این جرایم در صلاحیت دادگاه نظامی بود.

قانون‌گذار در سال ۱۳۷۵ با تصویب قانون تعزیرات و مجازات‌های بازدارنده،

ماده 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 صورتی که 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 آن جا که به موجب ماده‌ی ۷۲۹ این قانون، کلیه‌ی قوانین مغایر این قانون ملغی هستند، به نظر می‌رسد جایگاهی برای اعمال قانون مجازات اخلاص کنندگان 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 دستگاه‌ها 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 در برمی‌گیرد که کاربری عمومی دارند، لذا، به نظر می‌رسد تخریب دستگاه‌های مخابراتی شخصی که کاربرد عمومی ندارند، مشمول عموماًت 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، به‌نحوی که، صرفاً موضوع استفاده‌ی غیرمجاز از انشعاب تلفن در ماده‌ی ۶۶۰ قانون مجازات اسلامی^۱ 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 استفاده‌ی غیرمجاز از انشعاب تلفن پرداخته است و مجازاتی را برای استفاده‌ی غیرمجاز از خدمات مخابراتی قرار نداده و مرتکب را تنها به جبران خساراتی که از این طریق وارد کرده، محکوم نموده است؛ این نیز مجازات محسوب نمی‌شود.

در قانون جرایم رایانه‌ای، به استفاده‌ی غیرمجاز از خدمات مخابراتی و حتی سرقت آن‌ها نیز اشاره‌ای نشده و تنها به سرقت داده‌ها بسنده شده است.^۱ 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 نیست، تنها بهره‌برداری غیرمجاز از انشعاب دیگری قابل تحقق است؛ این امر نیز به دولت ارتباطی ندارد؛ هنگامی که مخابرات از کُنتور شخصی 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 دستگاه‌های مخابراتی، هنگامی است که افراد یا شرکت‌هایی، گوشی‌های تلفن همراه یا ثابت یا سایر محصولات مخابراتی را مشابه و هم‌مارک یک شرکت معتبر تولید کنند؛ (Collins, 2000, p.143) در این فرض جرم جعل بر روی دستگاه‌های مخابراتی تحقق یافته است که با عموماً

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 «Samsung» تولید نمایند و خریداران نیز به تصور آن که کالای اصلی است، آن را خریداری نمایند، وصف مجرمانه‌ی آن چیست؟ با توجه به آن که 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 صور 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 سکنه 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 این که ابزارهای مخابراتی در حکم وسیله هستند، امکان قتل به وسیله‌ی آن‌ها متصور است؟ و این که 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.»

ارتكابی در آن به وقوع پیوسته، قابل بررسی است، از این رو امکان آن که چنین اعمالی حتی منجر به قتل عمدی موضوع بند «ج» مادهی ۲۰۶ قانون مذکور شوند، دور از ذهن نیست. افزون بر این، به نظر می‌رسد فرضی که استفاده از امواج فرستنده‌های موجود در دستگاه‌های موبایل، موجب آسیب قلب مصنوعی بیماری شود که در حوزه‌ی تشعشعات آن قرار دارد، را بتوان موجب انتساب قتل غیرعمد به مرتکب آن دانست. همچنین هر گاه استفاده از تلفن‌ها یا دستگاه‌های مخابراتی در هواپیماهای معمولی منجر به ایجاد اختلال و یا احیاناً سقوط آن‌ها بشود، 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 وسیله‌ی دستگاه‌های مخابراتی از جمله تلفن، در قوانین جزایی پیش از انقلاب اسلامی حکم صریحی وجود نداشت؛ در این گونه موارد به عموماًت مقررات جزایی مراجعه می‌شد. صرف نظر از ماده‌ی ۳ آیین‌نامه‌ی امور خلافی مصوب ۲۲ مرداد ۱۳۲۴ که در ادامه‌ی ماده‌ی ۲۷۶ قانون مجازات اسلامی مصوب ۱۳۰۴ و ماده‌ی ۱۱ اصلاحی قانون کیفر عمومی مصوب 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 تأسیس شرکت مخابرات ایران مصوب ۱۳۵۰، اعمال مجرمانه‌ای تحت عنوان «وسيله 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 مورد مزاحمت تلفنی، مقرره‌ای وجود نداشت، به نحوی که دادگاه‌ها که به کرات

با این عمل ناهنجار اجتماعی مواجه بودند، مطابق عمومات قوانین جزایی اقدام می‌کردند. همچنان‌که اداره‌ی حقوقی قوه قضاییه در پاسخ به این پرسش که آیا برای مزاحمت تلفنی در قانون تعزیرات مجازاتی تعیین شده یا خیر؟ آورده است: «غیر از آنچه که در تبصره ۲ ماده‌ی ۱۴ قانون تأسیس 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 سوءنیت ارتباط دیگری را مختل کند، برای بار اول پس از کشف، ارتباط تلفنی او به مدت یک هفته همراه با اخطار کتبی قطع و تجدید ارتباط مستلزم پرداخت هزینه‌های مربوطه خواهد بود. برای بار دوم، پس از کشف، 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 مشترک را پس از تسویه حساب مسترد خواهد کرد».

در سال ۱۳۷۵، قانون‌گذار با تصویب کتاب پنجم قانون مجازات اسلامی با عنوان تعزیرات و مجازات‌های بازدارنده و به‌موجب ماده‌ی ۶۴۱، ایجاد مزاحمت از طریق تلفن یا سایر دستگاه‌های مخابراتی را جرم‌انگاری نمود. مطابق این ماده «هرگاه کسی به وسیله تلفن یا دستگاه‌های مخابراتی دیگر برای اشخاص ایجاد مزاحمت نماید، علاوه بر اجرای مقررات خاص شرکت مخابرات به حبس از یک تا شش ماه محکوم خواهد شد».

اصطلاح مزاحمت در این ماده معنای روشنی ندارد؛ این امر موجب می‌شود معنای ایجاد مزاحمت نیز مبهم شود. به ویژه آن‌که، تلفن معمولاً وسیله‌ی ارتکاب جرایم دیگری نیز قرار می‌گیرد. برای مثال به نظر می‌رسد 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 این که 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 آن که، مزاحمت صرفاً ارتکاب یک عمل غیرمباح نیست و ممکن است ارتکاب عمل جایزی در زمان یا مکان غیرمجاز باشد و دیگر آن که، 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 ارسال، 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 دستگاه‌هایی است 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. همچنان که اطلاق قید «اجرای مقررات خاص شرکت مخابرات» در متن ماده مؤید این مطلب است. (همان، ص ۸۱)

حال آن که علاوه بر این به نظر می‌رسد برای تحقق بزه 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، ص ۲۴۰)

در مورد این که 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 به حصول نتیجه‌ی مجرمانه نبوده و همین که شخص ایجاد مزاحمت کند، جرم مزاحمت تلفنی تحقق یافته است و نیز به این دلیل که این جرم، مقید به ایجاد وضع خاصی در شخص مقابل نیست، آن را از جمله جرایم مطلق می‌دانند. لیکن برخی دیگر، آن را جرم مقید می‌دانند، بدین معنی که وقوع جرم مزبور منوط به حصول نتیجه‌ی مجرمانه ایجاد مزاحمت است؛ (همان، ص ۲۴۱) همان‌گونه که قید «ایجاد مزاحمت نماید»، در متن ماده همین معنا را می‌رساند؛ به نظر می‌رسد دیدگاه اخیر صحیح‌تر باشد. 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)

با توجه به مطالب فوق در خصوص مزاحمت مخابراتی چند موضوع دیگر شایان توجه است که بدان‌ها پرداخته می‌شود:

نخست آن که، در رابطه با ارسال پیامک و با توجه به آنچه که پیش‌تر در خصوص مزاحمت گفته شد، هرگاه پیامک در زمان نامتعارف نیز ارسال شود، از مصادیق مزاحمت است؛ حال آن که، در پاره‌ای اوقات زمان ارسال پیامک از سوی فرستنده و

زمان دریافت آن از سوی گیرنده تفاوت بسیار دارد، به گونه‌ای که 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 آن که، 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 صور 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 آن که «الف» در فعل ارتكابی 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، بدین جهت «ب» در برابر «الف» دارای مسؤولیت است و «الف» نیز در برابر «ج» دارای مسؤولیت کیفری است؛ به‌رغم آن که مابشرتاً اقدام به مزاحمت برای «ج» نکرده است، مسؤولیت این مورد از مصادیق اقوی بودن سبب از مباشر است.

۳-۶. 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 تهیه 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 است، زیرا، این دستگاه‌ها در انتشار داده‌های خلاف عفت توانایی بالایی دارند.

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

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

الف) ارسال 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) استفاده از سیستم‌های ارتباطی مادون قرمز موجود در دستگاه‌های مخابراتی (اینفرارد)^۱، در این روش با گوشی‌ها و دستگاه‌های مخابراتی مجهز به این فن‌آوری که بُرد بسیار کوتاهی (بین بیست تا سی سانتیمتر) دارد، فایل‌های غیراخلاقی ارسال می‌کنند.

ج) استفاده از سیستم‌های ارتباطی بی‌سیم با بُرد بیشتر که از آن‌ها به بلوتوث^۲ یاد می‌شود؛ 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 سال ۱۹۹۸ شرکت اریکسون و چهار شرکت دیگر (آی بی ام، اینتل، نوکیا و توشیبا) یک گروه تشکیل دادند تا استاندارد بی‌سیم را برای اتصال ابزارهای مخابراتی / رایانه‌ای و ابزارهای جانبی آن‌ها طراحی کنند؛ استاندارد بی‌سیم که بُرد کوتاه، مصرف انرژی پایین و قیمتی ارزان داشته باشد. نام این پروژه، بلوتوث انتخاب شد که از نام یک پادشاه دانمارکی به نام Harald Blaatand گرفته شده است. کلمه‌ی Blaatand پس از انتقال به زبان انگلیسی به شکل Bluetooth تلفظ شد که به معنی دندان آبی است.

باز کرده است، به روشی 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) ارسال فایل‌های صوتی مستهجن و خلاف اخلاق از طریق دستگاه‌های فرستنده مخابراتی، که بر روی گوشی‌های تلفن همراه جدید نیز مشاهده می‌شود و امکان ارسال اصوات منافی عفت را دارند.

استفاده از دستگاه‌های مخابراتی در انتشار فایل‌های خلاف عفت به شدت رواج یافته و نگرانی‌های بسیاری را موجب شده است؛ در این میان امکان مجازات مرتکبان این اعمال به موضوعی بحث‌برانگیز بدل گشته است. 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 همان‌گونه که 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 می‌رسد تنها رکن قانونی موجود در خصوص مجازات انتشاردهندگان تصاویر و اصوات منافی عفت با دستگاه‌های مخابراتی، بند ۳ ماده‌ی ۶۴۰ قانون جرایم رایانه‌ای^۱ 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.

ابزارهای فوق الذکر را نیز در بر گیرد؛ هرچند نمی‌توان صرف نگهداری فایل‌های مستهجن در دستگاه‌های مخابراتی و خصوصاً گوشی‌های تلفن همراه را بدون قصد انتشار، جرم محسوب کرد.

موضوع دیگر آن‌که، در تبصره‌های ماده‌ی ۱۴ قانون جرایم رایانه‌ای، آثار مبتذل و نیز آثار مستهجن تعریف شده است؛ به موجب تبصره‌ی ۱ این ماده، «آثار مبتذل به آثاری اطلاق می‌گردد که دارای صحنه‌ها و صور قبیحه باشد.» مطابق تبصره‌ی ۴ این ماده نیز «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.» لذا، به نظر می‌رسد قانون‌گذار در این ماده میان آثار مبتذل و مستهجن قائل به تفکیک شده است؛ بنابراین، تصاویر آمیزش حیوانات را باید مشمول عنوان مبتذل دانست؛ زیرا، با تعریفی که از اصطلاح مستهجن در این ماده ارائه شده است، مطابقت ندارد.

۳-۷. 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 وسیله را در ارتکاب آن‌ها ایفاء می‌کنند. لذا، این قسم از جرایم را در زمره‌ی جرایم خاص مخابراتی ذکر نکردیم.

۳-۷-۱. توهین و قذف

ارتکاب بزه توهین به وسیله‌ی دستگاه‌های مخابراتی نیز متصور است؛

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

به‌نحوی که، این دستگاه‌ها به ابزارهایی برای ارتکاب بزه توهین بدل گشته‌اند. در مواد ۱۶، 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 به وسیله‌ی دستگاه دورنگار، ارسال مطالب توهین‌آمیز از طریق پیامک‌های صوتی، تصویری و تلفنی و یا از طریق پست الکترونیکی، می‌تواند مصداق این جرم باشد؛ به‌نحوی که، 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 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 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 آن که 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؛ به‌نحوی که، صرفاً در صورتی که 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؛ همان‌گونه که 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 آن که 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 نشر اکاذیب در ماده‌ی ۱۸ قانون جرایم رایانه‌ای مورد اشاره قرار گرفته است؛ با توجه به واژه‌ی «هرکس» که در این ماده به کار رفته است، مرتکب این جرم، تنها شخص حقیقی است، اما، بزه‌دیده می‌تواند شخص حقیقی یا حقوقی باشد. همچنین به نظر می‌رسد این جرم در زمره‌ی جرایم مطلق است و اعم از آن که به ایراد ضرر مادی و یا معنوی منجر شود و یا چنین نباشد، مسؤولیت مرتکب آن را به همراه خواهد داشت.

بزه نشر اکاذیب در ماده‌ی ۶۹۸ قانون مجازات اسلامی^۱ مورد اشاره قرار گرفته است؛ در این ماده، تنها وسایل خاصی برای ارتکاب این جرم مطرح شده است که همگی در زمره‌ی وسایل چاپی هستند؛ لذا، به نظر می‌رسد در دستگاه‌های مخابراتی تنها دورنگار و ایمیل را بتوان با این ماده منطبق دانست؛ زیرا، دورنگار، دستگاه 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

جرایم مخابراتی محض و جرایم مرتبط با دستگاه‌های مخابراتی موضوعات

۱. «هرکس به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی به وسیله نامه یا شکوایه یا مراسلات یا عرایض یا گزارش یا توزیع هرگونه اوراق چاپی یا خطی یا 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 این که از طریق مزبور به نخوی 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 فرهنگ دهخدا، «مراسله» به معنی نامه‌نگاری و مکاتبه کردن آمده و به نظر هر نوع نامه‌نگاری را شامل می‌شود.

عمده‌ی این نوشتار بودند که در دو بخش مستقل 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 هستند؛ شاید در آینده‌ای نزدیک میان این دو، فاصله‌ای نباشد و دستگاه‌هایی با هر دو ویژگی رایانه‌ای و مخابراتی جای دستگاه‌های صرفاً مخابراتی امروز را بگیرند، اما، به نظر می‌رسد جایگاه جرایم مخابراتی همواره ثابت باشد.

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

فهرست منابع

الف) فارسی

۱. آزمایش، علی؛ تقریرات جزای اختصاصی (جرایم علیه اشخاص و اموال)، مقطع کارشناسی ارشد، دانشگاه تهران، ۱۳۷۹-۱۳۷۸.
۲. آقایانی، حسین؛ جرایم علیه اشخاص (شخصیت معنوی)، انتشارات میزان، تهران، ۱۳۸۶.
۳. جلالی فراهانی، امیرحسین؛ بررسی قوانین و مقررات راجع به مزاحمت علیه اموال و اشخاص، مجله‌ی کانون وکلای دادگستری مرکز کرمانشاه، شماره‌ی ۲۱-۲۰، پائیز و زمستان ۱۳۸۷.
۴. میرمحمدصادقی، حسین؛ جرایم علیه اشخاص، چاپ اول، نشر میزان، تهران، ۱۳۸۶.
۵. میرمحمدصادقی، حسین؛ جرایم علیه اموال و مالکیت: کلاهبرداری، خیانت در امانت، سرقت 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. Craddock, 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 Illegality**, 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, Canberra, 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>.