فصلنامهٔ پژوهش‌های اطلاعاتی و جنایی، سال پانزدهم
شمارهٔ اول، بهار ۱۳۹۹

مطالعهٔ تطبیقی شنود غیرمجاز رایانه‌ای در قوانین کیفری ایران، انگلستان و فرانسه

نوع مقاله: پژوهشی

تاریخ دریافت: ۹۸/۰۶/۲۵ تاریخ پذیرش: ۹۸/۱۰/۰۵

از صفحهٔ ۹ تا ۳۲

زهرا محمدنسل[۱]، غلامرضا محمدنسل[۲]، ایرج گلدوزیان[۳]

چکیده

زمینه و هدف: استفاده از فضای مجازی به سرعت در حال افزایش است. در چنین شرایطی، حفظ حریم خصوصی و محرمانگی داده‌ها و سامانه‌های رایانه‌ای، قانون‌گذاران را وادار به جرم‌انگاری اعمال ناقض آن‌ها کرده است. یکی از این جرائم، شنود غیرمجاز است. هدف این پژوهش، تشریح و تبیین ارکان تشکیل‌دهندهٔ این جرم در حقوق جزای ایران و مقایسهٔ آن با قوانین کشورهای انگلستان و فرانسه است.

روش: تحقیق حاضر، یک تحقیق کیفی با رویکرد تطبیقی است که از نظر هدف، کاربردی و از حیث ابزار تحقیق، اسنادی و کتابخانه‌ای است و اطلاعات گردآوری‌شده شامل قوانین و مقررات کیفری سه کشور مورد مطالعه و همچنین کنوانسیون جرائم سایبری اتحادیهٔ اروپا بوده است که به روش توصیفی- تحلیلی مورد تجزیه و تحلیل قرار گرفته‌اند.

یافته‌ها: یافته‌ها حاکی از آن است که در مورد اوصاف شخص مرتکب، غیرمجاز بودن شنود، غیرعمومی بودن اطلاعات مورد شنود، مقید نبودن این جرم و در حال انتقال بودن ارتباط، همچنین عنصر معنوی جرم در قوانین سه کشور اشتراک نظر وجود دارد. در هر سه کشور، از مجازات حبس و جزای نقدی و محرومیت از حقوق اجتماعی برای سزادهی استفاده می‌شود، اما در قانون کیفری فرانسه ممکن است مراسلات در حال انتقال نباشند، اما دستیابی به آن‌ها شنود تلقی شود و نصب تجهیزات انجام شنود غیرمجاز نیز در حکم شنود است.

نتیجه‌گیری: توجه به تدابیر پیشگیرانه در قوانین انگلستان و تنوع مجازات در قوانین فرانسه از جمله مواردی هستند که برای قانون‌گذار ایران قابل تأسی است.

کلید واژه‌ها: شنود غیرمجاز، قانون جرائم رایانه‌ای ایران، قانون اختیارات تحقیقی انگلستان، قانون جزای فرانسه.

استناد: محمدنسل، زهرا؛ محمدنسل، غلامرضا و گلدوزیان، ایرج (بهار ۱۳۹۹). مطالعهٔ تطبیقی شنود غیرمجاز رایانه‌ای در قوانین کیفری ایران، انگلستان و فرانسه. *فصلنامهٔ پژوهش‌های اطلاعاتی و جنایی*. ۱۵(۵۷)، صص ۳۲-۹.

۱. دانشجوی دکتری حقوق جزا و جرم‌شناسی دانشگاه آزاد اسلامی واحد کرج، z_mnasl@yahoo.com
۲. دانشیار حقوق جزا و جرم‌شناسی دانشگاه علوم انتظامی امین، نویسندهٔ مسئول: g_mnasl@yahoo.com
۳. استاد حقوق جزا و جرم‌شناسی دانشگاه تهران، igoldoz@ut.ac.ir

مقدمه

حریم خصوصی مقولهٔ بسیار مهمی است که همواره حفظ آن موردتوجه بشر بوده است و در بسیاری از اسناد بین‌المللی راجع به حقوق بشر نظیر اعلامیهٔ جهانی حقوق بشر (۱۹۴۸)، کنوانسیون اروپایی حمایت از حقوق بشر و آزادی‌های بنیادین (۱۹۵۰)، میثاق بین‌المللی حقوق مدنی و سیاسی (۱۹۶۶) و اعلامیهٔ اسلامی حقوق بشر (۱۹۹۰) به غیرقابل تعرض بودن آن تصریح شده است. همچنین، امروزه تقریباً همهٔ کشورها حق حریم خصوصی را در قوانین اساسی خود به صورت کلی یا مصداقی مورد شناسایی و حمایت قرار داده‌اند و دست کم به حق غیرقابل تعرض بودن مسکن و خصوصی بودن ارتباطات اشاره کرده‌اند (انصاری، ۱۳۹۰، ص۷). حریم خصوصی ارتباطات و اطلاعات نیز مانند حریم خصوصی جسمانی و منزل از اهمیت بالایی برخوردار است تا آنجا که قانون-گذاران برای نقض حریم خصوصی ارتباطات و افشای اسرار مرتبط با آن اقدام به وضع مجازات کرده‌اند. با گسترش طرق ارتباطی و دستیابی افراد به ارتباطات مخابراتی و اینترنتی، امکان نقض این حریم نیز گسترش یافته و البته مقنن نیز در تکاپوی جرم-انگاری و مجازات آن برآمده است. آخرین قانونی که برای حفظ حریم خصوصی ارتباطات مخابراتی در کشورمان به تصویب رسیده، قانون جرائم رایانه‌ای مصوب ۱۳۸۸ است که در مادهٔ ۲ این قانون (مادهٔ ۷۳۰ ق.م.ا) قانون‌گذار اقدام به تعیین مجازات برای جرم «شنود غیرمجاز»[1] کرده است. حال سؤال این است که قانون‌گذاران کشورهای دیگر چگونه این عمل را جرم انگاری کرده و چه مجازاتی برای آن در نظر گرفته‌اند و آیا قانون‌گذار ایران در این زمینه، قانونی جامع و کامل را تهیه و تصویب کرده است یا بهتر است که با بررسی قوانین سایر کشورها ،در پی اصلاح و بازنگری در قانون جرائم رایانه‌ای فعلی برآمد. برای رسیدن به این نتیجه ضروری بود که از هر نظام حقوقی یک کشور انتخاب و مورد مطالعه قرار گیرد. انگلستان به نمایندگی از کشورهای دارای نظام حقوقی کامن‌لا و فرانسه به نمایندگی از کشورهای واجد نظام حقوقی رومی- ژرمنی انتخاب شدند و پس از برگرداندن قانون این کشورها از انگلیسی به فارسی، اقدام به مقایسهٔ قوانین سه کشور در این زمینه شد.

1.Unlawful Interception

با توجه به افزایش استفاده از رایانه در میان اقشار جامعه و بالأخص استفاده از اینترنت و فضای مجازی و از طرفی به علت مبهم بودن ماهیت جرائم ارتکابی در این فضا برای مردم، به نظر می‌رسد که باید هرچه بیشتر جرائم مرتبط با این فضا معرفی و تشریح شوند. شاید بتوان گفت که افراد جامعه هیچ آشنایی با این جرائم ندارند و ممکن است براثر این عدم آشنایی، خود بزهکار یا بزه‌دیدهٔ این جرائم واقع شوند. یکی از مهم‌ترین این جرائم، جرم شنود غیرمجاز است. از آنجا که از نظر شرعی و اخلاقی حفظ حریم خصوصی افراد همیشه موردتوجه بوده است، اهمیت توجه به این جرم چند برابر می‌شود. در همین راستا، سؤال اصلی تحقیق این است که ارکان متشکله و مجازات شنود غیرمجاز رایانه‌ای در حقوق کیفری کشورهای مورد مطالعه (ایران، انگلستان، فرانسه) کدام‌اند؟ و وجوه تشابه و تفاوت آن‌ها در سه کشور موردمطالعه کدام‌اند؟

در مورد جرم شنود غیرمجاز پس از تفحص در کتب و مقالات، کتاب یا مقاله‌ای که به مطالعهٔ تطبیقی جرم شنود غیرمجاز در قانون ایران و قوانین کشورهای فرانسه و انگلستان پرداخته باشد یافت نشد، اما در بررسی این جرم در حقوق ایران می‌توان به این موارد اشاره کرد. زر رخ (۱۳۸۹)، در مقاله‌ای با عنوان «جرائم مخابراتی»، به شرح جرم شنود غیرمجاز سامانه‌های مخابراتی پرداخته و معتقد است که گسترش دستگاه‌های ارتباطی از قبیل تلفن‌های ثابت و همراه، تلفن‌های اینترنتی و غیره، به توسعهٔ ارتباطات انجامیده است. این امر سبب توسعهٔ جرائم مرتبط با آن‌ها شده و جرم شنود غیرمجاز از آن جمله است. این شیوهٔ تجاوز به محرمانگی داده‌ها، به‌وسیلهٔ سامانه‌های رایانه‌ای و همچنین با سامانه‌های مخابراتی محقق می‌شود. به نظر ایشان، امکان شنود به دو روش وجود دارد؛ روش نخست آن است که نرم‌افزارهای ضبط مکالمات بر روی دستگاه‌های مخابراتی نصب‌شده و آن نرم‌افزارها بدون اطلاع فرد اقدام به ضبط تماس‌های وی کنند. روش دوم این است که شنود مکالمات به‌وسیلهٔ دستگاه‌های مجزایی صورت گیرد که با ورود به فرکانس یا خط مورداستفادهٔ فرد خاص، مکالمات وی را ضبط می‌کنند. هر دو روش را می‌توان با تعریف ذکر شده در قانون جرائم رایانه‌ای منطبق کرد. در خصوص مکالمات اینترنتی نیز این دو شیوه کاربرد دارند. از نظر ایشان، دسترسی به پیامک‌های شخصی را نمی‌توان مشمول عنوان جزایی شنود غیرمجاز دانست، اما با توجه به پیشرفت ابزارهای مخابراتی و توانایی ارسال پیام‌های چندرسانه‌ای، به نظر می‌رسد شنود غیرمجاز پیام‌های چندرسانه‌ای، پیام‌های صوتی در اتاق‌های گفت‌وگو، مکالمات بی‌سیم‌های شخصی و

ارتباطات از راه دور چندرسانه‌ای (مانند ویدیو کنفرانس) را نیز شامل می‌شوند. محمدنسل (۱۳۹۲) نیز در مبحث دوم از فصل نخست کتاب «حقوق جزای اختصاصی جرائم رایانه‌ای در ایران»، پس از بیان ملاحظات کنوانسیون جرائم سایبری در مورد جرم شنود غیرمجاز، مفصلاً به بررسی ارکان قانونی، مادی و معنوی و مجازات جرم شنود غیرمجاز رایانه‌ای در قانون ایران پرداخته است.

بهره‌مند و جلالی فراهانی (۱۳۹۳) در مقالهٔ خود با عنوان «شنود ارتباطات الکترونیک در حقوق کیفری ایران»، معتقدند آنچه درگذشته در پی دریافت غیرمجاز مکالمات تلفنی اشخاص، «استراق سمع» نامیده می‌شد، هم‌اینک گسترهٔ بی‌پایانی از داده‌های رایانه‌ای را در برمی‌گیرد که در بستر مبادلات الکترونیک جریان دارند. گرچه از هنگام به رسمیت یافتن ارتباطات الکترونیک در قوانین داخلی بیش از چهار دهه می‌گذرد، اما حمایت کیفری فراگیر از آن‌ها در برابر تعرضات ناروا، عمری کمتر از شش سال دارد. مقالهٔ حاضر با بررسی عناصر تشکیل‌دهندهٔ جرم شنود و بررسی مستندات قانونی این حوزه با تأکید بر مادهٔ ۷۳۰ قانون مجازات اسلامی، این نتیجه را اخذ می‌کند که مقررات موجود از جامعیت مناسبی برخوردارند، اما در تعیین پاسخ‌های کیفری می‌توان با اصلاحاتی بازدارندگی قوانین را افزایش داد. قربانی‌نژاد کوهستانی (۱۳۹۶) نیز در کتابی با عنوان «جرائم رایانه‌ای علیه محرمانگی داده‌ها؛ دسترسی غیرمجاز، شنود غیرمجاز و جاسوسی رایانه‌ای»، در مبحث دوم از فصل دوم این کتاب، جرم شنود غیرمجاز را در دو گفتار تشریح کرده و به بیان مباحثی مانند ویژگی و ماهیت جرم شنود غیرمجاز (شامل مفهوم شنود و اقسام آن و ماهیت عمومی شنود غیرمجاز)، ارکان شنود غیرمجاز (شامل رکن مادی و رکن روانی) و ارکان قانونی یا ابعاد کیفری شنود غیرمجاز در عرصهٔ فناوری اطلاعات و ارتباطات از دید حقوق کیفری ایران پرداخته است. همچنین، فتاحی (۱۳۹۷) در بخشی از مقالهٔ خود تحت عنوان «بررسی عناصر تشکیل‌دهندهٔ مادی و معنوی مصادیق جرائم رایانه‌ای»، ابتدا به تعریف جرم شنود غیرمجاز رایانه‌ای براساس مادهٔ ۲ قانون جرائم رایانه‌ای (مادهٔ ۷۳۰ ق.م.ا) پرداخته و آن را همان تعرض به حریم ارتباطات به‌وسیلهٔ شنود سنتی و ضبط مکالمات تلفنی افراد بیان می‌کند. ایشان سپس به بیان ارکان و عناصر قانونی و مادی و معنوی این جرم می‌پردازد.

مقالهٔ حاضر پس از بررسی ارکان این جرم در قانون جرائم رایانه‌ای ایران، به بررسی قوانین کشورهای انگلستان و فرانسه در مورد این جرم می‌پردازد تا علاوه بر مطالعهٔ

تطبیقی در مورد این جرم، نقاط ضعف و قوت قانون ایران مورد شناسایی قرار گیرد تا شاید در اصلاحات این قانون بتواند موارد ابهام یا اشکال و سکوت را برطرف کند. از طرفی، تشریح و آشنایی با قانون می‌تواند مقدمهٔ اتخاذ اقدامات پیشگیرانه برای کاهش ارتکاب و بزه‌دیدگی این جرائم شود.

معنا و مفهوم شنود غیرمجاز رایانه‌ای: شنود اسم مصدر از مصدر شنودن به معنی شنیدن و استماع است (دهخدا) و از نظر اصطلاحی به عنوان ورود مخفیانه به یک شبکهٔ ارتباطی، اعم از صوتی یا نوشتاری، بدون ایجاد هرگونه تغییر در محتوا یا اختلال در آن تعریف شده است. معادل انگلیسی این واژه، Interception است. با توجه به اینکه ارتباط اولیه و رایج بین افراد ارتباط صوتی و کلامی بوده است، لذا این عمل بیشتر تحت عنوان «استراق سمع» شناخته شده است که به صورت گوش دادن پنهانی به سخنان دیگران صورت می‌گرفته است. استراق سمع گاهی به سادگی و به وسیلهٔ گوش دادن و اصطلاحاً «فال گوش ایستادن» صورت می‌گیرد، اما در مواردی هم با استفاده از وسایل و تجهیزات و از راه دور صورت می‌گیرد. این عمل به ترتیب، علاوه بر پیام‌های صوتی، سایر ابزارهای ارتباطی را نیز در بر گرفته است.

شنود غیرمجاز در کشورهای مختلف جرم‌انگاری شده بود که با ظهور و گسترش استفاده از رایانه در امور ارتباطی، شنود آن نیز به تدریج پدیدار شد. شنود رایانه‌ای یا شنود ارتباطات[1] نیز همسان شنودهای سنتی به شنود مجاز و شنود غیرمجاز تقسیم می‌شود. شنود مجاز به حکم قانون و توسط مقامات صلاحیت‌دار صورت می‌گیرد، اما شنود غیرمجاز فاقد این ویژگی است. شنود ارتباطات زمانی رخ می‌دهد که ارتباطی خصوصی میان دو یا چند طرف که از طریق سیستم ارتباطی صورت گیرد، برای آشکار شدن محتوای آن، به صورت پنهانی شنود شود. شنود محدود به سیستم ارتباطی خاصی نیست؛ شنود پنهانی پیام‌های ارسالی از طریق شبکه‌های تلفنی، سیستم‌های پستی، ارتباطات از طریق پیجر یا مراسلات بی‌سیم دیگر همگی نمونه‌هایی از شنود هستند (شنود ارتباطات در انگلستان[2]، ۱۹۹۹: ۷). ضبط یا تحت کنترل داشتن مکالمات تلفنی، برنامه‌هایی مانند فیس‌تایم یا ارتباطات ویدیویی نیز شنود محسوب می‌شوند.[3]

1.Interception of Telecommunication Systems
2.INTERCEPTION OF COMMUNICATIONS IN THE UNITED KINGDOM, 1999, P 7
3.www.inbrief.co.uk/offences/electronic-communications-offences/

مادهٔ ۳ کنوانسیون جرائم رایانه‌ای اتحادیهٔ اروپا[1]، اوصاف و ویژگی‌های جرم شنود غیرمجاز رایانه‌ای را به شرح ذکر کرده است:

- شنود به گوش دادن، نظارت یا ملاحظه محتوای ارتباطات اطلاق می‌شود؛
- شنود شامل دستیابی به محتوای داده‌ها چه به‌صورت مستقیم (با دسترسی به رایانه و استفاده از سیستم رایانه‌ای) یا به شکل غیرمستقیم (با استفاده از دستگاه‌های استراق سمع الکترونیکی) می‌شود؛
- شنود می‌تواند شامل ضبط کردن نیز بشود؛
- ابزارهای فنی شنود ممکن است شامل دستگاه‌های فنی متصل به خطوط انتقال یا دستگاه‌های جمع‌آوری و ضبط ارتباطات بی‌سیم شود؛
- موضوع شنود باید ارتباطات غیرعمومی داده‌های رایانه‌ای باشد؛
- شنود می‌تواند در جریان انتقال اطلاعات در درون اجرای یک سامانه (مانند انتقال اطلاعات از واحد پردازشگر به صفحهٔ نمایشگر یا دستگاه چاپگر) یا در جریان انتقال اطلاعات از یک رایانه به رایانه دیگر یا در جریان انتقال اطلاعات در داخل یک شبکه صورت گیرد؛
- امواج الکترومغناطیسی با اینکه داده به مفهوم واقعی آن نیستند، اما چون می‌توان از طریق بازسازی آن‌ها، داده‌ها را به دست آورد، شنود شامل شنود امواج الکترومغناطیسی هم خواهد شد؛
- شنود باید به‌ناحق و به‌طور غیرمجاز صورت گرفته باشد؛
- شنود باید عمدی واقع شده باشد؛

با توجه به موارد فوق، می‌توان شنود غیرمجاز رایانه‌ای را به این شکل تعریف کرد: «شنود غیرمجاز رایانه‌ای عبارت است از گوش دادن و/یا نظارت و/یا ملاحظهٔ محتوای ارتباطات رایانه‌ای در حال انتقال خارج از چارچوب قانون».

روش‌شناسی تحقیق

تحقیق حاضر یک تحقیق کیفی است که از نظر هدف، کاربردی، از حیث ابزار تحقیق، اسنادی و کتابخانه‌ای، از حیث روش تجزیه و تحلیل، توصیفی- تحلیلی و از حیث رویکرد

1.Convention on Cybercrime, 23.XI.2001

مطالعه، از نوع تطبیقی بوده و مبتنی بر استنتاج مؤلفان از منابع و متون است. اطلاعات گردآوری شده شامل قوانین و مقررات کیفری سه کشور ایران و انگلستان و فرانسه و همچنین کنوانسیون جرائم سایبری اتحادیهٔ اروپا در خصوص شنود غیرمجاز رایانه‌ای بوده است. قوانین خارجی پس از جستجو به زبان انگلیسی استخراج و توسط محققان به فارسی ترجمه شده و سپس ارکان و عناصر متشکلهٔ جرم از قوانین موجود استخراج و در نهایت براساس چارچوب تهیه شده، مورد تجزیه و تحلیل قرار گرفته است.

یافته‌های تحقیق

در این بخش از مقاله، به بررسی ارکان تشکیل‌دهندهٔ جرم شنود غیرمجاز (شامل رکن قانونی، رکن مادی و رکن روانی) و نکات مرتبط با هریک و در نهایت مجازات مقرر برای این جرم در قوانین کشورهای مورد مطالعه پرداخته می‌شود.

شنود غیرمجاز در قوانین کیفری ایران

اسلام، استراق سمع و تجسس را حرام اعلام کرده است. در ایران نیز براساس اصل ۲۵ قانون اساسی، استراق سمع یا شنود ممنوع اعلام شده است؛ مگر به موجب قانون. ضمانت اجرای این اصل در مادهٔ ۵۸۲ قانون مجازات اسلامی پیش‌بینی و مقرر شده که هر یک از مستخدمان و مأموران 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 کنند یا بدون اجازهٔ صاحبان آن‌ها، مطالب آن‌ها را افشا کند، به حبس از یک سال تا سه سال یا جزای نقدی از شش تا هجده میلیون ریال محکوم خواهد شد. ملاحظه می‌شود که قانون‌گذار صرفاً استراق سمع توسط مأموران دولتی را جرم تلقی کرده و در مورد استراق سمع توسط افراد عادی سکوت کرده است. در فضای مجازی نیز قانون‌گذار به دنبال حفظ حریم خصوصی اطلاعات افراد است و در همین راستا، اقدام به جرم‌انگاری شنود غیرمجاز رایانه‌ای کرده است.

رکن قانونی شنود غیرمجاز در قوانین کیفری ایران، مادهٔ ۲ قانون جرائم رایانه‌ای مصوب ۱۳۸۸[۱] است. مطابق این ماده، «هرکس به‌طور غیرمجاز، محتوای در حال انتقال

۱. یا همان مادهٔ ۷۳۰ قانون مجازات اسلامی.

ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری را شنود کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون (۱۰/۰۰۰/۰۰۰) ریال تا چهل میلیون (۴۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد».

در خصوص رکن مادی این جرم باید خاطرنشان کرد که مرتکب جرم می‌تواند هرکسی باشد و سمت و قید خاصی برای وی در نظر گرفته نشده است. به نظر می‌رسد که ارتکاب این جرم صرفاً از طریق فعل مادی مثبت قابل‌تصور است و ترک فعل نمی‌تواند رفتار مرتکب این جرم باشد. بنا به‌تصریح متن ماده، موضوع شنود غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی است و اگر محتوا در حال انتقال نباشد و درواقع ذخیره‌شده در رایانه یا حامل‌های داده باشد، باید ذیل عنوان دسترسی غیرمجاز به داده‌های رایانه‌ای که جرم موضوع مادهٔ ۱[۱] قانون مذکور است بررسی شود. اما در ادامهٔ قانون، قانون‌گذار در تبصرهٔ ذیل مادهٔ ۴۸ این قانون[۲]، دسترسی به محتوای ارتباطات غیرعمومی ذخیره‌شده نظیر پست الکترونیکی یا پیامک را در حکم شنود دانسته است. سؤالی که ممکن است مطرح شود این است که آیا دسترسی به محتوای ارتباطات غیرعمومی چه در حال انتقال چه ذخیره‌شده، شنود است و مشمول مادهٔ ۲ قرار می‌گیرد یا اینکه مقنن منظور دیگری داشته است؟ در پاسخ باید گفت که به نظر می‌رسد قانون‌گذار دسترسی مأموران دولتی به سوابق ذخیره شدهٔ غیرعمومی در سامانه‌ها را برای مأموران دولت در حکم شنود تلفن گرفته و اخذ مجوز برای دسترسی به آن اطلاعات را تابع احکام شنود تلفن قرار داده است و منظور قانون‌گذار، تغییر عنوان مجرمانهٔ دسترسی غیرمجاز به داده‌های عمومی به شنود غیرمجاز نبوده است.

مطابق متن ماده، شنود باید غیرمجاز باشد. بنابراین، درصورتی‌که به‌موجب قانون یا اجازهٔ مقام قضایی یا مقامات مسئول صورت گیرد، مشمول جرم شنود قرار نمی‌گیرد. غیرعمومی بودن محتوای ارتباط در سامانه‌های رایانه‌ای یا مخابراتی شرط دیگری است که قانون‌گذار در متن ماده قید کرده است. بنابراین، درصورتی‌که محتوای عمومی ارتباط

---

۱ یا همان مادهٔ ۷۲۹ قانون مجازات اسلامی.

۲ یا همان مادهٔ ۷۷۶ قانون مجازات اسلامی.

رایانه‌ای یا مخابراتی شنود شود، مشمول این ماده نخواهد بود. اما در مورد وجه تمایز و تشخیص ارتباطات عمومی از غیرعمومی، قانون‌گذار هیچ ضابطه‌ای قرار نداده است.
فرقی ندارد که محتوای غیرعمومی رایانه‌ای یا مخابراتی از طریق سیم و کابل در حال انتقال باشد یا به‌صورت بی‌سیم منتقل شود، آنچه اهمیت دارد در حال انتقال بودن آن‌ها است. این جرم از جرائم مطلق است و صرفاً با انجام عمل مادی جرم و بدون نیاز به حصول نتیجه‌ای خاص محقق می‌شود.

در خصوص رکن معنوی شنود غیرمجاز در حقوق کیفری ایران باید گفت که در ایران شنود غیرمجاز از جرائم عمدی است. بنابراین، وجود عمد در شنود در شخص مرتکب ضروری است و چنانچه فردی سهواً یا به‌طور ناخواسته و ندانسته به اطلاعات در حال انتقال دسترسی پیدا کرده و بدون هرگونه اقدام غیرقانونی از سامانه خارج شود، عمل وی مشمول حکم این ماده نخواهد بود. علاوه بر عمد، احراز عنصر علم نیز در مرتکب ضروری است. بنابراین، فرد باید با عمد و علم به غیرمجاز بودن شنود مرتکب این عمل شود. از آنجا که وجود انگیزهٔ خاصی در مرتکب شنود غیرمجاز برای تحقق جرم شرط نشده است، بنابراین مرتکب با هر انگیزه‌ای (اعم از انتقام یا ارضای حس کنجکاوی یا کسب اطلاعات نسبت به اسرار خصوصی افراد و غیره) مرتکب شنود شود، تأثیری در عنوان مجرمانه نخواهد داشت. چون شنود غیرمجاز از جرائم مقید به نتیجه نیست. بنابراین، وجود سوءنیت خاص (قصد حصول نتیجهٔ موردنظر قانون‌گذار) هم در مرتکب ضروری نیست و مرتکب به‌صرف انجام شنود غیرمجاز، مشمول مجازات مقرر خواهد شد.

مجازات عادی اشخاص حقیقی مرتکب این جرم، محکومیت به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون (۱۰/۰۰۰/۰۰۰) ریال تا چهل میلیون (۴۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات حبس و جزای نقدی خواهد بود. در صورتی که مرتکب یا مرتکبان از کارمندان و کارکنان اداره‌ها و سازمان‌ها یا نهادهای دولتی یا وابسته به دولت یا نهادهای عمومی و نیروهای مسلح و قوای سه‌گانه (به‌تفصیل مقرر در مادهٔ ۲۶ قانون جرائم رایانه‌ای[1]) یا از متصدیان یا متصرفان قانونی شبکه‌های رایانه‌ای یا مخابراتی بوده و به سبب شغل خود مرتکب شنود غیرمجاز شده باشند یا اینکه، داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی موضوع شنود غیرمجاز، متعلق به دولت یا نهادها و مراکز

۱. یا همان مادهٔ ۷۵۴ قانون مجازات اسلامی.

ارائه‌دهندهٔ خدمات عمومی بوده باشند، همچنین در صورتی که جرم به‌صورت سازمان‌یافته یا در سطحی گسترده ارتکاب یافته باشد، مجازات مرتکب تشدید شده و مرتکب یا مرتکبان به بیش از دوسوم حداکثر یک یا دو مجازات حبس یا جزای نقدی محکوم خواهند شد.

براساس مادهٔ ۲۷ قانون جرائم رایانه‌ای[۱] و با لحاظ مادهٔ دو قانون مذکور، درصورتی‌که عنوان تکرار جرم رایانه‌ای برای بار سوم در مورد مرتکب یا مرتکبان شنود غیرمجاز مصداق داشته باشد، دادگاه می‌تواند آن‌ها را از خدمات الکترونیکی عمومی از قبیل اشتراک اینترنت، تلفن همراه، اخذ نام دامنهٔ مرتبهٔ بالای کشوری و بانکداری الکترونیکی به مدت یک ماه تا یک سال محروم کند.

چنانچه دادگاه براساس شرایط مندرج در مادهٔ ۱۹ قانون جرائم رایانه‌ای[۲]، شخص حقوقی را نیز در شنود غیرمجاز از نظر کیفری مسئول بشناسد، در آن صورت براساس مادهٔ ۲۰ قانون جرائم رایانه‌ای[۳] و با لحاظ مادهٔ ۲ قانون مذکور، مجازات اشخاص حقوقی مرتکب شنود غیرمجاز برای بار اول، محکومیت به جزای نقدی از یک‌صد و بیست میلیون (۱۲۰/۰۰۰/۰۰۰) ریال تا دویست و چهل میلیون (۲۴۰/۰۰۰/۰۰۰) ریال خواهد بود. علاوه بر آن، براساس بند «الف» مادهٔ ۲۰ و با لحاظ مادهٔ ۲ قانون پیش‌گفته، شخص حقوقی به‌طور موقت از یک تا نه ماه تعطیل خواهد شد. در صورت تکرار جرم، شخص حقوقی علاوه بر جزای نقدی مندرج دربند ۲، به تعطیلی موقت از یک تا پنج سال محکوم خواهد شد.

شنود غیرمجاز در قانون انگلستان

رکن قانونی جرم شنود غیرمجاز رایانه‌ای در انگلستان، بند ۱ مادهٔ ۳ قانون اختیارات تحقیقی[۴] مصوب ۲۰۱۶ است که این قانون شامل تلفن همراه، پیجر و پیام‌های الکترونیکی ارسالی در شبکه‌های رایانه‌ای و این قبیل موارد می‌شود.[۵] براساس بند مذکور: «شخصی مرتکب جرم شده است؛ اگر الف) به‌صورت عمدی، ارتباطی را در زمان انتقال

۱.یا همان مادهٔ ۷۵۵ قانون مجازات اسلامی.

۲.یا همان مادهٔ ۷۴۷ قانون مجازات اسلامی.

۳.یا همان مادهٔ ۷۴۸ قانون مجازات اسلامی.

4.Investigatory Powers Act 2016

5.Regulation of Interception of Communications in Selected Jurisdictions, P 12

آن از طریق یک سیستم ارتباط راه دور عمومی، یک سیستم ارتباط راه دور خصوصی یا یک سرویس پستی عمومی شنود کند. ب) شنود در انگلستان انجام شده باشد و ج) شخص اجازهٔ قانونی برای انجام شنود نداشته باشد».

بندهای ۲ تا ۷ از مادهٔ ۳ و مواد ۴ تا ۸ نیز به بیان موارد مرتبط با جرم شنود غیرمجاز اختصاص یافته‌اند که در ادامهٔ بحث به آن‌ها اشاره خواهد شد. با توجه به متن قانونی اشاره شده، ارکان مادی و روانی این جرم در حقوق کیفری انگلستان به این قرار هستند؛ مرتکب این جرم هرکسی می‌تواند باشد و وصف خاصی برای وی شرط نشده است. مطابق بند ۲ مادهٔ ۴، رفتار تشکیل‌دهندهٔ جرم شنود عبارت است از تغییر یا دخالت در سیستم مخابراتی یا عملکرد آن که منجر به شنود محتوای ارتباط شود، یا نظارت بر انتقالاتی که توسط سیستم مخابراتی انجام می‌شود و منجر به شنود محتوای آن شود، یا نظارت بر انتقالاتی که توسط سیستم تلگرافی بی‌سیم به دستگاه متصل به سیستم مخابراتی یا برعکس انجام می‌شود. به نظر می‌رسد همهٔ این اعمال تنها از طریق فعل مثبت مادی قابل ارتکاب هستند و ترک فعل نمی‌تواند عنصر مادی جرم شنود غیرمجاز مخابراتی یا رایانه‌ای باشد.

براساس بند «۳» از مادهٔ ۴ قانون موصوف، قانون‌گذار انگلستان تغییر سیستم مخابراتی را شامل متصل کردن هر دستگاهی به سیستم مخابراتی یا تغییر یا دخالت در هر قسمتی از سیستم مخابراتی یا دستگاه تلگرافی بی‌سیم می‌داند که برای انتقال اطلاعات از سیستم مخابراتی یا به آن، استفاده می‌شود. مطابق بند ۱ مادهٔ ۴ از قانون اختیارات تحقیقی مصوب ۲۰۱۶، شرط جرم بودن عمل شنود در سیستم مخابراتی این است که شخص، رفتار شنود را در ارتباط با سیستم مخابراتی انجام دهد. بنابراین، اگر شنود مرتبط با سیستم مخابراتی نباشد، مشمول این قانون نمی‌شود.

مطابق بند ۲ از مادهٔ ۲۶۱ این قانون، ارتباط در اپراتور مخابراتی، سرویس مخابراتی یا سیستم مخابراتی به معانی زیر است: هر چیزی که شامل گفتار، موسیقی، صدا، تصاویر دیداری یا اطلاعات مرتبط باشد و سیگنال‌هایی که برای انتقال هر چیز بین اشخاص، بین یک شخص و یک شیء یا بین اشیاء یا برای راه‌اندازی یا کنترل هر وسیله‌ای بکار می‌رود. تعریف محتوا نیز در بند ۶ مادهٔ ۲۶۱ قانون پیش‌گفته، چنین آمده است: در ارتباط و اپراتوری مخابراتی (سرویس مخابراتی یا سیستم مخابراتی)، محتوا به معنای هر عنصری از ارتباط یا هر اطلاعات پیوست شده یا به‌طور منطقی ملازم با ارتباط یا هر چیزی است

که به‌صورت معقول موجب افشای معنای ارتباط شود. اما معانی برگرفته از ارتباط یا اطلاعات مرتبط با انتقال ارتباط یا اطلاعات سیستم، محتوا تلقی نمی‌شوند. افشای محتوای ارتباط باید برای شخص یا اشخاصی باشد که فرستنده یا گیرندهٔ ارتباط مذکور نیستند. بنابراین، شخصی که محتوای ارتباط برای وی افشا می‌شود، ممکن است شخصی غیر از مرتکب شنود باشد. در هر حال چه شخصی که شنود می‌کند و چه شخصی که محتوا برای وی افشا می‌شود، باید اشخاصی غیر از فرستنده و گیرندهٔ آن ارتباط باشند.

ارتباط باید در حال انتقال باشد. این شرط در بند ۱ از مادهٔ ۴ قانون مذکور آمده است. بنابراین، در قانون انگلستان شرط در حال انتقال بودن از عناصر مهم جرم شنود رایانه‌ای است و اگر محتوایی در حال انتقال نباشد، دسترسی به آن تحت عنوان شنود غیرمجاز رایانه‌ای قرار نمی‌گیرد، اما ممکن است محتوا در زمان انتقال ذخیره و بعداً آشکار شود که باز هم شرط در حال انتقال بودن وجود خواهد داشت و این عمل نیز مشمول شنود غیرمجاز قرار می‌گیرد. دربند ۵ از مادهٔ ۴ این قانون، مواردی که در آن محتوایی از یک ارتباط برخط استخراج می‌شود تا بعداً در دسترس شخصی دیگر قرار گیرد مورد بحث قرار گرفته است.

شنود باید غیرمجاز باشد. بنابراین، درصورتی‌که شخص اجازهٔ شنود داشته باشد و درواقع شنود مجاز و قانونی باشد، این جرم محقق نمی‌شود. قانون‌گذار در مادهٔ ۶ این قانون مواردی را که شنود مجاز تلقی می‌شود را به این ترتیب آورده است: ابتدای مادهٔ ۲، فرض را قانون‌گذار از یکدیگر جدا کرده و سپس به تعیین شنود قانونی در هریک از موارد می‌پردازد. اول اینکه شنود در زمان انتقال ارتباط صورت گیرد که در سه صورت این شنود مجاز خواهد بود: ۱- شنود در راستای حکم شنود موردی صورت گرفته باشد، ۲- شنود در راستای حکم شنود انبوه صورت گرفته باشد (اشخاص معدودی اجازهٔ درخواست حکم شنود را دارند)[1]، ۳- به‌موجب مادهٔ ۴۴ از همین قانون، فرستنده یا گیرندهٔ ارتباط اجازهٔ شنود را داده باشند. دوم اینکه ارتباط توسط یا در سیستم مخابراتی ذخیره شده باشد و بعد شنود صورت گیرد که در صورت وجود یکی از این شروط، شنود مجاز خواهد بود: با حکم شنود موردی یا حکم شنود انبوه انجام شده باشد؛ در زمان اجرا

---

۱. برای فهرست افرادی که این اجازه را دارند ر. ک به:

Interception of Communications Code of Practice, Pursuant to section 71 of the Regulation of Investigatory Powers Act 2000, p6.

توسط هر مقام قانونی با هدف دستیابی به اطلاعات یا تسلط به هر مدرک یا اموال دیگری صورت بگیرد و در راستای حکم دادگاه مبنی بر شنود صورت گرفته باشد.

مطابق فصل نخست از بخش دوم این قانون (مادهٔ ۱۵)، مواردی که شنود ارتباطات قانونی است، عبارت است از حکم شنود موردی، حکم معاینهٔ موردی، حکم مساعدت متقابل و همان‌گونه که اشاره شد اشخاصی که اجازهٔ درخواست شنود را دارند، در آیین‌نامهٔ قانون اختیارات تحقیقی احصا شده‌اند که البته تمامی احکام شنود مجاز باید به امضای وزیر امور خارجه برسند. صدور این حکم توسط وزیر امور خارجه صرفاً نشانگر این است که شنود هیچ‌یک از حقوق فردی (حق محترم شمردن زندگی خانوادگی و خصوصی) مندرج در مادهٔ ۸ از کنوانسیون اروپایی حقوق بشر را نقض نمی‌کند. البته مواردی که در آن نقض این حقوق صورت گرفته است نیز وجود دارند؛ به‌طور مثال به گزارش گاردین که در تاریخ ۶ فوریهٔ ۲۰۱۵ منتشر شده است، دیوان اختیارات تحقیقی که IPT خوانده می‌شود، اعلام کرده است که مقررات ناظر بر دسترسی دفتر ارتباطات دولت انگلستان به ایمیل‌ها و مکالمات تلفنی ضبط شده که توسط آژانس امنیت ملی امریکا شنود شده بودند، مواد ۶ و ۸ قانون حقوق بشر را نقض کرده است[1] یا محاکمه‌ای که دادگاه اروپایی حقوق بشر در سال ۲۰۱ در مورد سه پروندهٔ تلفیقی متعلق به برنامهٔ شنود توده‌ای دولت انگلستان انجام داد که این مورد اولین بار توسط ادوارد اسنودن در سال ۲۰۱۳ مطرح شد و دادگاه کمبودهای قابل‌توجهی را در چارچوب قانون حاکم بر شنود توده‌ای یافته و اعلام کرد که مواد ۸ و ۱۰ کنوانسیون اروپایی حقوق بشر را که مرتبط با حقوق خصوصی و آزادی بیان است، نقض شده‌اند.[2] بنابراین، علاوه بر احراز این مورد، باید ضرورت شنود نیز احراز شود؛ یعنی باید یکی از این منافع وجود داشته باشد: منافع مرتبط با امنیت ملی، پیشگیری یا کشف جرم مهم و حفاظت از منافع اقتصادی انگلستان که این منافع مرتبط با امنیت ملی نیز باشند که این موارد در مادهٔ ۲۲ از فصل ۲ آیین‌نامهٔ قانون اختیارات تحقیقی اصلاحیهٔ ۲۰۱۹ ذکر شده‌اند.[3]

شرط دیگری که در قانون انگلستان برای جرم بودن عمل شنود غیرمجاز آمده است، تکوین آن در قلمرو انگلستان است. بند ۸ از مادهٔ ۴ همین قانون، مواردی را که شنود در

1.UK-US surveillance regime was unlawful ‘for seven years’.
2.New U.K. Law Fails European Court Standards on Mass Interception Disclosed by Snowden
3.Ibid, p 8.

انگلستان انجام می‌یابد را چنین آورده است: در راستای اهداف این قانون، شنود یک ارتباط انجام یافته در انگلستان تلقی می‌شود، اگر و تنها درصورتی‌که رفتار مرتبط یا شنود در انگلستان انجام شده باشد و ارتباط شنود شده باشد؛ در زمان انتقال آن توسط سیستم مخابراتی عمومی یا در زمان انتقال آن توسط سیستم مخابراتی خصوصی درصورتی‌که فرستنده یا گیرندهٔ موردنظر ارتباط، در انگلستان باشد.

از نظر قانون‌گذار بریتانیا فرقی ندارد که شنود از طریق سیستم مخابراتی عمومی صورت گیرد یا خصوصی. در هر دو حالت، شنود محقق می‌شود و تعریف سامانه‌های مخابراتی عمومی و خصوصی نیز در همین قانون آمده‌اند. همان‌گونه که گفته شد، شنود می‌تواند هم از طریق سیستم مخابراتی عمومی صورت پذیرد و هم خصوصی، اما درصورتی‌که از طریق سیستم مخابراتی خصوصی صورت گیرد، اگر شخصی که اقدام به شنود می‌کند، کسی باشد که اجازهٔ کنترل عملکرد یا اجازهٔ استفاده از سیستم را داشته باشد یا شخصی است که به‌صورت صریح یا ضمنی اجازهٔ شنود را از شخص کنترل‌کنندهٔ سیستم یا استفاده‌کننده از آن داشته باشد، جرم بند ۱ فوق‌الذکر محقق نمی‌شود. بنابراین، اولاً درصورتی‌که شخص کنترل‌کنندهٔ سیستم مخابراتی یا استفاده‌کنندهٔ از آن اقدام به شنود کند، جرم شنود غیرمجاز محقق نمی‌شود، ثانیاً درصورتی‌که چنین شخصی به دیگری اجازهٔ صریح یا ضمنی شنود را بدهد نیز جرم شنود نسبت به هیچ‌یک محقق نمی‌شود.

مطابق بند ۸ مادهٔ ۲۶۱ از این قانون، سرویس مخابراتی عمومی به معنی هر سرویس مخابراتی است که برای عموم مردم یا بخش قابل‌توجهی از آن‌ها در یک یا چند قسمت از انگلستان فراهم شده است. دربند ۹ از همین ماده، سیستم مخابراتی عمومی به معنی سیستم مخابراتی عمومی است که در انگلستان مستقر است که از طریق آن سرویس مخابراتی عمومی فراهم می‌شود یا از قسمت‌هایی از سیستم مخابراتی که چنین سرویسی را فراهم می‌کند، تشکیل شده باشد. دربند ۱۴ از این ماده، سیستم مخابراتی خصوصی به معنی هر سیستم مخابراتی است که سیستم مخابراتی عمومی نباشد، به‌صورت مستقیم یا غیرمستقیم به یک سیستم مخابراتی عمومی متصل باشد و شامل دستگاهی می‌شود که هم در انگلستان واقع شده است و هم در آنجا برای اتصال به آن سیستم مخابراتی عمومی (همراه یا بدون دستگاهی دیگر) استفاده می‌شود.

در حقوق کیفری بریتانیا برای تکوین جرم شنود غیرمجاز باید محتوای ارتباط، محتوای غیرعمومی باشد و همان‌گونه که دربند ۱ مادهٔ ۵ از قانون انگلستان آمده است، شنود ارتباطی که برای مخاطبان عمومی انتشاریافته است، مشمول عنوان مجرمانهٔ شنود غیرمجاز قرار نمی‌گیرد. در بریتانیا نیز این جرم از جرائم مطلق است و صرف شنود برای تکوین این جرم کفایت می‌کند و نیازی نیست که پس از آن منتج به نتیجهٔ خاص دیگری شود. در این کشور نیز این جرم از جرائم عمدی است. در بند ۱ مادهٔ ۳، شرط جرم بودن این عمل، داشتن عمد در شنود است. بنابراین، درصورتی‌که عمد در شنود وجود نداشته باشد، عمل مشمول جرم شنود غیرمجاز قرار نخواهد گرفت. عمد نیز شامل علم و اراده می‌شود. اگر ارادهٔ ارتکاب وجود نداشته باشد که ضمانت اجرا منتفی است و درصورتی‌که علم به غیرمجاز بودن عمل وجود نداشته باشد، ممکن است ضمانت اجرایی برای این عمل همان‌گونه که گفته خواهد شد وجود داشته باشد. بنابراین، در انگلستان تحقق این جرم نیاز به تکوین نتیجهٔ خاصی ندارد و نیازی به احراز سوءنیت خاص در مرتکب نخواهد بود. قانون‌گذار انگلستان نیز وجود انگیزهٔ خاصی در مرتکب را برای تحقق این جرم شرط ندانسته است.

مجازات مقرر برای جرم شنود غیرمجاز در انگلستان با توجه به نوع رسیدگی متفاوت است؛ اگر رسیدگی بدون حضور هیئت‌منصفه صورت گیرد، مجازات مقرر جزای نقدی خواهد بود، اما اگر رسیدگی با حضور هیئت‌منصفه صورت گیرد، مجازات می‌تواند حبس تا دو سال یا جزای نقدی یا هردوی آن‌ها باشد. برای اقدام به تحقیق و تعقیب در مورد جرم شنود غیرمجاز، مطابق بند ۷ مادهٔ ۳، باید مدیر تعقیبات عمومی، اجازهٔ اقدام دهد، در غیر این صورت، امکان اقدام وجود نخواهد داشت.

قانون‌گذار انگلستان در این قانون علاوه بر تعریف جرم شنود غیرمجاز و تعیین شرایط آن در بند ۱ مادهٔ ۳ و پیش‌بینی مجازات برای این جرم در بند ۶ از همین ماده، مادهٔ ۷ را در ۸ بند اختصاص به مواردی داده است که یکی از شروط جرم شنود غیرمجاز مذکور در مادهٔ ۳ وجود نداشته باشد. بنابراین، درصورتی‌که هر یک از شروط مادهٔ ۳ از این قانون وجود نداشته باشند، اعمال مجازات منتفی است، اما ممکن است شخص مشمول مادهٔ ۷ شود. به‌طور مثال، یکی از شرایط مذکور در مادهٔ ۳، داشتن عمد در ارتکاب جرم شنود غیرمجاز است و درصورتی‌که عمد در ارتکاب وجود نداشته باشد، بالطبع محاکمه توسط دادگاه نیز منتفی است. اما مطابق این ماده، کمیته‌ای تحت عنوان کمیتهٔ اختیارات

تحقیقی می‌تواند فرد مرتکب را به پرداخت جزای نقدی که شرایط آن در ادامه ارائه خواهد شد، محکوم کند. همان‌گونه که در متن ماده آمده است، برای شمول این ماده باید حتماً دو شرط در عمل فرد وجود داشته باشد: شرط اول این است که کمیته معتقد باشد که: الف) شخص در انگلستان، ارتباطی را در زمان انتقال آن توسط سیستم راه دور عمومی شنود کرده است، ب) شخص اجازهٔ قانونی برای انجام شنود نداشته است و ج) شخص در زمان شنود، در تلاش برای رفتار مطابق حکم شنود نبوده باشد. شرط دوم این است که کمیته احراز نکند که شخص مرتکب جرم ذیل بند ۱ از مادهٔ ۳ شده است. بنابراین، هرگاه شروطی که در بخش عنصر مادی ذکر شد، وجود نداشته باشند و شرط اول نیز فراهم باشد، کمیته پس از احراز این موارد، حکم به پرداخت جریمهٔ نقدی را صادر می‌کند که میزان آن مطابق بند ۵ از مادهٔ ۷ نباید از ۵۰/۰۰۰ یورو تجاوز کند.

شنود غیرمجاز در قانون فرانسه

رکن قانونی جرم شنود غیرمجاز در فرانسه، قسمت دوم مادهٔ ۱۵-۲۲۶ از قانون جزای این کشور است که در سال ۲۰۰۲ لازم‌الاجرا شده است، قانون‌گذار این ماده را ذیل بخش چهارم (نقض محرمانگی) از فصل ششم این قانون تحت عنوان جرائم علیه شخصیت معنوی آورده است و مقرر می‌دارد: «باز کردن، تخریب، به تأخیر انداختن یا منحرف کردن مراسلاتی که به شخص ثالث ارسال می‌شوند از روی سوءنیت، چه به مقصد خود برسد یا نرسد یا به دست آوردن متقلبانهٔ اطلاعاتی از آن، با یک سال حبس و ۴۵۰۰۰ یورو جزای نقدی مجازات می‌شود. همین مجازات در مورد شنود، منحرف کردن، استفاده یا افشای مراسلات ارسالی، انتقالی یا دریافتی توسط مخابرات یا نصب وسیله‌ای که برای تهیهٔ چنین شنودهایی طراحی شده است، از روی سوءنیت، اعمال می‌شوند».

براساس مادهٔ فوق، ارکان مادی و معنوی شنود غیرمجاز یارانه‌ای در «قانون جزای فرانسه»[1] به این قرار هستند: از نظر مقنن فرانسوی، این جرم می‌تواند توسط هرکسی ارتکاب یابد و قانون‌گذار وصف خاصی را برای مرتکب قائل نشده است. عمل مادی مرتکب این جرم عبارت است از شنود مراسلات ارسالی از طریق سیستم مخابراتی در جریان ارسال، انتقال یا دریافت آن‌ها. به نظر می‌رسد که این اعمال تنها از طریق فعل قابل ارتکاب هستند و شنود مراسلات از طریق ترک فعل ممکن نخواهد بود. عمل

1.France Penal Code, 2002

دیگری که در این ماده جرم‌انگاری شده است و در حکم شنود می‌باشد، نصب تجهیزاتی است که برای انجام شنود صورت می‌گیرد. این عمل در صورتی که در این ماده گنجانده نشده بود، می‌توانست تحت عنوان شروع به جرم شنود تحت تعقیب قرار گیرد، اما در این ماده، قانون‌گذار فرانسه پا را فراتر نهاده و این عمل را در حکم شنود دانسته است. بنابراین، حتی درصورتی‌که فرد پس از نصب تجهیزات موفق به شنود نشود نیز جرم تام صورت گرفته است و قابل مجازات است.

قانون‌گذار در این ماده، شنود مراسلات در حال ارسال، انتقال یا دریافت را جرم‌انگاری کرده است. آنچه از متن ماده به دست می‌آید این است که به نظر می‌رسد علاوه بر مراسلاتی که در حال انتقال از طریق سیستم مخابراتی هستند، آن‌هایی که از این طریق ارسال یا دریافت شده باشند نیز مشمول ماده می‌شوند؛ هرچند که در حال انتقال نباشند و شرط مهم این است که زمانی از طریق سیستم مخابراتی منتقل شده باشند که این زمان می‌تواند همان زمان شنود یا قبل از آن باشد. برای تقویت این نظر می‌توان به این نکته‌ای اشاره کرد که در فهرست اعمالی که در قسمت دوم این ماده آورده شده‌اند، علاوه بر شنود، منحرف کردن، استفاده یا افشای مراسلات ارسالی، در حال انتقال یا دریافتی از طریق سیستم مخابراتی نیز جرم‌انگاری شده‌اند. به نظر می‌رسد که افشای این مراسلات در اکثریت موارد پس از انتقال آن‌ها صورت می‌گیرد تا در زمان انتقال.

شنود مربوط به زمانی است که فرد از داده‌های مخابراتی یا اینترنتی مطلع می‌شود و با استراق سمع تفاوت دارد. به همین دلیل است که قانون‌گذار فرانسه در مادهٔ ۱-۲۲۶، ذیل بخش اول از فصل ششم تحت عنوان جرائم علیه حریم شخصی، استراق سمع کلمات در حال انتقال در فضای خصوصی بدون رضایت گوینده را جرم‌انگاری کرده است. شنود باید غیرمجاز باشد. در این ماده شرط جرم بودن شنود، ارتکاب آن از روی تقلب و مجرمانه بودن قصد ارتکاب آن دانسته شده است. بنابراین، درصورتی‌که شنود مجاز باشد، وصف مجرمانه نخواهد داشت. قانون آیین دادرسی کیفری فرانسه مقرر می‌کند، برای رسیدگی به جرائم و تخلفات، درصورتی‌که مجازات مقرر تحمل حداقل دو سال حبس باشد، قاضی تحقیق می‌تواند در صورت ضرورت برای انجام تحقیقات اجازهٔ انجام شنود، رهگیری، ضبط و رونویسی ارتباطات از راه دور ارسالی را بدهد. مطابق مادهٔ ۱۰۰ قانون آیین دادرسی کیفری فرانسه، تصمیم قاضی باید کتبی باشد و حداکثر برای مدت ۴ ماه صادر شود (و یک‌بار قابل تجدید در همان شرایط فرم و مدت زمان است). مادهٔ ۹۵-۷۰۶

از آیین دادرسی کیفری فرانسه مقرر می‌کند، به عنوان بخشی از تحقیقات مربوط به جرم و جنایات سازمان‌یافته و بزهکاری، دادستان‌های عمومی می‌توانند از قاضی مسئول آزادی و توقیف درخواست اجازهٔ شنود، ضبط و رونویسی مراسلات از راه دور را در راستای مادهٔ ۱۰۰ فوق‌الذکر بکنند. شنود فقط برای حداکثر پانزده روز ممکن است و برای یک‌بار قابل تجدید در همان شرایط فرم و مدت زمان است که این تصمیم قاضی باید کتبی باشد.[1]

در این ماده فرقی میان داده‌های عمومی و غیرعمومی وجود ندارد، اما آنچه به نظر می‌آید این است که در هر حال باید مراسلات محرمانه باشند و این شرط را قانون‌گذار در همین قانون قبل از بیان مادهٔ ۱۵-۲۲۶ به‌صورت تیتر قرار داده است؛ محرمانه بودن مراسلات به این معنی است که دسترسی به آن‌ها برای عموم آزاد نباشد.

این جرم از جرائم مطلق است. بنابراین، به‌محض شنود یا نصب تجهیزات برای شنود، این جرم به‌صورت تمام و کمال واقع شده است و نیازمند نتیجهٔ خاصی نیست. در قانون جزای فرانسه نیز جرم شنود غیرمجاز رایانه‌ای از جرائم عمدی است. قید «از روی تقلب» در مادهٔ فوق نیز بیانگر این است که فرد باید به‌صورت عمدی مرتکب این جرم شده باشد. بنابراین، علاوه بر ارادهٔ ارتکاب، باید نسبت به محرمانه بودن و تعلق مراسلات به دیگری نیز اطلاع داشته باشد. بنابراین، درصورتی‌که شخص به‌صورت ناخواسته به این مراسلات دسترسی یابد، مرتکب جرم این ماده نشده است.

وجود انگیزهٔ خاصی در مرتکب این جرم شرط نشده است. بنابراین، مرتکب با هر انگیزه‌ای مرتکب شنود شود یا تجهیزات شنود را نصب کند، این جرم تکوین می‌یابد. همان‌طور که گفته شد، این جرم از جرائم مطلق است، بنابراین وجود قصد نتیجه در مرتکب جرم منتفی است.

مجازات پیش‌بینی‌شده برای اشخاص حقیقی مرتکب شنود غیرمجاز رایانه‌ای یک سال حبس و ۴۵۰۰۰ یورو جزای نقدی است. در مادهٔ ۹-۴۳۲ از همین قانون، قانون‌گذار با توجه به سمت مرتکب جرم، اقدام به تشدید مجازات وی کرده است. بدین‌صورت که اگر مرتکب از مقامات رسمی یا افرادی باشد که فراهم‌کنندهٔ سرویس‌های مخابراتی هستند و در راستای انجام‌وظیفه‌اش مرتکب این جرم شود، مجازات وی ۳ سال حبس و ۴۵۰۰۰ یورو جزای نقدی خواهد بود. علاوه بر افزایش مجازات این افراد، در مادهٔ ۹-۴۳۲،

1.Provision of Real-time Lawful Interception Assistance

قانون‌گذار تسهیل ارتکاب و دستور ارتکاب شنود غیرمجاز توسط این اشخاص را در حکم شنود دانسته و مجازات این جرم را بر این اشخاص اعمال می‌کند. این خود نوع دیگری از تشدید در قالب جرم‌انگاری مستقل اعمالی است که در حالت عادی معاونت محسوب می‌شوند. بنابراین، تسهیل ارتکاب یا دستور ارتکاب جرم شنود برای اشخاص عادی، مصداق معاونت در جرم است، اما در مورد اشخاص مذکور در مادهٔ ۹-۴۳۲ جرمی مستقل خواهد بود.

مطابق مادهٔ ۲-۱۲۱ قانون جزای فرانسه، اشخاص حقوقی نیز با وجود شروطی که در این ماده مقرر شده، دارای مسئولیت کیفری هستند و می‌توانند مورد مجازات قرار گیرند. در مادهٔ ۳۷-۱۳۱ این قانون، مجازات جزای نقدی برای اشخاص حقوقی پیش‌بینی شده است که میزان این جزای نقدی مطابق مادهٔ ۳۸-۱۳۱ می‌تواند تا حداکثر ۵ برابر جزای نقدی مقرر برای اشخاص حقیقی باشد. علاوه بر این مجازات، در مادهٔ ۳۹-۱۳۱ مجازات‌های دیگری نیز برای اشخاص حقوقی در نظر گرفته شده است که برای جلوگیری از اطالهٔ مطلب از علاقه‌مندان درخواست می‌شود که در صورت علاقه به این ماده مراجعه کنند.

بحث و نتیجه‌گیری

هدف از انجام این تحقیق، مقایسهٔ ارکان متشکله و همچنین مجازات شنود غیرمجاز رایانه‌ای در قوانین کشورهای ایران و انگلستان و فرانسه بود. تحقیقات قبلی انجام شده در قانون جرائم رایانه‌ای ایران فاقد وصف مطالعهٔ تطبیقی بود. به همین دلیل، یافته‌های آن‌ها فقط در خصوص قوانین ایران با تحقیق حاضر اشتراک وجه دارند. به ترتیب نتایج مقایسهٔ عنصر قانونی، عنصر مادی و عنصر معنوی و مجازات ارائه می‌شود.

عنصر قانونی جرم شنود غیرمجاز در کشورهای مورد مطالعه شامل مادهٔ ۲ قانون جرائم رایانه‌ای ایران مصوب ۱۳۸۸، بند ۱ مادهٔ ۳ «قانون اختیارات تحقیقی انگلستان»[1] مصوب ۲۰۱۶ و قسمت دوم مادهٔ ۱۵-۲۲۶ از قانون جزای فرانسه الحاقی ۲۰۰۲ است. در مورد قانون ایران لازم به ذکر است که در متن مادهٔ ۲ این قانون، قانون‌گذار شنود غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی

1.Investigatory Powers Act, 2016

یا امواج الکترومغناطیسی یا نوری را جرم انگاری کرده است و درواقع به ذکر تمامی مصادیقی که ارتباط مخابراتی تلقی می‌شوند، پرداخته است. اما در قوانین انگلستان و فرانسه به ذکر ارتباطات مخابراتی بسنده شده است و درواقع در قانون ایران قانون‌گذار با ذکر مصادیق، راه را برای هرگونه ابهامی در مورد شمول یا عدم شمول این قانون بر ارتباط بسته است و هر ارتباطی که از طریق مخابرات و سیستم مخابراتی از قبیل اینترنت صورت گیرد، می‌تواند موضوع این جرم باشد.

در خصوص عنصر مادی در بیان نقاط تفاوت و تشابه این سه قانون، باید به چند مورد توجه کرد:

- براساس قوانین هر سه کشور مورد مطالعه، مرتکب جرم می‌تواند هرکسی باشد و وجود سمتی خاص در وی شرط نشده است؛

- رفتار مرتکب در جرم شنود غیرمجاز مطابق قانون ایران عبارت است از شنود غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری. این رفتار در قانون انگلستان مطابق بند ۲ مادهٔ ۴، در سه قسمت تعیین شده است: ۱- تغییر یا دخالت در سیستم مخابراتی یا عملکرد آن که منجر به شنود محتوای آن ارتباط شود یا ۲- نظارت بر انتقالاتی که توسط سیستم مخابراتی انجام می‌شود و منجر به شنود محتوای آن شود یا ۳- نظارت بر انتقالاتی که توسط سیستم تلگرافی بی‌سیم به دستگاه متصل به سیستم مخابراتی یا برعکس انجام می‌شود. در قانون فرانسه نیز رفتار مرتکب جرم شنود چنین توصیف شده است: شنود، منحرف کردن، استفاده یا افشای مراسلات ارسالی، انتقالی یا دریافتی توسط مخابرات یا نصب وسیلهٔ طراحی شده برای انجام چنین شنودهایی از روی سوءنیت است. بنابراین، در قانون فرانسه، علاوه بر عمل شنود غیرمجاز ارتباطات، قانون‌گذار این کشور اقدام به جرم‌انگاری مستقل عملی که می‌تواند مقدمهٔ ارتکاب این جرم باشد نیز پرداخته است. به این صورت که در صورت نصب تجهیزاتی که برای عمل شنود طراحی شده‌اند، جرم شنود واقع می‌شود؛ چه در عمل از این تجهیزات استفاده شده و شنود واقع شود و چه واقع نشود؛

- در قوانین هر سه کشور مورد مطالعه، برای جرم بودن شنود لازم است که غیرمجاز بودن آن احراز شود. البته در قوانین انگلستان و فرانسه موارد شنود مجاز و قانونی به صورت روشن و با ذکر حتی مواعد قانونی بودن شنود پیش‌بینی شده است. اما در مورد

قانون ایران تصریحی در این زمینه وجود ندارد و به نظر می‌رسد که برای رفع ابهامات و تعیین حدود و ثغور آن باید قانون‌گذار به صورت شفاف، موارد قانونی و مجاز بودن شنود را به تصویب برساند؛

- مطابق قوانین ایران و انگلستان، برای تحقق شنود غیرمجاز رایانه‌ای، محتوای مورد شنود باید در حال انتقال باشد. بنابراین، درصورتی‌که محتوا در حال انتقال نبوده، بلکه ذخیره‌شده در سیستم رایانه‌ای یا مخابراتی باشد، ممکن است با احراز سایر شرایط بتوان این عمل را ذیل عنوان مجرمانهٔ دسترسی غیرمجاز قرار داد. اما در قانون فرانسه، در متن مادهٔ مربوطه، محتوای در حال انتقال، فرستاده یا دریافت شده را موضوع شنود غیرمجاز قرار داده است و از این عبارت چنین نتیجه می‌توان گرفت که وصف در حال انتقال بودن مدنظر قانون‌گذار فرانسه نبوده است، بلکه ممکن است محتوا قبلاً توسط سیستم مخابراتی انتقال‌یافته باشد، اما در زمان ارتکاب عمل شنود در حال انتقال نباشد و در هر دو صورت، جرم شنود غیرمجاز محقق می‌شود؛

- در قوانین هر سه کشور مورد مطالعه برای تحقق جرم شنود غیرمجاز رایانه‌ای، وصف «غیرعمومی بودن» برای محتوای موضوع جرم پیش‌بینی‌شده است؛

- در قوانین هر سه کشور مورد مطالعه، جرم شنود غیرمجاز محتوای در حال انتقال سامانه‌های مخابراتی، جرمی مطلق محسوب شده و صرف شنود برای تکوین این جرم کافی است و در صورت ارتکاب جرائم دیگر، مورد از موارد تعدد جرم خواهد بود؛

- در مورد عنصر معنوی، قانون‌گذاران هر سه کشور جرم شنود غیرمجاز رایانه‌ای را از جرائم عمدی دانسته و وجود عناصر سوءنیت عام را لازم دانسته‌اند. اما از آنجا که جرم در هر سه قانون، جرمی مطلق است، وجود سوءنیت خاص در شخص مرتکب منتفی است. بنابراین، صرف علم به غیرمجاز بودن شنود و ارادهٔ ارتکاب، برای تکوین عنصر معنوی کفایت می‌کند؛

- در مورد مجازات مقرر در قوانین سه کشور مورد مطالعه برای شنود غیرمجاز، نکتهٔ اولی که به ذهن می‌رسد مقایسهٔ نوع مجازات‌های مقرر در این جرائم است. در هر سه قانون، مجازات‌های حبس و جزای نقدی برای مرتکبان در نظر گرفته شده است که البته امکان اعمال هر دو مجازات در هر سه قانون پیش‌بینی شده است. نکتهٔ دومی که با مراجعه به قوانین این سه کشور به دست می‌آید، این است که امکان مجازات اشخاص حقوقی نیز وجود دارد و درواقع ممکن است علاوه بر شخص حقیقی مرتکب جرم، شخص حقوقی

نیز مجازات شود.

تشکر و قدردانی

در پایان، از سردبیر و اعضای هیئت تحریریه، داوران و مدیر اجرایی و ویراستاران محترم فصلنامه که کمال همکاری و راهنمایی در تنظیم نهایی این مقاله را داشتند، کمال تشکر و امتنان را داریم.

منابع

منابع فارسی

- انصاری، باقر (۱۳۹۰). *حقوق حریم خصوصی*. تهران: انتشارات سمت. چاپ اول.
- بهره‌مند، حمید و امیرحسین جلالی فراهانی (تابستان ۱۳۹۳). شنود ارتباطات الکترونیک در حقوق کیفری ایران. *فصلنامهٔ مجلس و راهبرد*. ۲۱(۷۸). صص۵- ۳۳. بازیابی از: http://nashr.majles.ir/article_25.html
- دهخدا، علی اکبر (۱۳۷۷). *لغت‌نامهٔ فارسی دورهٔ کامل ۱۶ جلدی* دهخدا. تهران: دانشگاه تهران. چاپ اول.
- زر رخ، احسان (بهار ۱۳۸۹). جرائم مخابراتی. *مجلهٔ حقوقی دادگستری*. ۷۴(۶۹). صص۳۷- ۸۰. بازیابی از: http://www.jlj.ir/article_11186.pdf
- فتاحی، مختار (تابستان ۱۳۹۷). بررسی عناصر تشکیل‌دهندهٔ مادی و معنوی مصادیق جرائم رایانه‌ای. *فصلنامهٔ علمی- حقوقی قانون‌یار*. ۲(۶). صص۹۹- ۱۲۰. بازیابی از: https://www.magiran.com/paper/1853013
- قربانی‌نژاد کوهستانی، اعظم (۱۳۹۶). *جرائم علیه محرمانگی داده‌ها، دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای*. تهران: انتشارات فرهوش. چاپ اول.
- محمدنسل، غلامرضا (۱۳۹۲). *حقوق جزای اختصاصی جرائم رایانه‌ای در ایران*. تهران: انتشارات میزان. چاپ اول.

قوانین داخلی و معاهدات بین‌المللی

- اعلامیهٔ اسلامی حقوق بشر (۱۹۹۰).
- اعلامیهٔ جهانی حقوق بشر (۱۹۴۸).
- قانون اساسی جمهوری اسلامی ایران همراه با اصلاحات (۱۳۶۸).
- قانون جرائم رایانه‌ای (۱۳۸۸).
- قانون مجازات اسلامی (۱۳۷۵).
- کنوانسیون اروپایی حمایت از حقوق بشر و آزادی‌های بنیادین (۱۹۵۰).
- میثاق بین‌المللی حقوق مدنی و سیاسی (۱۹۶۶).

منابع انگلیسی

- French Penal Code (2002). Retrieved from: *https://www.legifrance.gouv.fr/Traductions/en-English/Legifrance-translations*

- Interception Of Communication In The United Kingdom (June 1999). A Consultation Paper, Presented To Parliament By The Secretary Of State For The Home Department By Command Of Her Mahesty. obtained from: *http://www.cyber-rights.org/interception/ioca99.htm*

- Interception of Communications Code of Practice, Pursuant to section 71 of the Regulation of Investigatory Powers Act 2000 (February 2015). Draft for public consultation. Retrieved from: *https://ulii.org/ug/legislation/act/2015/18-2*

Investigatory Powers Act of U.K (2016). Retrieved from: *http://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga_20160025_en.pdf*

- Legal Opinion on Intercept Communication, OXFORD PRO BONO PUBLICO, University of Oxford (January 2006). Retrieved from: *http://www2.law.ox.ac.uk/opbp/OPBP%20Intercept%20Evidence%20Report.pdf*

- Lorenzo Valeri, Geert Somers, Neil Robinson, Hans Graux, Jos Dumortier (2006). Handbook of Legal Procedures of Computer and Network Misuse in EU Countries, RAND Corporation. Retrieved from: *https://www.rand.org/content/dam/rand/pubs/technical.../2006/RAND_TR337.pdf*

- Electronic Communications Offences; Intercepting communications: The definition. Retrieved from: *www.inbrief.co.uk/offences/electronic-communications-offences/*

- Regulation of Interception of Communications in Selected Jurisdictions, Prepared by Thomas WONG, Research and Library Services Division Legislative Council Secretariat, 2 (February 2005). Hong Kong.

- UK-US surveillance regime was unlawful ‘for seven years’. Retrieved from:

https://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa

- New U.K. Law Fails European Court Standards on Mass Interception Disclosed by snowden. Retrieved from: *https://privacyinternational.org/feature/2301/new-uk-law-fails-european-court-standards-mass-interception-disclosed-snowden*

- Provision of Real-time Lawful Interception Assistance. Retrieved from: *https://clfr.globalnetworkinitiative.org/country/france/*