ISSN: 2538-3787
http://www.Joce.ir

مجله علمی فقه، حقوق و علوم جزا (سال ششم)
شماره ۱۹ / بهار ۱۴۰۰ / ص ۱۰۹– ۹۷

بررسی جرم شنود غیرمجاز در حقوق کیفری ایران

نفیسه نجفی[۱]، ابوالفتح خالقی[۲]

[۱] دانشجوی کارشناسی ارشد حقوق جزا و جرم شناسی.

[۲] دانشیار دانشکده حقوق دانشگاه قم

نام نویسنده مسئول:
نفیسه نجفی

تاریخ دریافت: ۱۴۰۰/۰۱/۲۰
تاریخ پذیرش: ۱۴۰۰/۰۳/۱۳

چکیده

رفتار جنسی دو زن با هم از جمله مصادیق انحراف جنسی است که از آن به مساحقه تعبیر می‌شود. در دیدگاه اسلام، مساحقه در شمار جرم هایی است که برایش مجازات حدی تعیین شده است. قانون‌گذار در ماده ۲۳۹ قانون مجازات اسلامی، حد سحق زن محصنه را صد تازیانه، قرار داده است. در نظر برخی از قدماء نیز همچون شیخ مفید، ابن ادریس و علامه حلی، زن محصنه مساحق، محکوم به صد تازیانه است. عمده مستند قائلین این نظریه، روایت زراره است که در آن تعبیر "السحاقه تجلد" به کار رفته است. در مقابل، برخی دیگر همچون شیخ طوسی در نهایه، ابن براج و ابن حمزه، مجازات سحق محصنه را رجم می دانند. مهمترین دلیل این عده، روایتی است که طبق مضمون آن، حد سحق، معادل حد زنا دانسته شده است. از آنجا که به نظر می‌رسد حیثیاتی در ادله هر دو نظریه، مغفول مانده است و نیز اهمال در این مورد، به انحراف در عرصه‌ی تقنین منجر می‌گردد، واکاوی ادله طرفین، به منظور دستیابی به قول صواب، ضرورت می یابد.

واژگان کلیدی: ماده۲۳۹ قانون مجازات اسلامی، حد، مساحقه، احصان، رجم، جلد.

ISSN: 2538-3787
http://www.Joce.ir

مقدمه

جامعه بشری در مسیر تکامل خود شاهد تحولات و دگرگونی‌های زیادی بوده که عوامل مختلفی در بوجود آمدن انها نقش داشته‌اند. دانش حقوق هم متناسب با پیشرفت جوامع از ساده‌ترین تا پیچیده‌ترین آنها مسیری انتخاب نموده تا در اشکال متفاوت از جمله سیاست کیفری، تعیین اعمال مجرمانه و اجرای مجازات‌ها به نیازهای هر زمان پاسخ دهد. از جمله اعمالی که مورد مذمت ادیان الهی و اخلاق عمومی جوامع بوده ورود به حریم خصوصی شهروندان و نقض امور محرمانه آنهاست که با گسترش عرصه فن‌آوری ارتباطات توسعه یافته و آفت‌های این پدیده شگرف نیز علیرغم پیچیدگی زیادی که دارد؛ آشکار شده است. هر چند تمامی جرائم، امنیت و آسایش عمومی را خدشه‌دار می‌کنند لیکن این اوصاف در برخی از آنها روشن‌تر و ملموس‌تر است. از همین روست که طبق اصل ۲۵ قانون اساسی جمهوری اسلامی ایران، بازرسی نامه‌ها و محصولات ارسال‌شده، ضبط و افشای مکالمات تلفنی اشخاص، مخفیانه گوش کردن به صحبت‌های دیگران و هرگونه تجسس در مکالمات، جز به حکم قانون، جرم اعلام شده است.

در دهه‌های اخیر استفاده از فضای تبادل اطلاعات مجازی به سرعت درحال افزایش است، در چنین شرایطی حفظ حریم خصوصی و محرمانگی داده‌ها و سامانه‌های رایانه‌ای، قانون‌گذار را ناچار به جرم‌انگاری اعمال ناقض آنها کرده است. از جمله این جرایم، جرم شنود غیر مجاز محتوای درحال انتقال است. تعریف، تشریح و تبیین ارکان تشکیل دهنده این جرم، هدف اساسی این پژوهش بوده که موجب شده تا تحقیق حاضر یک تحقیق کیفی با رویکرد توصیفی باشد. پژوهش حاضر از نظر اهداف، کاربردی و از حیث ابزار تحقیق اسنادی و کتابخانه‌ای است. اطلاعات گرداوری شده شامل تعریف عناصر، اجزا، ارکان و شرایط جرم شنود غیر مجاز (ماده ۲ق.ج.ر)[۱] بوده که به روش توصیفی و تحلیلی مورد تجزیه و تحلیل قرار گرفته است.

بسیاری از اعمال مجرمانه که در فضای فیزیکی قابل تحقق است، در فضای مجازی هم امکان فعلیت دارد. چه بسا ارتکاب جرایم در این فضا از برخی جهات آسان‌تر و فراتر از تبعات قضایی آن به مراتب امکان پذیرتر باشد، جرایم علیه محرمانگی داده‌ها از طریق سامانه‌های رایانه‌ای و مخابراتی نیز از این امر مستثنی نمی باشد. قانون جرایم رایانه‌ای مصوب ۱۳۸۸ با پذیرش این مهم مقررات نسبتاً جامعی را برای مقابله با جرایم رایانه‌ای من جمله جرایم علیه محرمانگی داده‌ها پیش بینی کرده و در صدد پیشگیری از رخداد جرم جدید و بزهکاران جدید است. تولید و تبادل سریع اطلاعات توسط فن‌آوری‌های نوین ارتباطی، ضمن افزایش سرعت تحولات اجتماعی- اقتصادی و پیشرفت‌های خارق العاده، حاوی جنبه‌های خطرناک پیش بینی نشده؛ نیز می‌باشند که پیدایش طیف وسیعی از جرایم نوین و همچنین بهره‌برداری از فن‌آوری جدید در ارتکاب جرایم سنتی، بخشی از انها به شمار می‌روند. پیشرفت‌های مذکور با ظهور شبکه‌ها و ابر شاهراهای ارتباطی از جمله اینترنت گسترش پیدا کرده و از طریق انها هر فرد قادر خواهد بود تا به تمامی خدمات اطلاعات الکترونیک، دسترسی داشته باشد صرف نظر از این که موقعیت مکانی وی در کجای عالم قرار دارد. فضای بوجود آمده که محیط به سایبر شهرت دارد مورد سو استفاده مجرمان و برخی کاربران قرار گرفته است.

جرایم مربوط به مبادله اطلاعات در فضای مجازی از منظر فلسفه قانونگذاری و قوانین حاکم بر ان‌ها به دو گروه تقسیم می‌شوند. گروه اول شامل طیفی از جرایم رایانه‌ای است که با قوانین مربوط به جرایم کلاسیک قابل تعقیب و مجازات هستند و نیاز به قانونگذاری جدید ندارند و می‌توان آنها را به جرایم علیه اشخاص، اموال، امنیت و اسایش عمومی، اخلاق و عفت عمومی و خانواده دسته بندی نمود. گروه دوم شامل جرایم جدیدی هستند که ارتکاب آنها قبل از پیدایش فن‌آوری اطلاعات به هیچ وجه امکان پذیر نبوده است، نظیر: دستیابی غیر مجاز، اخلال در داده، شنود غیر مجاز و اخلال در سیستم. [۱۹] بنابراین حقوق جزا می‌بایست با ایجاد و تاسیس مفاهیم و نهادهای نوین، تدابیر لازمی، متناسب با این فن‌آوری پیش بینی کند و همچنین سلب فرصت‌های پیش امده جهت سوء استفاده از فضای سایبر را در نظر داشته باشد. سال ۱۳۸۸ قانون جرایم رایانه‌ای در ایران تصویب که مقررات نسبتاً جامعی را برای مقابله با پدیده‌های مجرمانه رایانه‌ای پیش بینی و در صدد جلوگیری از پیدایش

---

[۱] - بر اساس شماره مسلسل بخش تعزیرات قانون مجازات اسلامی ماده ۷۳۰ و مطابق شماره مواد کامل قانون مجازات اسلامی شماره ۹۵۱ خواهد بود. برای اجتناب از سرگردانی در این مقاله شماره مواد مورد بررسی بر اساس مقررات مستقل از قانون مجازات درج می‌شوند.

ISSN: 2538-3787
http://www.Joce.ir

مجرمان نوپدید برآمد. این قانون با الهام از کنوانسیون بوداپست، به طور روشن به بزه‌های ضد محرمانگی در اشکال سه گانه؛ دسترسی غیر مجاز، شنود غیر مجاز و جاسوسی رایانه‌ای پرداخته است.

ما در نوشتار پیش رو به تحلیل و بررسی جرم شنود رایانه‌ای (ماده ۲ق.ج.ر و ماده ۷۳۰ ق.م.ا) می‌پردازیم. به همین منظور نخست به مفاهیم و تبیین واژگان پرداخته و ضمن ملاحظه مقررات این جرم در ادبیات تقنینی کشورمان با بیان عناصر تشکیل دهنده و شرایط ان دامنه شمول این جرم را مشخص می‌کنیم. در انتها به بررسی مجازات این جرم در حالات مختلف پرداخته و بعد از جمع بندی مطالب پیشنهاداتی در زمینه مجازات این جرم و نقد وارده به این مقررات بیان می‌گردند.

مفهوم شناسی

شنود

شنود یکی از جرایم عمده در محیط سایبر است ودر صورتی که بدون مجوز باشد به ان غیر مجاز اطلاق می‌شود. از نظر فنی شنود معادل ترجمه ***sniffing)*** استشمام کردن است ***[۱۰]*** در فرهنگ دهخدا شنود, مصدر مرخم شنودن، استماع بیان شده است ***[۷]*** همچنین این واژه در فرهنگ معین اینگونه معنی شده است؛ ۱-عمل شنیدن،۲-دستگاه رسانه‌ای مخفی برای جاسوسی و کنترل مخالفان ***[۲۴]*** با این حال در کنوانسیون جرایم سایبر[۲] معروف به «کنوانسیون جرایم سایبری بوداپست» یا به اختصار «کنوانسیون بوداپست» از عبارت *(Ilegal interceeption)* استفاده شده است که این عبارت نیز با اندکی مسامحه قابل انطباق با عبارت شنود غیر مجاز می‌باشد زیرا در متن ماده آنچه بیان شده همان شنود غیرمجاز در معنی فنی است[۳]. به موجب ماده ۳ هر یک از اعضای کنوانسیون باید به گونه‌ای به وضع قوانین و دیگر تدابیر اقدام کنند که در صورت لزوم بر اساس حقوق داخلی خود، شنود عمدی و بدون حق داده‌های رایانه‌ای در حال انتقال غیرعمومی را که از طریق ابزارهای فنی به سیستم‌های رایانه‌ای یا از طریق آن ارسال شده یا در آن جریان دارد را جرم انگاری کنند. همچنین ارسال امواج الکترومغناطیسی از یک سیستم رایانه‌ای که اینگونه داده‌های رایانه‌ای را انتقال می‌دهند نیز تحت شمول این ماده قرار گیرد. اعضا می‌توانند مقرر دارند این جرم در صورتی انجام می‌شود که قصد سوئی وجود داشته یـا سیستم رایانه‌ای بـه سیستم رایانه‌ای دیگری متصل بوده است. با الهام از ضوابط مندرج در کنوانسیون بوداپست طیف وسیعی از جرایم رایانه‌ای از جمله شنود غیر مجاز در مقررات کیفری ایران (قانون جرایم رایانه‌ای مصوب سال ۱۳۸۸) جرم‌انگاری شده است. ***[۹]***

شنود غیر مجاز با شنود تفاوت دارد؛ شنود یا استراق سمع ویژه جرایم مخابراتی سنتی است در حالی که شنود غیر مجاز به جرایم در محیط سایبر اطلاق می‌شود. شنود راجع به گوش کردن یا استماع غیر مجاز در حین مکالمات شنیداری و احیاناً ضبط ان است در حالی که شنود غیر مجاز مطابق قانون جرایم رایانه‌ای به کنترل، نظارت، مراقبت و یا هر نوع رهگیری، مسیر یا به بررسی، تجزیه و تحلیل داده و یا امواج الکترومغناطیسی در حال انتقال برای اطلاع از محتوای آن و اقدامات مشابه اطلاق می‌گردد.

شنود مختص اصوات و امواج شنیداری می‌باشد در حالی که شنود غیر مجاز اختصاص به داده‌ها و امواج حامل داده دارد. ***[۹]*** شنود مجاز، شنودی است که براساس مقررات، شنود مکالمات تلفنی صورت گیرد و گرنه جرم محسوب می‌شود. ***[۸]*** ولی شنود غیرمجاز را می‌توان "هر گونه دریافت غیر قانونی محتوای در حال انتقال ارتباطات غیر عمومی در بستر فضای تولید و تبادل اطلاعات به طور پنهانی "تعریف نمود. ***[۱]***

---

[2]- Convention on Cybercrime

[3]- Article 3 – Illegal interception: Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

ISSN: 2538-3787
http://www.Joce.ir

سیستم رایانه‌ای

کارشناسان فنی علوم رایانه، سامانه رایانه‌ای را نوعی سیستم تعریف کرده‌اند که در آن، داده‌ها از طریق ورودی به سیستم وارد می‌گردد و پس از پردازش داده‌ها (اطلاعات) از طریق خروجی ارائه خواهد شد. تعریف کنوانسیون جرایم سایبری (بوداپست) از سیستم رایانه‌ای[۴] بدین شرح است: منظور از «سیستم رایانه‌ای» هر دستگاه یا مجموعه‌ای از دستگاه‌های مرتبط یا متصل به هم است که طبق برنامه، یک یا چند دستگاه، پردازش خودکار داده‌ها را انجام می‌دهد. و منظور از «داده رایانه‌ای» هرگونه نماد حقایق، اطلاعات یا مفاهیم به شکلی مناسب برای پردازش در یک سیستم رایانه‌ای است، مانند برنامه‌ای که باعث اجرای یک سیستم رایانـه‌ای می‌شود؛

بنابر این سیستم رایانه‌ای، هرگونه ابزاریا مجموعه‌ای از ابزارهای مرتبط یا متصل به هم است که مطابق با یک برنامه، پردازش خودکار داده‌ها را انجام می‌دهد. در قانون تجارت الکترونیکی سامانه رایانه‌ای چنین تعریف شده است: "هر نوع دستگاه یا مجموعه‌ای از دستگاه‌های متصل سخت افزاری -نرم افزاری است که از طریق اجرای برنامه‌های پردازش خودکار (داده پیام) عمل می‌کند.

اما جدیدترین تعریف ارائه شده از سیستم یا سامانه مزبور در بند «و» ماده دو ایین نامه نحوه استفاده از سامانه‌های رایانه‌ای مخابراتی بدین شرح است: هر نوع دستگاه یا مجموعه‌ای از دستگاه‌های متصل سخت‌افزاری- نرم‌افزاری است که از طریق اجرای برنامه‌های پردازش خودکار «داده پیام» عمل می‌کند. مطابق این تعریف گوشی‌های هوشمند تلفن همراه و دستگاه‌های خودپرداز نیز مصادیقی از سامانه رایانه‌ای محسوب می‌شوند.

داده پیام، محتوا و ترافیک

مطابق تعریف مندرج در بند الف ماده ۲ قانون تجارت الکترونیکی، داده پیام عبارتند از"هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری و یا فناوری‌های جدید اطلاعات، تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود" تفاوت داده رایانه‌ای با داده پیام در این است که داده رایانه‌ای لزوماً قابلیت پردازش دارد، در حالی که در داده پیام ضرورتاً این قابلیت وجود ندارد. در واقع می‌توان گفت رابطه داده و داده پیام عموم و خصوص من وجه است. به طور مثال اطلاعات تولید شده یک دستگاه تلگراف که از طریق خطوط مخابراتی غیر دیجیتالی ارسال و دریافت می‌گردد، داده پیام بشمار می‌آید در حالی که نمی توان به آن داده رایانه‌ای اطلاق کرد. در مقابل داده‌هایی رایانه‌ای وجود دارند که حاوی یکسری اطلاعات غیر قابل فهم برای انسان هستند که آنها داده پیام اطلاق نمی‌شوند مثل داده‌هایی که هنگام راه اندازی یک سیستم رایانه‌ای به اجزای مختلف دستور می‌دهد.

عنوان داده محتوا، برای نخستین بار در لایحه اولیه جرایم رایانه‌ای مطرح شده بود. در واقع به داده‌هایی که حاوی مفاهیم قابل درک برای انسان باشد، داده محتوا گفته می‌شود و می‌توان تعبیر اطلاعات را در مورد این داده‌ها را بکار برد[۲] این نوع داده، همان داده حاصل از مبادله داده محتواست که با هر دو تعبیر و با تعریفی تقریباً مشابه در بند (ج) ماده یک پیش نویس اولیه لایحه جرایم رایانه‌ای قید شده بود. تبصره یک ماده ۳۲ ق.ج.ر، همچنین تبصره یک ماده ۶۶۷ قانون ایین دادرسی کیفری به شرح زیر در معرفی مفهوم داده ترافیک بیان گردیده است. «داده ترافیک، هر گونه داده‌ای است که سامانه‌های رایانه‌ای در زنجیره ارتباطات رایانه‌ای و مخابراتی تولید می‌کنند تا امکان ردیابی آنها از مبدا تا مقصد وجود داشته باشد. این داده‌ها شامل اطلاعاتی از قبیل مبدا، مسیر، تاریخ، زمان، مدت، حجم ارتباط و نوع خدمات مربوطه می‌شود.» این نوع داده‌ها در قالب متن، صوت یا تصویر نیستند تا برای مخاطب عادی قابل درک باشند بلکه آنها در جریان فعل و انفعالات فنی نقل و انتقال اطلاعات بوجود می‌ایند و در حقیقت، شناسه آن فرایند را ارائه می‌دهند، به عبارتی یک سری ارقام و عباراتی هستند که کارشناسان

4- For the purposes of this Convention:
a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;
b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a
computer system to perform a function

ISSN: 2538-3787
http://www.Joce.ir

قادرند اطلاعاتی را از آن استنتاج کنند؛ داده هایی که می‌توانند در شناسایی مخاطبان یک ارتباط نقش بسزایی داشته باشند و از لحاظ امور انتظامی و جزایی در جایگاه ویژه‌ای قرار دارند. ***[۲]***

سامانه مخابراتی

هر چندتعبیر "سامانه مخابراتی"در کنوانسیون جرایم سایبر بیان نشده است، ولی با توجه به اینکه در قانون جرایم رایانه‌ای به عنوان بستر جرم معرفی شده است، تعریف آن ضرورت می‌یابد. اگر چه امروزه، کلیه تجهیزات مخابراتی مبتنی بر رایانه هستند و از طریق پردازش خودکار داده‌ها اقدام می‌نمایند و به نوعی سامانه رایانه‌ای محسوب می‌شوند جه بسا از این جهت بوده که کنوانسیون مزبور، از این نوع سامانه ذکری به میان نیاورده است. نخستین تعریف از مخابرات در تبصره ۱ماده ۱ قانون تأسیس شرکت مخابرات ایران به این شرح بیان شده است: «مقصود از مخابرات در این قانون عبارت است از: انتقال و ارسال علائم و نوشته‌ها و تصاویر و صداها و هر گونه اطلاعات دیگر به وسیله سیم یا بی سیم و یا نور و یا هر ابزار الکترو مغناطیسی» در بند (ز) ماده ۱پیش نویس اولیه لایحه جرایم رایانه‌ای نیز سیستم مخابراتی چنین تعریف شده بود**:**

"هر نوع دستگاه یا مجموعه‌ای از دستگاه‌ها برای انتقال الکترونیکی اطلاعات میان یک (منبع فرستنده، منبع نوری) و یک گیرنده با آشکار ساز نوری از طریق یک یا چند مسیر ارتباطی به وسیله قراردادهایی که برای گیرنده قابل فهم وتفسیر باشد**"** این تعریف عینا در بند (پ) ماده یک آیین نامه نحوه استفاده از سامانه‌های رایانه‌ای یا مخابراتی بدون هیچ تغییری بیان گردیده است**.**

پیشینه تقنینی

استراق سمع یا گوش دادن پنهانی به مکالمات دیگران با احکام و موازین حفظ حریم خصوصی تزاحم دارد امری اخلافاً در خور نکوهش است. از این رو در اصل ۲۵ قانون اساسی جمهوری اسلامی ایران، بازرسی نامه‌ها و محصولات ارسال‌شده، ضبط و افشای مکالمات تلفنی اشخاص، مخفیانه گوش کردن به صحبت‌های دیگران و هرگونه تجسس در مکالمات، جز به حکم قانون، جرم دانسته شده است.بنابراین، استراق سمع بدون حکم قانون ممنوع اعلام گردیده است ***[۲]*** به جز مقررات قانون اساسی، پیشینه حمایت قانونی در قبال جرایم ارتباطاتی شهروندان به قانون تاسیس شرکت مخابرات ایران، مصوب ۱۳۵۰ باز می‌گردد**.**

در تبصره یک ماده ۴۱این قانون امده است":هر کس از وسایل مخابراتی، عمومی یا اختصاصی که در اختیار دارد به طور غیر مجاز استفاده کند در نوبت اول به او کتباً اخطار می‌شود و در نوبت دوم به مدت ۱۵ روز ارتباط او قطع یا از استفاده ممنوع خواهد شد. در صورت تکرار، اشتراک یا اجازه استفاده او لغو می‌شود و تجدید تقاضای اشتراک یا استفاده پس از انقضای شش ماه با رعایت امکانات فنی پذیرفته خواهد شد. موارد استفاده غیر مجاز در ایین نامه‌ای که از طرف شرکت تهیه و به تصویب وزیر (ارتباطات) پست و تلگراف و تلفن خواهد رسید تعیین می‌گردد.") ***[۳]***

پیشینه دیگر ماده ۵۸۲ قانون مجازات اسلامی (تعزیرات) است، این ماده مقرر می‌کند که: **"**هر یک از مستخدمین و ماموران دولتی، مراسلات یا مخابرات یا مکالمات تلفنی اشخاص را در غیر مواردی که قانون اجازه داده حسب مورد مفتوح یا توقیف یا معدوم یا بازرسی یا ضبط یا استراق سمع نماید یا بدون اجازه صاحبان آنها مطالب آنها را افشا نماید، به حبس از یک سال تا سه سال یا جزای نقدی از شش تا هجده میلیون ریال محکوم خواهد شد**."**

این ماده پیش از انکه ناظر به امور پستی باشد به امور مخابراتی مربوط می‌شود و بنابراین با توجه به تعریف گسترده‌ای که از مخابرات در نصوص قانونی آمده به خوبی شامل سوءاستفاده‌های نوین هم می‌شود و در مقام اعمال قوانین جدیدی مانند قانون جرایم رایانه‌ای، باید دامنه شمول ان را مدّنظر قرار داد). ***[۳]***

مطابق این ماده استراق سمع را صرفاً برای مستخدمان و مأموران دولتی جرم‌انگاری گردیده و شاید از این جهت که تصویب این ماده قبل از خصوصی سازی و در زمانی صورت پذیرفته که سیستم مخابراتی و جابه جایی مرسولات پستی تنها در اختیار دولت بوده لذا این جرم فقط برای کارکنان قوای عمومی و دولت پیش بینی شده بود اما با توسعه فناوری اطلاعات و ارتباطات و تنوع بسترهای انتقال محتوا و در اختیار قرار گرفتن این بستر به غیر از مامورین دولتی، ضرورت حمایت از این بستر و محرمانگی

ISSN: 2538-3787
http://www.Joce.ir

آن بیشتر احساس می‌شد. بنابراین در کنوانسیون بوداپست به کشورهای عضو توصیه شده است تا هر یک از اعضا در قوانین داخلی خود نسبت به جرم‌انگاری شنود غیر مجاز اقدام نمایند. [۲] قانونگذار کشور ما نیز در ماده ۲ قانون جرایم رایانه‌ای به جرم‌انگاری آن به عنوان جرمی علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی اقدام نموده است. مضافاً بر آن که در ماده ۶۸۳ قانون آیین دادرسی کیفری ضوابط تکمیلی بدین شرح مقرر شده است: کنترل محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی مطابق مقررات راجع به کنترل ارتباطات مخابراتی مقرر در آیین دادرسی کیفری است. دسترسی به محتوای ارتباطات غیرعمومی ذخیره شده، نظیر پیام‌نگار (ایمیل) یا پیامک در حکم کنترل و مستلزم رعایت مقررات مربوط است.

ارکان و شرایط جرم شنود غیرمجاز

رکن قانونی

رکن قانونی جرم شنود غیر مجاز ماده۲ قانون جرایم رایانه‌ای می‌باشد مطابق این ماده: «هر کس به طور غیر مجاز محتوای در حال انتقال ارتباطات غیر عمومی در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری را شنود کند به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون (۱۰۰۰۰۰۰۰) ریال تا چهل میلیون (۴۰۰۰۰۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد». قابل توجه این که مجازات جزای نقدی مندرج در این ماده به موجب مصوبه مورخ۱۳۹۹/۱۲/۲۵ هیات وزیران به بیست و پنج میلیون (۲۵.۰۰۰.۰۰۰) ریال تا صد و پنجاه میلیون (۱۵۰.۰۰۰.۰۰۰) ریال تعدیل شده است.

مطابق منطوق و مفهوم مندرجات ماده ۲ قانون جرایم رایانه‌ای برای تحقق جرم شنود غیرمجاز، رفتار مجرمانه معینی نسبت به موضوع جرم باید ارتکاب یابد. مرتکب رفتار مجرمانه توصیف خاصی ندارد. هر یک از شهروندان اعم از کارکنان بخش‌های عمومی، دولتی، خصوصی یا شهروندان عادی در قبال شنود مسئول شناخته خواهند شد. مشروط به آن که این رفتار شنود غیرمجاز در بستر سامانه‌های رایانه‌ای یا شبکه‌های مخابراتی انجام شود. در حال انتقال بودن داده محتوی و وصف غیرعمومی بودن پیام مورد مبادله، از شروط مهم قانونی است که در این ماده به آنها اشاره شده و در بررسی سایر ارکان مورد مطالعه قرار خواهند گرفت.

رکن مادی

رفتار مجرمانه

عمل مادی و رفتار مرتکب این جرم، شنود است. هرچند معنی شنود ظهور در استماع الفاظ و محاورات دارد اما منظور از شنود در ماده ۲ قانون جرایم راینه‌ای صرفاً شنیدن محتوی مکالمات صوتی یا پیام های شنیداری با قوای سماعی نیست تا تنها شامل محتوای صوتی شود بلکه به معنای دریافت کردن محتوی یا در اختیار گرفتن آن است، از اینرو مشاهده نمودن محتوی با قوای بصری، گرچه عرفا و منطقا از طریق حس شنوائی صورت نمی‌گیرد اما از نظر قانونی مصداق شنود محسوب می‌شوند. برای رفع چنین ابهاماتی سابقاً واژه «دریافت» به جای شنود در متن لایحه اولیه پیشنهاد شده به مجلس قید شده بود ولی به دلیل همپوشانی بسیار با واژه شنود کنار گذاشته شد. همچنین واژه شنود در بند «و» ماده یک آیین نامه جمع‌آوری و استنادپذیری ادله الکترونیکی مرادف با دریافت به این شرح تعریف گردیده است "هرگونه دستیابی به محتوای در حال انتقال ارتباطات غیر عمومی در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی با استفاده از سامانه‌ها و تجهیزات سخت افزاری و نرم افزاری مربوط.» [۲] نتیجه آن که شنود محتوا اعم از دریافت اطلاعات شنیداری است و شامل اطلاعات نوشتاری و دیداری هم می‌گردد. نظیر رفتاری شخصی که از طریق بلوتوث پیام نوشتاری، صوتی یا تصویری از شخصی که در حال انتقال به دیگری را به طور غیر قانونی دریافت می‌کند. یا متصدیان شبکه‌های ارتباطی، ارائه دهند خدمات رایانه‌ای، سرورهای میزبانی یا شبکه‌های اجتماعی اقدام به دستیابی غیرقانونی محتوی پیام‌های نوشتاری، دیداری یا شنیداری نمایند که کاربران آنها در حال ارسال به مخاطبان انتخابی خود هستند. به این ترتیب روشن می‌شود که رفتار شنود تنها از طریق فعل مثبت امکان پذیر است زیرا فرض شنود از طریق ترک فعل امری بعید به نظر می‌رسد. واژه غیر مجاز که در این ماده به آن اشاره گردیده گرچه با نظر به حریم

ISSN: 2538-3787
http://www.Joce.ir

شخصی و خصوصی شهروندان، به معنای دریافت محتوی بدون اجازه و رضایت دارنده آن است اما محدود به اذن و اجازه نیست. بدین توضیح که بنا به مصالح عمومی، ممکن است به حکم قانون ولو بدون رضایت دارنده یا ارسال کننده محتوی، پیام دیداری، شنیداری یا نوشتاری اصطلاحاً شنود شوند. لذا چنانچه رفتار شنود محتوا توأم با رضایت دارنده باشد و نیز شنود با مجوز قانونی و حتی بدون رضایت دارنده محتوا، رفتار مجرمانه بنوده و موضوع این ماده نخواهد بود. [۲]

رفتار مجرمانه شنود غیرمجاز همانند دسترسی غیرمجاز می‌تواند مقدمه و زمینه ساز جرایم سایبری باشد لذا در زمره جرایم مادر و محرک می‌باشد. [۱] وجه تمایز شنود غیرمجاز از جرم دسترسی غیرمجاز موضوع جرم می‌باشد موضوع جرم دسترسی غیرمجاز داده‌های ذخیره شده و یا داده‌های در حال پردازش در سامانه‌های رایانه‌ای یا مخابراتی است که به طور غیرمجاز توسط افراد ناصالح مورد رصد قرار می‌گیرند. ولی موضوع جرم شنود غیرمجاز محتوای در حال انتقال ارتباطات غیر عمومی در سامانه‌های رایانه‌ای و مخابراتی یا امواج الکترومغناطیسی یا نوری می‌باشد و هر گونه کیفیت اضافه بر آن جرم را با توصیف‌های دیگر همراه کرده و حتی می‌تواند موجب تحقق تعدد جرم باشد. [۱۱]

شنود غیرمجاز محتوای در حال انتقال پدیده‌ای خاص است و با استراق سمع تفاوت دارد زیرا استراق سمع به صورت شنیداری و در بستر مکالمات تلفنی مخابراتی صورت می‌گیرد اما عمل شنود تنها در خصوص سیگنال‌ها و امواج مطرح می‌باشد این سیگنال‌ها و امواج ممکن است به صورت نوری صوتی و الکترومغناطیسی (رادیویی، مادون قرمز، ماورای بنفش) باشد. هر یک از موارد ذکر شده می‌توانند به صورت آنالوگ و دیجیتال مبادله شوند. [۱] در رفتار مجرمانه این جرم برخلاف دسترسی غیر مجاز الزامی به حفاظت داده‌ها به وسیله تدابیر امنیتی وجود ندارد و صرف شنود محتوای ارتباطات غیر عمومی موجب تحقق این جرم می‌شود. [۱۱] با توجه به این که شنود به معنای صرف دریافت و دستیابی به محتوا است بنابراین استمرار رفتار در آن شرط نیست، از اینرو همانند دسترسی غیر مجاز رفتار مجرمانه ی آنی است. [۲]

موضوع جرم و شرایط آن

موضوع جرم شنود غیر مجاز، دریافت محتوای در حال انتقال می‌باشد. شرط اساسی در تحقق جرم مزبور مطابق ماده ۲ قانون جرایم رایانه‌ای دریافت غیرقانونی محتوای در حال انتقال است. اینک پرسش مهم آن است که منظور از محتوا چیست و چه نوع داده‌هایی را در بر می‌گیرد؟ در ماده ۱ قانون جرایم رایانه‌ای«داده محتوا» چنین تعریف شده: "داده محتوا: هر نمادی از موضوع‌ها، مفهوم‌ها، دستورالعمل‌ها نظیر متن صوت یا تصویر که به صورت در جریان یا ذخیره شده، که به منظور برقراری ارتباط بین سیستم‌های رایانه‌ای یا پردازش توسط شخص یا سیستم رایانه‌ای به کار گرفته شده و به وسیله سیستم رایانه ایجاد شود". [۲۲] در واقع به داده‌هایی که حاوی مفاهیم قابل فهم و درک برای انسان باشد داده محتوا گفته می‌شود و می‌توان تعبیر اطلاعات را در مورد این نوع داده‌ها به کار برد. داده محتوا (اطلاعات) حاصل پردازش داده‌های رایانه‌ای است بدین مفهوم که داده‌های رایانه‌ای بعد از پردازش به صورت داده محتوا نمود پیدا می‌کند و یا به عبارت ساده‌تر همان خروجی سامانه رایانه‌ای است که می‌تواند به صورت متن، صوت، فیلم یا تصویر نمود یابد. [۲]

اما سایر داده‌ها از جمله داده ترافیک نمی‌توانند موضوع جرم شنود غیرمجاز قرار گیرند. زیرا داده ترافیک همان طور که در مفاهیم بیان شد، داده‌هایی هستند که در قالب متن، صوت یا تصویر نیستند تا برای مخاطب عادی قابل درک باشند بلکه انها در جریان فعل و انفعالات فنی نقل و انتقال اطلاعات به وجود می‌آیند و در حقیقت، شناسه آن فرآیند را ارائه می‌دهند؛ به عبارتی این داده‌ها نه صوت و نه تصویر هستند بلکه یکسری ارقام و عباراتی می‌باشند که کارشناسان فنی قادرند اطلاعات راجع به مقصد، تاریخ، اندازه، مدت زمان و نوع خدمات اصلی مورد استفاده در برقراری ارتباط را از آنها استنتاج کنند؛ داده‌هایی که می‌توانند در شناسایی مخاطبان یک ارتباط نقش بسزایی داشته باشند و از لحاظ امور انتظامی و جزایی در جایگاه ویژه‌ای قراردارند.[۹]

مطابق آنچه در ماده یک قانون جرایم رایانه‌ای به عنوان موضوع جرم بیان شد، محتوی است. همانطور که می‌دانیم محتوی مصداق خاصی از داده است زیرا محتوی یا (داده محتوی) به داده‌های گفته می‌شوند که حاوی مفاهیم قابل فهم و درک برای انسان باشد و به نوعی می‌توان تعبیر «اطلاعات» را در مورد این نوع داده‌ها به کار برد. داده محتوا یا اطلاعات، حاصل پردازش داده‌های رایانه‌ای است؛ بدین مفهوم که داده‌های رایانه‌ای بعد از پردازش به صورت داده محتوا نمود پیدا می‌کند به عبارت

ISSN: 2538-3787
http://www.Joce.ir

ساده‌تر به خروجی سامانه‌های رایانه‌ای که می‌تواند به صورت متن، صوت، فیلم یا تصویر آشکار گردد؛ داده محتوا یا اطلاعات می‌گویند. در حالی که داده رایانه‌ای مفهومی عام‌تر و به مجموعه مطالب ورودی به رایانه پیش از پردازش اطلاق می‌شود. بنابراین شنود محتوا علاوه بر دریافت اطلاعات شنیداری شامل اطلاعات نوشتاری و دیداری هم می‌گردد. [۲]

درحال انتقال بودن محتوی

از جمله شرایط مهم تحقق جرم شنود غیرمجاز مطابق ماده ۲ ق.ج.ر در صورتی است که رفتار مجرمانه نسبت به محتوای در حال انتقال انجام شود. محتوای در حال انتقال در برابر محتوای ذخیره شده قرار دارد. به محتوایی در حال انتقال اطلاق می‌شود که داده مربوط به محتوی یا اطلاعات از یک مقصد منفک و به مقصد دیگری در حال جابجایی و انتقال باشد. در نتیجه موضوع شنود غیرمجاز علاوه بر آن داده محتواست و شامل شنود غیرمجاز داده ترافیک نمی‌شود؛ همزمان باید این محتوی در حال جابجایی باشد. بنابراین اگر فردی داده ترافیک ولو در حال انتقال را شنود و دریافت کند نظیر آن که اطلاعاتی از قبیل مبدا، مسیر، تاریخ، زمان، مدت و حجم ارتباط را دریافت نماید؛ مشمول جرم شنود غیرمجاز نخواهد بود.

همچنین با توجه به این که رفتار مجرمانه در جرم شنود غیر مجاز نسبت به محتوای در حال انتقال انجام می‌شود؛ از این رو شامل محتوای ذخیره شده که در حال انتقال نباشد، نخواهد شد. چنین رفتاری یعنی دریافت محتوای ذخیره شده به شرط این‌که محتوا یا سامانه تحت تدابیر امنیتی حفاظت شده باشد، مشمول وصف جرم دسترسی غیر مجاز است. [۲] برای مثال اگر شخصی به محتوای ذخیره شده در صندوق دریافت ایمیل دیگری دسترسی یابد؛ مشمول شنود غیر مجاز نیست. واضح است که شنود محتوای ارتباطات در فضای تبادل در طول مسیر انتقال توسط شخص ثالث انجام می‌شود. [۵]

اگر شخص ثالثی با تجهیزات فنی اقدام به ضبط محتوای در حال انتقال نماید مشمول شنود غیرمجاز موضوع این ماده است چرا که دستیابی از سوی این شخص در زمان انتقال محتوا انجام گرفته و اگر چه بعدا ضبط و ذخیره شده باشد اما اگر شخص دیگری به این محتوای ضبط و ذخیره شده دست یابد یا آنها را دریافت کند؛ رفتار آن شخص مشمول جرم شنود غیرمجاز نخواهد بود. چون دسترسی وی به محتوی مزبور در هنگام انتقال داده نبوده بلکه پیام ارتباطی پس از خاتمه ارسال توسط شخص، دریافت شده است. با این حال چنانچه این محتوا تحت تدابیر امنیتی حفاظت قرار داشته باشد؛ رفتار ارتکابی شخص دریافت کننده مشمول عنوان مجرمانه دسترسی غیر مجاز دانست.

غیر عمومی بودن محتوی

واژه غیر عمومی بودن به ماهیت فرایند انتقال و نه ماهیت محتوای در حال انتقال اشاره دارد. بنابراین محتوای در حال انتقال باید در بستر ارتباطات غیر عمومی (خصوصی) باشد؛ بدین معنا که الزاماً فرایند انتقال باید خصوصی و تحت محرمانگی باشد، به نحوی که منحصراً شخص یا افراد خاصی قانوناً اختیار دریافت آن را داشته‌اند و دیگران مجاز به دریافت آن نباشند، نه آن که مضمون محتوی هم می‌بایست کاملاً شخصی و خصوصی باشد. از اینرو وصف محتوی ممکن است عمومی یا غیر عمومی باشد. تنها کافی است که فرآیند انتقال محتوی در بستر ارتباطات غیرعمومی باشد هر چند که محتوی در این فرایند محتوایی عمومی باشد. نظیر اینکه در فرایند ارتباط خصوصی میان دو نفر محتوای مربوط به اخبار سراسری پخش شده در حال انتقال باشد. دریافت چنین محتوایی توسط سایرین مشمول شنود غیر مجاز خواهد بود. [۲]

ارتباط غیر عمومی، ارتباطی بین دو یا چند شخص به صورت هماهنگ با یکدیگر و با مبدا، مقصد و مسیر انتقال مشخص برقرار می‌شود. [۲۲] عمومی یا خصوصی بودن فرایند ارتباط، نسبی است؛ به طور مثال، فرایند ارتباط گروه‌های اجتماعی یا چت روم نسبت به اعضا، عمومی و نسبت به غیر اعضا خصوصی به حساب می‌آید. [۲] ملاک شناسایی عمومی بودن محتوای اطلاعات یا نبودن آن، به ماهیت محتوای ارسالی و قصد ارسال کننده وابسته می‌باشد؛ مثلاً ارسال امواج رادیویی یا تلویزیونی، عمومی است ولی ارسال پیامک، متنی یا تصویری، میان دو نفر، و نیز امواج و سیگنال‌های حاوی داده‌های ادارات دولتی موجود در سامانه‌های آنها در بستر فضای سایبر، غیرعمومی است. [۱۱]

قانون گذار در جرم‌انگاری شنود غیر مجاز بیشتر به معنای عرفی تعبیر غیرعمومی، توجه داشته است که پس از دریافت محتوای مبادلاتی، حتماً بایستی به وسیله یک سری عملیات به صورت اصلی درآید تا قابل شناسایی باشد .لذا این واژه دارای

ISSN: 2538-3787
http://www.Joce.ir

ابهام است). ***[۵]*** و لازم است تا مقنن رفع ابهام نماید. نکته دیگر که در مورد غیرعمومی بودن محتوی وجود دارد این است که نیاز نیست محتوا با تدابیر امنیتی حفاظت شده باشد بلکه به صرف شنود محتوای غیر عمومی، این جرم محقق می‌شود.

نتیجه ارتکاب جرم

نتیجه رفتار مرتکبان این جرم بسیار ساده بوده و چه بسا تنها در یک واژه قابل انعکاس و بازتاب باشد. آن نتیجه، دریافت و شنود است. یعنی به محض دریافت یک محتوای در حال انتقال از یک ارتباط غیر عمومی، شنود تحقق پیدا خواهد کرد. مثلاً مرتکب اقدام به دریافت تصاویر در حال ارسال در سامانه‌های رایانه‌ای می‌نماید یا مکالمات در حال انجام در شبکه‌های اجتماعی را به طور غیرقانونی شنود می‌کند. نکته مهم این است که لازم نیست مرتکب در همان لحظه از مفاد محتوا آگاهی پیدا کند و آن را درک کند. کما این که در شنود مکالمات تلفنی هم شنود کننده ممکن است همزمان از مفاد مکالمه آگاه نشود و تنها به ضبط آن بسنده کند و در زمان دیگری برای آگاهی از محتوا به آن مراجعه کند حتی ممکن است قبل از آگاهی و درک محتوا تحت پیگرد قرار گرفته و دستگیر شود. نظیر موردی که محاورات در حال انجام به زبان یا گویشی است که مرتکب قادر به فهم و درک آنها در زمان ارتکاب جرم شنود غیرمجاز نیست.

همچنین ممکن است شنود به طور واقعی و زنده صورت گیرد و مرتکب همزمان از مفاد محتوای ارتباطی آگاه گردد. لیکن آگاهی از محتوای در حال جریان شرط لازم برای تحقق نتیجه این جرم به شمار نمی‌آید. و صرف دریافت محتوا چه بالمباشره و چه به تسبیب برای تحقق نتیجه جرم کافی خواهد بود***[۳]*** شنود غیرمجاز مانند دسترسی غیرمجاز جرم مطلق می‌باشد و قانونگذار آن را مقید به نتیجه خاصی ندانسته است و صرفاً با انجام عمل مادی این جرم محقق می‌گردد. ***[۲]***

بستر ارتکاب جرم

در ماده ۲ ق.ج.ر برای تبیین بستر ارتکابی شنود، واژه ارتباطات بکار رفته است. ارتباط در مفهوم عام، به معنای برقراری پیوند معنادار و هدفمند میان دو یا چند چیز است که مصادیق آن می‌تواند انسان، سایر جانداران و اشیا باشند. اما در مفهوم خاص، ارتباطات رایانه‌ای، پستی و مخابراتی متناظر آن شده که حسب مورد میان انسان‌ها با یکدیگر، انسان‌ها با سامانه‌ها و یا سامانه‌ها با یکدیگر برقرار می‌شود.

با توجه به کثرت مفهوم و معنی ارتباط، مسأله قابل بررسی این است که در این ماده کدامیک از معانی و مفاهیم ارتباطات مقصود قانونگذار است؟ آیا هر شکل از ارتباط، اعم از ارتباط سامانه با سامانه، انسان با انسان و سامانه با انسان را در بر می‌گیرد؟ یا اینکه باید به مفهوم خاص آن بر پایه مفهومی متداول و عام که از دیر باز در پیشینه قانون گذاری کشورها وجود داشته بسنده کرد؟ با توجه به نوپدید بودن جرایم رایانه‌ای و فلسفه جرم‌انگاری این گونه از جرایم نوظهور به نظر می‌رسد که پذیرش مفهوم عام از ارتباطات با اغراض مقنن سازگارتر باشد. تا آنجا که ارتباط بین اجزای یک سامانه توسط انسان را هم می‌توان مشمول این حکم دانست. برای مثال هنگامی که شخصی از یک صفحه کلید بدون سیم برای وارد کردن داده‌های خود استفاده می‌کند تردیدی وجود ندارد که از مصادیق ارتباط خواهد بود و در نتیجه در دامنه شمول این ماده قرار خواهد گرفت. حتی برخی تجهیزات تولیده شده وجود دارند که با بکار گیری آنها از فاصله مناسب می‌توان نوسانات کابل‌های رابط را دریافت کرد و داده‌های شنیداری، دیداری یا نوشتاری در حال انتقال آنها را دریافت کرد. مؤید چنین دیدگاهی وضع عبارت سامانه‌های رایانه‌ای در کنار سامانه‌های مخابراتی در ماده ۲ ق.ج.ر است، چنانچه تفسیری جز این داشته باشیم، قید عبارت مخابراتی یا امواج الکترومغناطیسی از سوی قانونگذار کاربردی نخواهند داشت.

مضاف بر آنکه کنوانسیون جرایم سایبری هم به کشورهای عضو اجازه می‌دهد که مفهوم ارتباطات را به وجود دو یا چند سامانه تسری دهند یا ارتباطات میان اجزای یک سامانه را نیز مشمول عنوان مجرمانه شنود بداند. علاوه بر اینکه دلیلی وجود ندارد داده‌های در جریان میان اجزای یک سامانه از چنبن حمایتی برخوردار نباشد. مضاف براین انچه گستره به ظاهر گسترده، قلمرو مشخص و معنا داری می‌بخشد قید "غیر عمومی" گنجانده شده در ماده ۲ ق.ج.ر است. دریافت محتواهایی که به طور عمومی پخش می‌شود را از شمول ماده خارج می‌کند.

ISSN: 2538-3787
http://www.Joce.ir

سرانجام وجود کلمه "در" پیش از تعبیر (سامانه‌های رایانه‌ای و مخابراتی،) دریافت و ضبط هر گونه محتوا از محیط فیزیکی به وسیله‌ی ابزارهای الکترونیک را از شمول این ماده خارج می‌کند. زیرا رخداد آنها در فضای غیر سایبر و محیطی خارج از سامانه‌های مقرر قانونی به وقوع پیوسته است.

رکن روانی

شنود غیرمجاز موضوع ماده ۲ قانون جرایم رایانه‌ای جرمی عمدی است که نیازمند وجود قصد و سوءنیت است. رکن روانی جرم شنود غیرمجاز متشکل از دو جزء علم و اراده است؛ علم و آگاهی به رفتار غیرقانونی شنود محتوی، آگاه بودن از غیرعمومی یا خصوصی بودن فرآیند انتقال محتوی و اراده یا قصد برای دریافت محتوی و انجام شنود. یعنی مرتکب با اراده آگاه قصد دارد تا محتوی را بر خلاف قانون دریافت کند و عامدانه بخواهد تا اقدام به شنود محتوای دیگری نماید با آگاهی و علم به اینکه در بستر ارتباط خصوصی مبادله پیام صورت می‌گیرد. بنابراین چنانچه شخصی ناخواسته یا ندانسته، به صورت اتفاقی محتوای در حال انتقال دیگری را شنود کند؛ مطابق ماده ۲ ق.ج.ر رفتارش جرم نبوده و در نتیجه مجازات نمی‌گردد.

صرف وجود سوء نیت عام برای تحقق جرم شنود غیرمجاز کفایت می‌کند. بنابراین از آنجا که جرم مزبور از جرایم مطلق است و مقید به نتیجه نیست لذا به قصد و سوء نیت خاص نیاز ندارد. [۲] در نتیجه تنها قصد عام یعنی اراده آگاه مرتکب به غیرقانونی بودن شنود و دریافت محتوی برای تحقق جرم ضرورت دارد. همچنین انگیزه در وصف کیفری این رفتار مانند بسیاری از جرایم دیگر بی تأثیر است و از جایگاه خاصی برخوردار نمی‌باشد. [۱]

مجازات

ماده ۲ ق.ج.ر مجازات جرم شنود غیرمجاز را حبس از ۶ ماه تا ۲ سال یا جزای نقدی از ده میلیون ریال تا چهل میلیون ریال یا هر دو مجازات و بیان نموده است. این گونه که معلوم است این مجازات‌ها که طیف گسترده‌ای را در بر می‌گیرد، قانونگذار خواسته اساراده کرده تا در اختیار و به صلاح دید قاضی واگذار شود. چرا که این جرم بر خلاف ظاهرش گونه‌های فراوان وگسترده‌ای را در بر می‌گیرد که به همان نسبت می‌تواند آسیب‌های کم یا زیادی را به بزه‌دیدگان وارد آورد. در مورد شروع به جرم این جرم نظرات مختلفی وجود دارد، برخی معتقدند با توجه به اینکه مجازات جرم شنود غیر مجاز درجه ۶ می‌باشد مطابق ماده ۱۲۲ قانون مجازات اسلامی شروع به جرم شنود غیرمجاز نه جرم و نه قابل مجازات است. [۲] ولی از منظر دانش مهندسی رایانه و واقعیت عینی، امکان تحقق شروع به جرم در شنود غیر مجاز وجود دارد [۱] برخی نیز با توجه به تعریف شروع به جرم، تحقق آن را در جرایم مطلق هم متصور می‌دانند [۲۳] در صورت تکرار بیش از دو بار این جرم دادگاه می‌تواند مرتکب را به مجازات تکمیلی مذکور در بند الف ماده ۲۷ ق.ج.ر محکوم نماید [۲] چنانچه اشخاصی در ارتکاب جرم شنود غیرمجاز مباشرت ننمایند ولیکن از طریق انتشار و یا در دسترس قرار دادن محتویات آموزش شنود غیرمجاز در این جرم معاونت کنند تحت عنوان مستقل به شرح مذکور در بند چ ماده ۲۵ ق.ج.ر مجازات می‌گردند انتشار یا در دسترس قراردادن محتویات آموزش شنود غیرمجاز، داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی حرم بوده .و چنان چه اشخاص یاد شده این کار را به عنوان حرفه خود قرار داده باشند مطابق تبصره ماده مذکور به حداکثر هر دو مجازات مذکور در این ماده محکوم می‌شود؛ مانند اینکه شغل شخصی در دسترس قرار دادن محتویات آموزش شنود غیرمجاز از طریق آموزش و برگزاری دوره در این زمینه باشد. شرکت و معاونت در جرم موضوع این ماده هم تابع قواعد و عمومات حقوق کیفری است. [۱]

برخی معتقدند با تصویب ماده ۲ ق.ج.ر با توجه به گستردگی و شمول این ماده، بخشی از ماده ۵۸۲ قانون مجازات اسلامی که درباره شنود غیرمجاز کارمندان دولتی است نسخ گردیده و از این پس همه شنودهای غیر مجاز با دستاویز ماده ۲ ق.ج.ر مشمول کیفر می‌گردد. هنگامی که مرتکب کارمند دولت باشد با توجه به بند یک ماده ۲۶ ق.ج.ر مجازات تشدید می‌شود [۲]

سرانجام مسئولیت شخص حقوقی نیز باید مورد توجه قرار گیرد. این موضوع از آن جهت اهمیت دارد که احتمال وقوع آن از سوی موسسات بنگاه‌ها و شرکت‌ها وجود دارد. بسیاری از کارفرمایان به دلایل گوناگون مایل هستند که ارتباطات کارکنانشان را شنود کنند. همچنین ارائه دهندگان خدمات مخابراتی نیز که هم اینک طیف بسیار گسترده‌ای از ارتباطات را برای کاربران

ISSN: 2538-3787
http://www.Joce.ir

شان فراهم می‌کنند در معرض ارتکاب چنین جرمی قرار دارند. به این ترتیب با عنایت به اینکه ماده (۱۹ ق.ج.ر) ارتکاب جرایم رایانه‌ای از سوی اشخاص حقوقی را سزاوار کیفر دانسته است و در تسری حکم ماده ۲ ق.ج.ر به این ماده تردیدی وجود ندارد، در صورت جمع بودن شرایط حاکم بر آن کیفرهای مقرر در ماده (۲۰ ق.ج.ر) بر شخص حقوقی اعمال خواهد شد. [۱۴]

مقایسه ماده ۲قانون جرایم رایانه‌ای با ماده ۴۸ این قانون

ماده ۴۸ ق.ج.ر نیز درباره شنود است منتها در ان ضوابط امکان شنود مجاز و قانونی را بیان می‌کند که مانند مقررات شنود مجاز مکالمات تلفنی است. اما در ماده ۲ ق.ج.ر شنود غیر مجاز، جرم‌انگاری شده و مجازات ان نیز تعیین گردیده است. بنابراین ماده ۴۸ ق.ج.ر درباره شنود مجاز و احکام ان است اما ماده ۲ این قانون درباره شنود غیر مجاز می‌باشد. [۱۱] تبصره ماده ۴۸ ق.ج.ر دسترسی به محتوای ارتباطات غیر عمومی ذخیره شده را در" حکم شنود "می داند. ابهامی که در اینجا وجود دارد، آن است که شرط تحقق جرم شنود غیر مجاز" در حال انتقال بودن ارتباطات" است اما با توجه به تبصره ماده ۴۸ ق.ج.ر شنود محتوای ذخیره شده یا آماده انتقال نیز مشمول ماده ۲ ق.ج.ر می‌باشد؟

ظاهر قانون اقتضای پاسخ مثبت را دارد زیرا ظاهر تبصره حرف تفسیر است پس در حکم شنود دانسته است امکان دارد گفته شود حرف" و" در تبصره حرف تفسیر است پس در حکم شنود بودن به معنای لزوم رعایت مقررات شنود می‌باشد نه اینکه مجازات شنود نیز نسبت به آن اعمال شود نتیجه این که شرط در حال انتقال بودن برای تحقق این جرم لازم است. [۱۱]

مقایسه ماده ۲ ق.ج.ر با ماده ۵۸۲ قانون مجازات اسلامی

جرم شنود یا استراق سمع موضوع ماده ۵۸۲ قانون مجازات اسلامی با جرم شنود غیرمجاز موضوع ماده ۲ ق.ج.ر تفاوت دارد:

الف-جرم شنود موضوع ماده (۵۸۲ ق،م،ا) ویژه جرایم مخابراتی سنتی و استماع مکالمات تلفنی می‌باشد در حالی که شنود غیر مجاز موضوع ماد ۲ ق.ج.ر راجع به شنود در فضای مجازی نیز می‌شود.

ب-جرم شنود موضوع ماده ۵۸۲ راجع به شنیدن غیر مجاز در حین مکالمات صوتی و احیاناً ضبط آن می‌باشد، در حالی که جرم شنود غیر مجاز مقرر در ماده ۲ ق.ج.ر به کنترل یا نظارت یا مراقبت یا هر نوع رهگیری یا مسیر یابی یا بررسی یا تجزیه و تحلیل داده‌ها یا امواج الکترومغناطیسی یا نوری در حال انتقال جهت اطلاع از محتوای آن و اقدامات مشابه، اطلاق می‌گردد.

ج-جرم شنود یا استراق سمع موضوع ماده (۵۸۲ ق،م،ا) صرفاً از ناحیه ماموران دولت قابل ارتکاب است، در حالی جرم شنود غیر مجاز ماده ۲ ق.ج.ر از ناحیه هر شخص قابل ارتکاب است. [۱۲]

برآمد و نتیجه

از جمله موضوعاتی که ضروری است به هنگام وضع قوانین به ویژه قوانین کیفری حوزه فناوری ارتباطات آن توجه شود رویکرد به اصطلاح فناوری خنثی یا بی طرف است به این معنا که قانونگذار خود را به رفتار یا ابزار یا وسیله خاصی محدود نمی کند تا چنانچه نمونه‌های نوآورانه‌ای به وجود آمدن با بن بست در اجرا مواجه نشود. برای مثال چنانچه برای شنود تنها به ذکر تلفن بسنده می‌شد سایر سامانه‌های پیام رسان الکترونیک را دربر نمی گرفت و نارسایی قانونی جدی پدید می‌آمد. خوشبختانه قانونگذار ایران خواسته یا ناخواسته به این امر مهم پایبند بوده است بنابراین سنگ بنای نخستین این حوزه به درستی پایه گذاری شده است و راه را برای قانونگذاری‌های بعدی هموار کرده است. از بررسی ماده ۲ قانون جرایم رایانه‌ای در کنار سایر احکام قانونی مرتبط می‌توان امیدوار بود که کاستی‌ها و نارسایی‌های قانون که زمینه سوء استفاده از آن را فراهم کند وجود نخواهد داشت. اما نادیده انگاشتن یا نادیده ماندن برخی از موضوعات می‌تواند اجرای شایسته این حکم را با محدودیت روبرو کند.

درباره موضوع جرم همان گونه که بیان شد؛ محتوای رایانه‌ای مورد توجه قانونگذار قرار گرفته است با توجه به اینکه دیدگاه‌های مختلفی در مورد شمول یا عدم این ماده در مورد داده ترافیک وجود دارد ضروری است از دریافت غیرمجاز این داده‌ها هم حمایت کیفری به عمل آید و اینگونه ابهامات برطرف شود. در حال انتقال بودن ویژگی ذاتی جرم شنود است و حساسیت این محتواها به حدی است که نوع ذخیره شده آنها، ولو باید با درجه کمتری، مورد حمایت کیفری قرار گیرد.

ISSN: 2538-3787
http://www.Joce.ir

در مورد مفهوم و گستره ارتباطات هم دیده شد دو مفهوم بسیار گسترده و بسیار محدود قابل استنباط است. شاید موثرترین عنصری که می‌تواند اجرای این حکم را با چالشی جدی روبرو کند همین واژه باشد. به نظر می‌رسد قانونگذار باید وارد عمل شود و منتظر رویه قضایی نماند زیرا ممکن است برخی با ضمانت اجراهای سنگین کیفری روبرو و برخی دیگر از مجازات متناسب و بازدارنده معاف گردند.

غیر عمومی بودن ارتباط نیز یکی از عناصر اصلی جرم شنود می‌باشد. سزاوار است قانونگذار با بیان مصادیقی از باب تمثیل به شناسایی سایر مصادیق متناسب به مقام قضایی صلاحیتدار کمک کند.

همان گونه که ملاحظه شد؛ در مورد امکان تحقق شروع به جرم هم نظرات مختلفی وجود دارد؛ شایسته است که قانون گذار این ابهام را برطرف کند. نقدی که به مجازات مقرره در این ماده وجود دارد؛ این است که به نظر می‌رسد مجازات نه کافی و بازدارنده نیست و با شدت این جرم تناسبی ندارد، لذا در مورد کیفر این جرم پیشنهاد می‌گردد قانونگذار از توانمندی کیفرهای اجتماعی، برای افزایش میزان بازدارندگی این ضمانت اجراها بهره گیرد. اصل محرومیت از اشتغال در مشاغلی که امکان ارتکاب دوباره این جرم را فراهم می‌سازد یا محدودیت از اشتراک یا کاربری خدمات ارتباطات عمومی الکترونیک، می‌تواند دستاورد بازدارندگی خوبی نسبت به جزای نقدی یا حبس در بر داشته باشد.

یافته‌ها حاکی از ان است که در مورد اوصاف شخص مرتکب، شرط خاصی وجود ندارد. ولی در مورد اوصاف شنود غیر مجاز بودن و در مورد اطلاعات مورد شنود غیر عمومی بودن و در حال انتقال بودن شرط است. همچنین این جرم مقید به نتیجه نبوده و عنصر معنوی به سوءنیت خاص نیاز ندارد. تحقق رکن مادی با فعل مثبت بوده و ترک فعل نمی تواند عنصر تشکیل دهنده ان باشد.

ISSN: 2538-3787
http://www.Joce.ir

منابع و مراجع

[۱] الهی منش، (۱۳۹۸)؛ محمد رضا؛ سدره نشین، ابوالفضل؛ محشّای قانون جرایم رایانه‌ای، چاپ ۷، تهران، انتشارات مجد
[۲] بابایی، جواد؛ (۱۳۹۸)؛ جرایم رایانه‌ای و آیین دادرسی حاکم بر آن، چاپ ۲، تهران، انتشارات مرکز آموزش قوه قضائیه.
[۳] بهره‌مند، حمید؛ جلالی فراهانی، امیر حسین، (۱۳۹۳)؛ شنود ارتباطات الکترونیک در حقوق کیفری ایران، فصلنامه مجلس و راهبرد، شماره ۷۸، سال.
[۴] پیش نویس اولیه لایحه قانون جرایم رایانه ای
[۵] ترکی، غلام عباس، (۱۳۸۸)؛ نگرش علمی وکاربردی به قانون جرایم رایانه‌ای، ماهنامه دادرسی، صص .
[۶] جاویدنیا، جواد، (۱۳۸۷) جرایم تجارت الکترونیک، چ۱، تهران، انتشارات خرسندی
[۷] دهخدا، علی اکبر، (۱۳۵۲)؛ لغت نامه، تهران، چاپخانه و انتشارات دانشگاه تهران
[۸] زراعت، عباس، (۱۳۹۴)؛ شرح مختصر ق.م.ا، جلد۲، چاپ۱، تهران، انشارات ققنوس
[۹] زندی، محمد رضا؛ (۱۳۹۷)؛ تحقیقات مقدماتی در جرایم سایبر، چاپ ۱، تهران، انتشارات جنگل، جاودانه،
[۱۰] زندی، محمد رضا؛ مشتاقی، مریم؛ (۱۳۹۵)؛ شنود غیر مجاز و رویه جرایم رایانه‌ای، چاپ۱، تهران، انتشارات مجد،
[۱۱] صالح احمدی، سحر؛ (۱۳۹۸)؛ جرایم رایانه‌ای در نظم کنونی، چاپ۱، تهران، کتاب اوا،
[۱۲] صنعتی، سید مهدی؛ عطایی جنتی، مجید؛ (۱۳۹۷)؛ تحلیلی برجرایم رایانه‌ای و مخابراتی (جرایم در بستر رایانه، فضای مجازی، شبکه‌های اجتماعی و پیام رسان) چاپ۱، قم، نشر حقوق پویا،
[۱۳] عالی پور، حسن، (۱۳۹۵)؛ حقوق کیفری فناوری اطلاعات، چاپ۴، تهران، انتشارات خرسندی،
[۱۴] فضلی، مهدی؛ (۱۳۹۶)؛ مسئولیت کیفری در فضای سایبر، چاپ۳، تهران، انتشارات خرسندی،
[۱۵] قانون اساسی جمهوری اسلامی ایران ۱۳۵۸
[۱۶] قانون تاسیس شرکت مخابرات ایران ۱۳۵۰
[۱۷] قانون تجارت الکترونیک، ۱۳۸۲
[۱۸] قانون جرایم رایانه‌ای، ۱۳۸۸
[۱۹] قانون مجازات اسلامی، ۱۳۹۲
[۲۰] قربانی نژاد کوهستانی، اعظم؛ (۱۳۹۶)؛ جرایم علیه محرمانگی داده ها: دسترسی غیر مجاز، شنود غیر مجاز، جاسوسی رایانه‌ای؛ چاپ۱، تهران، انتشارات فرهوش،
[۲۱] کنوانسیون جرایم سایبری (بوداپست) ۲۰۰۱ میلادی
[۲۲] مرکز پژوهش‌های مجلس، (۱۳۸۷)؛ اظهار نظر کارشناسی در باره لایحه جرایم رایانه‌ای،
[۲۳] مصدق، محمد؛ (۱۳۹۷)؛ شرح قانون مجازات اسلامی (جرایم، مسئولیت کیفری، ادله اثبات)، جلد۲، چاپ۳، تهران، انتشارات جنگل-جاودانه،
[۲۴] معین، محمد؛ (۱۳۹۱)، فرهنگ فارسی معین، جلد ۵، چاپ ۲۷، تهران، انتشارات امیر کبیر