



سیاست جنایی ایران در قبال شنود غیرمجاز رایانه‌ای



محمد شفيعی، کارشناس ارشد جامعه‌شناسی

چکیده

از میان رفتارهای تعرض آمیز به حریم ارتباطات الکترونیک اشخاص، «شنود» جایگاه برجسته و متمایز خویش را حفظ کرده است. شنود غیرقانونی موجب از بین رفتن حیثیت شخصی افراد می‌شود و حریم خصوصی و حقوق شهروندی را مورد تعرض قرار می‌دهد. در این مقاله درصدد هستیم سیاست جنایی ایران در قبال شنود غیرمجاز رایانه‌ای را مورد بررسی قرار دهیم. یافته‌ها نشان داده است سیاست جنایی ایران در قبال شنود غیرقانونی در اسناد بالادستی مانند قانون اساسی، قانون مجازات اسلامی، قانون مبارزه با جرایم رایانه‌ای و سایر قوانین نشان‌دهنده جرم انگاری شنود غیرقانونی در سیاست جنایی ایران است. اگرچه در موارد خاصی اجازه شنود قضایی توسط مرجع قضایی داده می‌شود؛ اما در حالت عادی شنود مکالمات و داده‌های خصوصی افراد ممنوع است و طبق ماده ۵۸۲ قانون مجازات اسلامی، مرتکب به حبس از یک تا سه سال یا جزای نقدی از ۸۰/۰۰۰/۰۰۰ تا ۲۵۰/۰۰۰/۰۰۰ ریال محکوم خواهد شد؛ بنابراین سیاست جنایی حقوق ایران در قبال شنود غیرمجاز رایانه‌ای، برخورد شدید با عاملان آن است و در این زمینه لازم است اقدامات پیشگیرانه‌ای جهت حفظ داده‌های شخصی از جمله بالا بردن ضریب امنیت داده‌ها و استفاده از برنامه‌های رایانه‌ای و تلفن همراه هوشمند انجام گیرد. واژگان کلیدی: سیاست جنایی ایران، شنود غیرمجاز رایانه‌ای، حریم خصوصی، داده‌های شخصی

درآمد

حریم خصوصی اشخاص، مانند مکالمات و تماس‌های تلفنی، حریم منزل و محل کار، نامه‌نگاری‌های سنتی و ارسال نامه الکترونیک و محتوای قرار و ملاقات‌های خصوصی، به حکم قانون اساسی و منشور حقوق شهروندی، غیرقابل تعرض است. شنود غیرمجاز، در جایی مصداق دارد که شخص شنودکننده که مورد تعقیب جرم شنود غیرمجاز قرار خواهد گرفت، اجازه شنود نداشته و مخفیانه گوش کرده باشد. این عمل به نوعی تعرض به حریم خصوصی افراد محسوب می‌شود که البته با جرم دسترسی غیرمجاز متفاوت است.

جرایم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای به عنوان جرایمی که حریم خصوصی اشخاص را مورد تعرض قرار داده و سبب از بین رفتن محرمانگی داده‌ها و سامانه‌های رایانه‌ای می‌گردند، به موازات طرح در حقوق داخلی در قلمرو اسناد بین‌المللی نیز قابل بررسی می‌باشند. این دسته از جرایم تهدیدی جدی برای اشخاص حقیقی و حقوقی همه کشورها، علی‌الخصوص تجاوز به حریم خصوصی محسوب شده و سیستم‌ها و داده‌های همه کشورها را حتی با وجود تدابیر امنیتی در معرض خطر قرار می‌دهند. این امر به طور گسترده در سطح ملی و بین‌المللی شناخته شده است و به عنوان یک جرم، با ورود بشر به عصر فناوری اطلاعات و به ویژه با شکل‌گیری فضای سایبر که از دنیای فیزیکی کاملاً متمایز بود، پا به عرصه وجود گذاشته است. فضای سایبر که مجموعه جهان را به شهری کوچک تبدیل می‌کرد، امکان ارتکاب جرایم مدرنی که در قوانین قبل جرم‌انگاری نشده بود را برای مجرمان در اقصی نقاط

جهان فارغ از مرزهای جغرافیایی به وجود آورد؛ لذا این موضوع توجه قانون‌گذاران در سطح ملی و بین‌المللی را به خود جلب کرد و حتی قانون‌گذاران دریافتند که محدود نمودن قلمرو جرایم رایانه‌ای به موارد مدون در اسناد و قوانین ملی یارای مقاومت در برابر این جرایم را ندارد (عرب پور، ۱۳۹۰: ۹).

سیاست جنایی ایران مبتنی بر حفظ حریم خصوصی است و در این زمینه هرگونه تجاوز به حریم خصوصی در فضای واقعی و مجازی را منع کرده است. اهمیت مسئله نقض حریم خصوصی فضای مجازی ناشی از توسعه فناوری و امکان بیشتر و خسارت‌بارتر نقض حریم است. مسئولیت مدنی ناشی از نقض حریم خصوصی در فضای مجازی، از پیچیدگی‌های بیشتری نسبت به مسئولیت مدنی ناشی از نقض سایر حریم خصوصی برخوردار است (جعفری، ۱۳۹۶: ۴۴).

با پیدایش فناوری‌های ارتباطی الکترونیک، حریم خصوصی ارتباطات اشخاص با دگرگونی‌های بسیاری روبه‌رو شده است. کاربران ابزارها و گزینه‌های ارتباطی گوناگونی دارند. هرچند به همان نسبت دریافت غیرمجاز ارتباطاتشان نیز افزایش یافته است. آنچه در گذشته در پی دریافت غیرمجاز مکالمات تلفنی اشخاص «استراق سمع» نامیده می‌شد، هم‌اینک گستره بی‌پایانی از داده‌های رایانه‌ای را در بر می‌گیرد که در بستر مبادلات الکترونیک جریان دارند. گرچه از هنگام 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 (بهره‌مند، جلالی، ۱۳۹۳: ۵).

از میان رفتارهای تعرض‌آمیز به حریم ارتباطات الکترونیک اشخاص، «شنود» جایگاه برجسته و متمایز خویش را حفظ کرده است. شاید دلیل اصلی این امر، بکر بودن اطلاعاتی است که در بستر ارتباطی مربوطه جریان دارد. در اینجا فرض بر این است که پدیدآورنده اطلاعات، به محض پیدایش، دست‌کم برای بار نخست می‌خواهد تنها آنهایی از آن آگاهی یابد که آنها را به عنوان گیرنده مجاز می‌شناسد. پس از آن و در صورت ذخیره شدن اطلاعات در یک یا چند سامانه، از قلمرو حریم ارتباطی به قلمرو حریم اطلاعاتی وی راه می‌یابد که با اینکه همچنان آنها را سزاوار صیانت و احترام می‌داند، اما دیگر به اندازه حالتی نیست که مشمول حریم ارتباطی‌اش می‌شوند.

۱- مفهوم شنود غیرمجاز

شنود در معنای واژگانی، به کارکرد حس شنوایی اشاره دارد که اصوات محیط را برای آدمی درک‌شدنی می‌سازد؛ اما در اینجا معنای خاص و متمایزی یافته است و منظور رفتار هنجارشکنانه‌ای است که قانون‌گذار آن را سرزنش‌آمیز دانسته و برای آن ضمانت اجرای کیفری پیش‌بینی کرده است، لذا باید به دنبال واژگانی بود که بتواند مفهوم دقیق‌تر آن را بازتاب دهد (بهره‌مند، جلالی فراهانی، پیشین: ۱۲). قانون‌گذار پیش‌تر در قوانین عبارت «استراق سمع» را به کار برده است (ماده ۵۸۲ قانون مجازات اسلامی). معادل استراق سمع در زبان لاتین Eavesdropping است که در دانشنامه‌ها برایش معنای شنیدن پنهانی فیزیکی یا حتی به وسیله ابزارهای مخابراتی آمده است (گارنر، ۱۹۹۹: ۵۲۹).



در بر نمی گیرد و اینها ماهیت متفاوتی دارند گرچه می توانند باعث جابه جایی داده ها و محتوای رایانه ای شوند و با دریافتشان می توان داده ها را بازسازی کرد (جلالی، ۱۳۸۹: ۳۰).

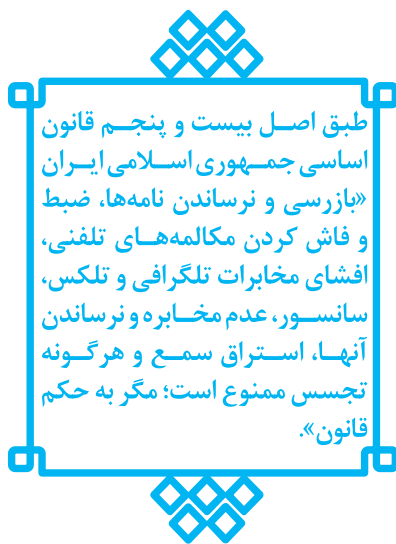
۲- مبانی جرم شنود غیرمجاز

نقض حریم خصوصی در فضای مجازی یکی از مهم ترین مسائل روز جامعه ماست که از دو منظر قابل بررسی است. یکی از جانب قربانیان نقض حریم خصوصی در فضای مجازی و دیگری از سوی ناقضان حریم خصوصی در فضای مجازی. طبیعی است که هردوی این جنبه ها در تعریف و ترسیم مفهوم حریم خصوصی و تفاوت های آن با فضای فیزیکی مؤثر خواهد بود (فتحی، شاهمرادی، ۱۳۸۹: ۲۲۹).

یکی از نموده های جرایم سایبری، شنود غیرقانونی است که موجب نقض حریم خصوصی افراد و ایجاد آسیب روانی و حیثیتی به آنها می شود.

بر اساس اصل ۲۵ قانون اساسی بازرسی و نرساندن نامه ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آنها، استراق سمع و هرگونه تجسس ممنوع است مگر به حکم قانون؛ بنابراین می توان نتیجه گرفت ضبط و فاش کردن مکالمات تلفنی در زمره استراق سمع است و بر همین اساس هرگونه تجسس در مکالمات، ممنوع است. همچنین بر اساس ماده ۵۸۲ قانون مجازات اسلامی «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 کند یا بدون اجازه صاحبان آنها مطالب را افشا کند، به حبس از یک سال

در حال انتقال ارتباطات رایانه ای است. لذا بر پایه تفسیر ادبی و فنی (مبتنی بر حریم خصوصی ارتباطی) می توان گفت داده های ترافیک مشمول داده محتوا می شوند؛ بنابراین شنود آنها پیرو شرایط ماده (۷۳۰) قانون مجازات اسلامی، جرم و قابل مجازات است. نکته دیگری که باید درباره داده های رایانه ای تبیین شود، این است که آیا باید به شکل دیجیتالی، یعنی مبتنی بر صفر و یک ذخیره و جابه جا شوند یا اینکه به شکل آنالوگ هم امکان جابه جایی آنها وجود دارد؟ به نظر می رسد توان سامانه های رایانه ای در پردازش دیجیتالی داده ها اهمیت دارد و جابه جایی آنها می تواند به دو شکل دیجیتال و آنالوگ صورت گیرد. به این ترتیب، صداهایی که با دستگاه های بی سیم موسوم به واکای تاکی جابه جا می شوند، می توانند موضوع جرم شنود قرار گیرند.



با توجه به این ملاحظات، در ماده ۵۸۲ قانون مجازات اسلامی علاوه بر محتوای رایانه ای، امواج الکترومغناطیسی هم موضوع شنود غیرمجاز در این ماده قرار گرفته اند. با توجه به تعریفی که از داده و محتوای رایانه ای ارائه شد، امواج الکترومغناطیسی یا رادیویی را

فرهنگ های واژگان فارسی در تعریف این عبارت آورده اند: «شنود، پنهانی گوش کردن سخنان دیگران بدون آگاهی و رضایت آنها یا مستقیم و یا غیرمستقیم از راه دستگاه های مخابراتی» است (دهخدا، ۱۳۸۹: ۲۳۶). تعریف دانشنامه ای این عبارت به خوبی مفهوم منفی شنود را بازتاب می دهد، لیکن پرسش اینجاست که چرا قانون گذار جرایم رایانه ای، همین عبارت را به کار نبرده و واژه شنود را جایگزین آن کرده است؟ به نظر می رسد پیدایش جنبه ها و ویژگی های فن آورانه و نوآورانه در ارتکاب این جرم، قانون گذار را بر آن داشته تا از مفهوم سنتی اش فاصله بگیرد و واژه مناسب تری را جایگزین آن کند که با توجه به کاربردش در عرف، امکان تسری آن به سایر موضوعات هم وجود داشته باشد.

به این ترتیب، واژه شنود به کار رفته در این متن دلالت بر «دریافت» محتوا دارد و نه «درک شدن» آن به شکل شنیدن یا با حواس دیگر. برای «دریافت» محتوا به این شکل نیز باید آن را از مسیر اصلی خود خارج و به سامانه ای که توان ذخیره یا پردازش آن را دارد، وارد کرد و سپس به مسیر اصلی بازگرداند. چنین تغییر یا انحرافی در مسیر ارتباطی، رکن اصلی ارتکاب این رفتار است و به همین دلیل برای آن واژه Interception و نه Eavesdropping به کار رفته است.

با توجه به این توضیحات، پرسش اینجاست که آیا داده های ترافیک مشمول مفهوم «محتوای» برشمرده در ماده ۵۸۲ قانون مجازات اسلامی می شوند؟ واقعیت این است که داده های ترافیک در تعریف محتوای رایانه ای می گنجند و از آن بیرون نیستند و آن گونه که اشاره شد، مبنای تفکیک آنها، تعرض آمیزی کمتر دسترسی به آنها در مقایسه با محتوای

تاسه سال یا جزای نقدی از ۸۰/۰۰۰/۰۰۰ تا ۲۵۰/۰۰۰/۰۰۰ ریال محکوم خواهد شد». بر اساس ماده ۱۵۰ قانون آیین دادرسی کیفری: «کنترل ارتباطات مخابراتی افراد ممنوع است، مگر در مواردی که به امنیت داخلی و خارجی کشور مربوط باشد یا برای کشف جرایم موضوع بندهای (الف)، (ب)، (پ) و (ت) ماده ۳۰۲ این قانون لازم تشخیص داده شود...».

۳- غیرمجاز بودن شنود

شرط مهم برای اتصاف عنوان مجرمانه شنود، «غیرمجاز» بودن آن است. پرسش آن است که چه شخصی باید اجازه شنود را اعطا کند تا وصف «غیرمجاز» نداشته باشد؟ نکته بسیار مهمی که باید از آن به عنوان ویژگی متمایز این ماده با سایر مواد این قانون یاد کرد، این است که در اینجا مالکیت محتوا، مبنایی برای احراز مجاز یا غیرمجاز بودن رفتار به شمار نمی آید و مهم آن است که خط ارتباطی به چه کسی یا کسانی تعلق دارد. ممکن است محتوای در حال انتقال میان دو یا چند شخص به دیگری تعلق و وی قصد داشته باشد آن را دریافت کند. با اینکه داده‌ها در تعلق یا مالکیت اوست، اما حق ندارد به این حریم ارتباطی تعرض و محتوایش را دریافت کند و ممکن است به شنود مقرر در این ماده محکوم شود.

با توجه به معنی لغوی، اصطلاح به کار رفته در قانون جرایم رایانه‌ای دارای ابهام است، مگر آنکه بگوییم با توجه به اینکه شنود محتوای ارتباطات در فضای مجازی و پنهانی انجام می‌شود از این رو نیازی به تصریح قید «پنهانی» نیست. همچنین شنود محتوای ارتباطات در فضای تبادل «طول مسیر انتقال» توسط شخص ثالث انجام می‌شود. البته این به معنای آن نیست که در مبدأ و مقصد

امکان شنود وجود ندارد؛ به عبارت دیگر از زمانی که پیام وارد سامانه رایانه‌ای یا مخابراتی می‌شود، مسیر انتقال محسوب می‌شود. در یک دستگاه نمابر یا دورنگار نیز که تصاویر و کلمات نوشتاری روی کاغذ را از طریق خطوط تلفن انتقال می‌دهد یا پیامک‌های تلفن‌های همراه از زمان ارسال تا زمان دریافت احتمال شنود غیرمجاز آن وجود دارد، لذا چون با این عمل حریم خصوصی افراد دچار تعرض می‌شود قانون‌گذار دیگر بحث اینکه موارد شنود باید دارای کدها یا قفل‌های حفاظتی باشد را قید ننموده، لذا به همین منظور می‌توان جرم شنود غیرمجاز را در زمره جرایم علیه آسایش عمومی دانست. نکته بسیار مهمی که باید از آن به عنوان ویژگی متمایز این ماده با سایر مواد این قانون یاد کرد، این است که در اینجا مالکیت محتوا، مبنایی برای احراز مجاز یا غیرمجاز بودن رفتار به شمار نمی آید و مهم آن است که خط ارتباطی به چه کسی یا کسانی تعلق دارد. ممکن است محتوای در حال انتقال میان دو یا چند شخص به دیگری تعلق و وی قصد داشته باشد آن را دریافت کند. با اینکه داده‌ها در تعلق یا مالکیت اوست، اما حق ندارد به این حریم ارتباطی تعرض و محتوایش را دریافت کند و ممکن است به شنود مقرر در این ماده محکوم شود. توجه به این نکته نیز حائز اهمیت است که در این حالت نیز رضایت پیشینی همه طرفه‌های ارتباط غیرعمومی شرط است و چنانچه یکی از طرفه‌ها رضایت خود را اعلام نکند، جرم تحقق خواهد یافت. لیکن این رضایت می‌تواند صریح یا ضمنی باشد که هر دو شکل آن معتبر خواهد بود (بهرمند، جلالی فراهانی، پیشین: ۲۰).

از سوی کارفرمایان آنها می‌تواند مسئله‌ساز باشد. در چنین مواردی، معمولاً کارفرما یا مدیر یک شرکت، به هنگام عقد قرارداد با کارمندان یا کارگران خود، رضایت آنها را مبنی بر شنود ارتباطاتشان می‌گیرد. باین‌حال، چنین رضایتی نسبت به ارتباطات درون‌سازمانی پرسنل این مجموعه‌ها معتبر و قابل استناد خواهد بود و ارتباطات برون‌سازمانی آنها تنها در صورتی مجاز خواهد بود که پیشاپیش رضایت آن سوی ارتباط نیز گرفته شود.

۴- پیشینه تقنینی حفاظت از داده‌های شخصی

از جمله تمایزهای بارز حریم ارتباطی و حریم اطلاعاتی اشخاص این است که در اینجا از بستر ارتباطی و تبادل داده‌ها و اطلاعات و نه خود آنها حمایت می‌شود. لذا تفاوتی نمی‌کند که چه نوع اطلاعاتی در اینجا جابه‌جا شود. ممکن است اطلاعات عمومی باشد، لیکن به دلیل قرار گرفتن در چنین موقعیتی از مزایای محرمانگی برخوردار می‌شود. اما در حریم خصوصی اطلاعاتی، نوع اطلاعات مهم است؛ بنابراین کوشش می‌شود از آن تعریف روشن و مشخصی به عمل آید؛ مانند اطلاعات شخصی در برابر اطلاعات عمومی و تقسیم‌بندی اطلاعات شخصی به عادی و حساس (انصاری، ۱۳۸۶: ۶۹). به جز مقررات قانون اساسی، پیشینه حمایت قانونی از حریم ارتباطاتی شهروندان به قانون تأسیس شرکت مخابرات ایران، مصوب ۱۳۵۰ برمی‌گردد. در تبصره «۱» ماده ۱۴ این قانون آمده است: «هرکس از وسایل مخابراتی عمومی یا اختصاصی که در اختیار دارد به‌طور غیرمجاز استفاده کند در نوبت اول به او کتباً اخطار می‌شود و در نوبت دوم به مدت پانزده روز ارتباط او قطع یا از استفاده ممنوع خواهد شد.



ماهوی را در برمی گیرد و با در نظر گرفتن اصول و معیارهای دادرسی عادلانه و رعایت کرامت انسانی، درصدد است تا با کشف و اثبات به موقع و بهینه جرم، واکنش کیفری مناسبی اعمال نماید تا به هدف کاهش نرخ جرم نایل آید (کرمی، ۱۳۹۴: ۹). سیاست جنایی در مقابل جرایم سایبری به طور عام و شنود غیرمجاز در قانون مجازات اسلامی، قانون مجازات جرایم رایانه‌ای مصوب ۱۳۸۸ و قانون تجارت الکترونیک مصوب ۱۳۸۲ است. اگرچه چگونگی رعایت معیارهای جرم‌انگاری، رابطه‌ای مستقیم با سیاست کیفری دارد، لیکن نظریه‌های مبنایی حاکم بر نظام حقوقی، سیاست جنایی، رویکردهای کلان کیفری قانون‌گذار، شرایط اقتصادی، سیاسی و اجتماعی میزان اهمیت و تأثیر ارزش‌های اخلاقی نیز در تعریف اصول محوری جرم‌انگاری در هر نظام حقوقی نقش بسزایی دارد (فرجی‌ها، علمداری، ۱۳۹۶: ۶۴۲).

از آنجاکه این آیات و روایات و همچنین اصول فقهی نام برده شده همگی قائل به ممنوعیت نقض حریم خصوصی و حرمت این حریم شده‌اند؛ بنابراین می‌توانند مبنای جرم‌انگاری جرایم علیه حریم خصوصی از جمله شنود، دسترسی و افشای مراسلات واقع شوند و مورد استناد قرار گیرند. مشهور فقها جرایم دسترسی، شنود و افشای مراسلات را منع نموده و آن را مستلزم ضمان دانسته‌اند، حقوق کیفری ایران نیز در خصوص این‌گونه جرایم، مجازات در نظر گرفته و مرتکبین آنها را مستلزم مسئولیت کیفری می‌داند (رزمجو دوکشکانی، ۱۳۹۷: ۱۲).

در این زمینه طبق اصل بیست و پنجم قانون اساسی جمهوری اسلامی ایران «بازرسی و نرساندن نامه‌ها، ضبط و فاش کردن مکالمه‌های تلفنی، افشای

مقام اعمال قوانین جدیدی مانند قانون جرایم رایانه‌ای، باید دامنه شمول آن را مدنظر قرار داد. این مهم در قسمت ضمانت اجرای مقرر برای این جرم خواهد آمد.



بر اساس ماده ۵۸۲ قانون مجازات اسلامی «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 کند یا بدون اجازه صاحبان آنها مطالب را افشا کند، به حبس از یک سال تا سه سال یا جزای نقدی از ۸۰/۰۰۰/۰۰۰ تا ۲۵۰/۰۰۰/۰۰۰ ریال محکوم خواهد شد».



همچنین ماده ۲ قانون جرایم رایانه‌ای مقرر می‌دارد: «هرکس به طور غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری را شنود کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد». همچنین در ماده ۴۸ همان قانون آمده است: «شنود محتوای در حال انتقال ارتباطات غیرعمومی در سیستم‌های رایانه‌ای یا مخابراتی مطابق مقررات راجع به شنود مکالمات تلفنی خواهد بود».

۵- سیاست جنایی ایران در قبال شنود غیرمجاز

سیاست جنایی مجموعه‌ای منسجم و یکپارچه از تدابیر تقنینی، قضایی و اجرایی در حوزه حقوق کیفری شکلی و

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 غیرمجاز در آیین‌نامه‌ای که از طرف شرکت تهیه و به تصویب وزیر پست و تلگراف و تلفن خواهد رسید تعیین می‌گردد».

در این تبصره، عبارت «استفاده غیرمجاز» آمده که قاعدتاً شامل نقض حریم ارتباطات مخابراتی نیز می‌شود و با توجه به تعریفی که از مخابرات در تبصره «۱» ماده ۱ این قانون آمده و به‌خوبی شامل ابزارها و فناوری‌های امروزی نیز می‌شود، در صورت روزآمد شدن آن آیین‌نامه از سوی وزارت مذکور، می‌تواند سوءاستفاده‌های نوین مخابراتی را هم در برگیرد و مشمول ضمانت اجرای آن شود. به‌ویژه آنکه یکی از وظایف اصلی این وزارتخانه به موجب بند «ف» ماده ۳ قانون وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات، مصوب ۱۳۸۲، «حفاظت و حراست و عدم ضبط و افشای انواع مراسلات و امانات پستی و همچنین مکالمات تلفنی و مبادلات شبکه اطلاع‌رسانی و اطلاعات مربوط به اشخاص حقیقی و حقوقی طبق قانون عنوان شده است که انتظار می‌رود وزارتخانه مقررات لازم‌الاجرا را از سوی کمیسیون تنظیم مقررات ارتباطات به تصویب برساند (بهره‌مند، جلالی فراهانی، پیشین: ۱۰).

پیشینه قانونی دیگر، ماده ۵۸۲ قانون مجازات اسلامی است.^(۱) این ماده بیش از آنکه ناظر به امور پستی باشد، به امور مخابراتی مربوط می‌شود؛ بنابراین با توجه به تعریف گسترده‌ای که از مخابرات در نصوص قانونی آمده، به‌خوبی شامل سوءاستفاده‌های نوین هم می‌شود و در



مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آنها، استراق سمع و هرگونه تجسس ممنوع است؛ مگر به حکم قانون». در این اصل ضبط و فاش نمودن مکالمه‌های تلفنی و استراق سمع و هرگونه تجسس ممنوع اعلام شده است که با جامعیت کم‌نظیری تمامی شنودهای مجاز و غیرمجاز توسط دستگاه‌های دولتی و افراد و دستگاه‌های غیردولتی یا عمومی را شامل می‌شود. از این رو همواره با پیشرفت فن‌آوری‌ها هماهنگ بوده و جامعیت خود را از دست نمی‌دهد. اصل مذکور به عنوان شالوده و اساس قانون‌گذاری‌های عادی همواره باید مورد توجه قرار گیرد. متأسفانه تا قبل از تصویب قانون جرایم رایانه‌ای بسیاری از شنودهای غیرمجاز تلفنی و نظایر آن از ناحیه افراد غیردولتی جرم به حساب نمی‌آمد؛ در حالی که بر ممنوعیت آنها در این اصل تصریح شده بود. نکته دیگر این است که در آخر اصل ۲۵ استثنای شنود غیرمجاز تنها به حکم قانون باید باشد که همان شنود مجاز است و این استثنا مقید شده است صرفاً به حکم قانون. از این رو سایر مقررات مانند تصویب‌نامه‌ها و آیین‌نامه‌ها را شامل نمی‌شود. با تصویب قانون جرایم رایانه‌ای در سال ۱۳۸۸ و تصریح به سامانه‌های مخابراتی و امواج الکترومغناطیسی در آن و به استناد ماده ۱۲ قانون استفاده از بی‌سیم‌های اختصاصی، مجازات مذکور در ماده ۱۱ قابلیت اعمال نداشته و باید به قانونی که مجازات آن اشد است، عمل شود. طبق ماده ۵۸۲ قانون مجازات اسلامی (تعزیرات و مجازات‌های بازدارنده) [اجرای نقدی اصلاحی ۱۳۹۹/۱۱/۸]، «هر یک از مستخدمین و مأمورین 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 افشاء نماید به حبس از یک سال تا سه سال و یا جزای نقدی از ۸۰/۰۰۰/۰۰۰ تا ۲۵۰/۰۰۰/۰۰۰ ریال محکوم خواهد شد». آن‌گونه که پیداست این کیفرها طیف گسترده‌ای را در برمی‌گیرند که می‌توان چنین پنداشت قانون‌گذار خواسته است اختیار صلاح‌دیدگی کافی را به قاضی اعطا کند؛ چراکه این جرم، گونه‌های فراوان و گستره‌ای فراگیر را در برمی‌گیرد که می‌تواند آسیب‌های کم و زیادی را به بزه‌دیدگان وارد آورد. موضوع جرم شنود غیرمجاز، باید در مورد ارتباطات غیرعمومی داده‌ها باشد. ماده ۲ قانون جرایم رایانه‌ای ایران «شنود غیرمجاز سایبری» را از مصادیق جرایم رایانه‌ای و شنود محتوای در حال انتقال ارتباطات غیرعمومی را در زمره جرم شنود غیرمجاز دانسته است. مرتکب جرم شنود غیرمجاز رایانه‌ای که کارمند دولت یا نهادهای حکومتی و عمومی یا از اعضای نیروهای مسلح و متصدی یا متصرف قانونی شبکه‌های رایانه‌ای یا مخابراتی باشد یا اینکه جرم به صورت سازمان‌یافته ارتکاب یافته باشد، به ۱۶ ماه و یک روز حبس تا دو سال یا جزای نقدی تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد. داده‌های صوتی که توسط شخص شنیده می‌شود همان استراق سمع سنتی است اما ملاحظه ایمیل‌ها یا نامه‌های الکترونیکی و سایر داده‌های مجازی، در حکم شنود غیرمجاز است. موضوع جرم شنود غیرمجاز سایبری، محتوای در حال انتقال است. مخفیانه گوش کردن به مطالبی که ذخیره شده‌اند به عنوان جرم دسترسی غیرمجاز محسوب شده و جرم شنود

غیرمجاز نیست. تفاوت دیگر دسترسی غیرمجاز با شنود غیرمجاز رایانه‌ای، امکان ارتکاب جرم دسترسی غیرمجاز نسبت به داده‌ها و سامانه‌ها است. با توجه به آنکه امروزه به بهانه مقابله با تروریسم و دیگر جرایم امنیتی، استفاده از شنود تلفنی و رهگیری اطلاعات و داده‌ها به یکی از برجسته‌ترین راه‌های کنترل شهروندان تبدیل شده است حمایت شهروندان نسبت به دسترسی غیرمجاز به داده‌های شخصی آنان اهمیتی بیش از پیش پیدا کرده است.

۶- موارد ضروری و مجاز شنود

گاهی لازم است به منظور کشف جرم (به‌خصوص در جرایم مهم) تلفن و مکالمات اشخاص مورد شنود قرار گیرد که از آن به عنوان شنود مجاز یا مشروع یاد شد. به همین ترتیب امکان دارد مکالمه‌های شخص ضبط شود و بعداً مورد استفاده و شنود قرار گیرد. جرم شنود غیرمجاز رایانه‌ای که مرتکب آن کارمند دولت یا نهادهای حکومتی و عمومی یا از اعضای نیروهای مسلح و متصدی یا متصرف قانونی شبکه‌های رایانه‌ای یا مخابراتی باشد یا اینکه جرم به صورت سازمان‌یافته ارتکاب یافته باشد، مستوجب ۱۶ ماه و یک روز حبس تا دو سال یا جزای نقدی تا چهل میلیون ریال یا هر دو مجازات می‌باشد. تکرار جرم شنود غیرمجاز رایانه‌ای برای بار سوم، محرومیت از خدمات الکترونیک عمومی از یک ماه تا یک سال را در پی دارد. با توجه به بخشنامه رئیس محترم وقت قوه قضاییه می‌توان گفت امر شنود مکالمه‌های تلفنی تا حدود زیادی نظام‌مند شده و تلاشی در جهت جلوگیری از شنودهای خودسرانه توسط دستگاه‌های اطلاعاتی و امنیتی صورت گرفته است.



اختصاصی در خصوص لزوم اعمال قوانینی که مجازات آنها اشد است.

۷-۲- شنود در قانون جرایم رایانه‌ای و قانون مجازات اسلامی

ماده ۵۸۲ قانون مجازات اسلامی اختصاص به مستخدمان و مأموران دولتی دارد و شنود غیرمجاز توسط آنها را جرم‌انگاری کرده است؛ درحالی‌که ماده ۲ قانون جرایم رایانه‌ای عام بوده و شامل تمامی افراد جامعه می‌شود. از نظر مصالح اجتماعی نیز مجازات مقرر در ماده ۵۸۲ قانون مجازات اسلامی شدیدتر از مجازات مذکور در ماده ۲ قانون جرایم رایانه‌ای است و به لحاظ موقعیت ویژه کارکنان و مستخدمان دولتی و دسترسی بسیاری از آنها به امکانات شنود باید تفاوتی بین مجازات آنها و سایر شهروندان وجود داشته باشد، همچنین ماده ۷۳۰ قانون مجازات اسلامی ۱۳۹۲ را می‌توان قانون عام‌تر برای شنود غیرمجاز در نظر گرفت.

۷-۳- شنود در قانون جرایم رایانه‌ای و قانون آیین دادرسی کیفری

با توجه به توضیحی که در ذیل ماده ۴۸ قانون جرایم رایانه‌ای داده شد و به لحاظ ارجاع امر شنود مجاز به سایر قوانین و مقررات مربوط به شنود مکالمه‌های تلفنی، هیچ مغایرتی میان ماده ۴۸ قانون جرایم رایانه‌ای و تبصره آن با ماده ۱۵۰ قانون آیین دادرسی کیفری وجود ندارد.

۷-۴- شنود در قانون جرایم رایانه‌ای و قانون تجارت الکترونیکی

با توجه به اینکه قانون تجارت الکترونیکی در محدوده امور تجارت الکترونیکی وضع شده است، مواد ۶۴ و ۷۵ این قانون به لحاظ خاص بودن آنها نسبت به قانون عام لاحق (قانون جرایم رایانه‌ای) در محدوده امور تجاری لازم‌الاجرا بوده و منسوخ نیستند.

برای شنود غیر مجاز مجازات حبس یا جزای نقدی در نظر گرفته است. در این زمینه نظریه مشورتی ۱۸۵۹/۹۸/۷ مورخ ۱۳۹۸/۱۲/۱۱ اداره کل حقوقی قوه قضاییه با عنایت به اطلاق عبارت «کنترل ارتباطات مخابراتی افراد» در ماده ۱۵۰ قانون آیین دادرسی کیفری مصوب ۱۳۹۲ که در راستای نحوه اعمال اصل بیست و پنجم قانون اساسی جمهوری اسلامی ایران تصویب شده است، ممنوعیت موضوع این ماده علاوه بر محتوای ارتباطات مخابراتی شامل «اخذ پرینت فهرست ورودی و خروجی تماس‌ها و پیامک‌های متهم» نیز می‌شود و ردیابی از طریق تلفن همراه از مفهوم «کنترل ارتباطات مخابراتی افراد» موضوع ماده ۱۵۰ قانون آیین دادرسی کیفری خارج است.

۷-۵- مقایسه بزه شنود غیرمجاز در قانون جرایم رایانه‌ای و سایر قوانین مرتبط

با تصویب قانون دادرسی جرایم نیروهای مسلح و دادرسی الکترونیکی بسیاری از قوانین سابق نسخ ضمنی شده‌اند؛ بنابراین با مقایسه بزه شنود غیرمجاز در قانون جرایم رایانه‌ای و سایر قوانین مرتبط می‌توان نکات زیر را دریافت.

۷-۱- شنود در قانون جرایم رایانه‌ای و قانون استفاده از بی‌سیم‌های اختصاصی

با توجه به اینکه ماده ۲ قانون جرایم رایانه‌ای شنود محتوای در حال انتقال تمامی سامانه‌های مخابراتی یا امواج الکترومغناطیسی را جرم دانسته و بی‌سیم‌های اختصاصی نیز در زمره وسایلی هستند که از سیستم امواج الکترومغناطیسی استفاده می‌کنند و با عنایت به صراحت ماده ۱۲ قانون استفاده از بی‌سیم‌های

اما ترتیب پیش‌بینی شده در دستورالعمل مذکور؛ یعنی پیش‌بینی یک قاضی در حوزه قضایی استان‌ها به عنوان قاضی ویژه شنود و منحصر کردن امر شنود مجاز به تشخیص و صلاحدید این قاضی با تبصره ذیل ماده ۱۰۴ قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور کیفری مغایر است؛ چراکه منظور قانون‌گذار از قاضی مندرج در تبصره مذکور، قاضی رسیدگی‌کننده به پرونده است، نه قاضی دیگری که هیچ اطلاعی از محتویات پرونده ندارد.

بنابراین پیش‌بینی تعیین قاضی ویژه شنود با قوانین موضوعه سازگار نیست؛ هرچند می‌توان مزایایی برای آن قائل شد؛ از جمله اینکه در هر موردی تلفن افراد مورد کنترل قرار نمی‌گیرد و از پراکندگی تصمیم‌ها در این زمینه جلوگیری می‌شود؛ اما نباید از نظر دور داشت که قاضی مربوطه نیز مسئول اعمالی است که در مقام رسیدگی و تحقیق انجام می‌دهد و نمی‌تواند خودسرانه دستور شنود را در هر موردی صادر نماید.

در ماده ۱۵۰ قانون آیین دادرسی کیفری بیان شده است: «کنترل ارتباطات مخابراتی افراد ممنوع است، مگر در مواردی که به امنیت داخلی و خارجی کشور مربوط باشد یا برای کشف جرایم موضوع بندهای (الف)، (ب)، (پ) و (ت) ماده (۳۰۲) این قانون لازم تشخیص داده شود. در این صورت با موافقت رئیس کل دادگستری استان و با تعیین مدت و دفعات کنترل، اقدام می‌شود. کنترل مکالمات تلفنی اشخاص و مقامات موضوع ماده (۳۰۷) این قانون منوط به تأیید رئیس قوه قضاییه است و این اختیار قابل تفویض به سایرین نمی‌باشد». یا همان‌طور که در ماده ۷۳۰ قانون مجازات اسلامی ۱۳۹۲،

برآمد

رعایت و حفظ حریم خصوصی افراد از حقوقی است که مورد توجه نظام‌های حقوقی مختلف و همچنین مورد تأیید اسلام و فقها قرار گرفته است؛ حقوق ایران نیز به تبعیت از شریعت اسلام و فقه امامیه ورود غیرمجاز به حریم خصوصی را منع نموده و برای آن مجازات در نظر گرفته است. جرایم علیه محرمانگی داده‌ها و یا به دیگر سخن، جرایم دسترسی، شنود غیرمجاز و افشای غیرمجاز مراسلات از مصادیق جرایم علیه محرمانگی داده‌ها به شمار می‌آیند که مورد جرم‌انگاری قرار گرفته‌اند. حریم خصوصی اشخاص، دسترسی غیرمجاز، استراق سمع و افشای مراسلات افراد از اهمیت خاصی در فقه اسلامی و حقوق ایران برخوردار هستند و قواعد خاصی در این زمینه از سوی شارع وضع گردیده است، به طوری که زندگی خصوصی اشخاص و مکالمات و مراسلات آنها بایستی علاوه بر اینکه از سوی حکومت اسلامی مصون از تعرض باشد بلکه حفظ آنها وظیفه‌ای همگانی از سوی تمام افراد جامعه می‌باشد؛ بنابراین می‌توان نتیجه گرفت که قواعد مربوط به حفظ حریم خصوصی و حفظ مکالمات و مراسلات افراد در فقه و حقوق اسلام از مترقی‌ترین قواعد حتی در دوران کنونی می‌باشد.

مبنای اصلی شنود غیرمجاز حفظ حریم خصوصی و رعایت حقوق شهروندی است که از طرف حکومت یا سایر افراد نباید مورد تجاوز قرار گیرد. با گسترش فناوری نوین ارتباطی، دسترسی غیرمجاز به اطلاعات و شنود غیرقانونی به عنوان جرایم خاص این حوزه، جرم‌انگاری شده‌اند؛ به عنوان مثال طبق ماده ۵۸۲ قانون مجازات اسلامی، شنود غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی، حبس از یک سال تا سه سال و یا جزای نقدی یا هر دوی آنها را در پی دارد. آن گونه که پیداست این کیفرها طیف گسترده‌ای را در بر می‌گیرند که می‌توان چنین پنداشت قانون‌گذار خواسته است اختیار صلاح‌دید کافی را به قاضی اعطا کند؛ چراکه این جرم، گونه‌های فراوان و گستره فراگیری را در بر می‌گیرد که می‌تواند آسیب‌های کم و زیادی را به بزه دیدگان وارد آورد. موضوع جرم شنود غیرمجاز، باید در مورد ارتباطات غیرعمومی داده‌ها باشد.

شواهد نشان می‌دهد سیاست جنایی ایران در چند دهه اخیر در زمینه شنود غیرقانونی و جرایم مشابه با آن برخورد کیفری است و با پیشرفت فناوری رایانه‌ای، مجازات‌های متناسبی نیز تدوین شده است؛ از جمله اینکه در قانون مجازات اسلامی و جرایم رایانه‌ای، برای جرم شنود غیر مجاز کیفر تعیین کرده است. مبنای فقهی و حقوقی جرم‌انگاری شنود غیرمجاز، حفظ حریم خصوصی به عنوان یکی از حقوق قانونی و شرعی افراد جامعه است. این حق به افراد اطمینان می‌دهد که حریم خصوصی آنها محفوظ خواهد بود، اما به نظر می‌رسد لازم است در کنار اقدامات کیفری، مجموعه‌ای از طرح‌های پیشگیرانه برای مقابله با جرایم سایبری؛ از جمله شنود غیرقانونی تصویب و اجرا کرد. همچنین از آنجایی که قوانین تصویب شده عمدتاً مبتنی بر داده‌های رایانه‌ای است، با گسترش تلفن همراه پیشنهاد می‌شود قوانین و مقررات متناسب با شنود غیرقانونی تلفن‌های همراه نیز تدوین و وضع گردد.

پی‌نوشت

۱- این ماده جایگزین ماده ۶۴ قانون مجازات اسلامی مصوب ۱۳۶۲ است.

فهرست منابع

- ۱- انصاری، باقر، حقوق حریم خصوصی، تهران، سمت، ۱۳۸۶
- ۲- بهره‌مند، حمید؛ جلالی فراهانی، امیرحسین، شنود ارتباطات الکترونیک در حقوق کیفری ایران، مجلس و راهبرد دوره ۲۱، شماره ۷۸، ۱۳۹۳
- ۳- جعفری، علی؛ رهبر پور، محمدرضا، مسئولیت مدنی ناشی از نقض حریم خصوصی داده‌ها در فقه امامیه و حقوق موضوعه، حقوق خصوصی، دوره ۵، شماره ۱۸، ۱۳۹۶
- ۴- جعفری، جوان، جرایم سایبر و رویکرد افتراقی حقوق کیفری (با نگاهی به قانون مجازات اسلامی بخش جرایم رایانه‌ای)، مجله دانش و توسعه (علمی - پژوهشی)، سال هفدهم، شماره ۳۴، ۱۳۸۹
- ۵- جلالی فراهانی، امیرحسین، تفتیش و توقیف رایانه‌ها و تحصیل دلایل الکترونیکی در تحقیقات کیفری، تهران، نشر روزنامه رسمی، ۱۳۸۹
- ۶- دهخدا، علی‌اکبر، لغت‌نامه دهخدا، تهران، موسسه انتشارات دانشگاه تهران، ویرایش چهارم، ۱۳۸۹
- ۷- رزمجو دوکشانی، غزل، بررسی مبانی فقهی جرم‌انگاری جرایم دسترسی و شنود غیرمجاز مخابراتی و افشای غیرمجاز مراسلات و

- ماهیت این جرایم در حقوق کیفری ایران، پایان‌نامه کارشناسی ارشد دانشگاه آیت‌الله‌العظمی بروجردی، ۱۳۹۷
- ۸- زرکلام، ستار؛ عبدی، قاسم، جایگاه حریم خصوصی در سیاست جنایی تقنینی ایران، مجله قضاوت، شماره ۷۹، ۱۳۹۳
 - ۹- عرب پور، حمزه، جرایم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای در نظام حقوقی ایران و اسناد بین‌المللی، پایان‌نامه کارشناسی ارشد، دانشکده علوم اداری و اقتصاد، ۱۳۹۰
 - ۱۰- غریب‌زندی، احمد و همکاران، احکام حریم در حقوق خصوصی ایران، فصلنامه مطالعات علوم اجتماعی، دوره ۱، شماره ۱، ۱۳۹۴
 - ۱۱- فتحی، یونس؛ شاهمادی، خیراله، گستره و قلمرو حریم خصوصی در فضای مجازی، مجله حقوقی دادگستری، شماره ۹۹، ۱۳۸۹
 - ۱۲- فرجی‌ها، محمد؛ علمداری، علی، مطالعه تطبیقی معیارهای جرم‌انگاری در فضای سایبر در نظام کیفری ایران و آلمان، مطالعات حقوق تطبیقی دوره ۸، شماره ۲، ۱۳۹۶
 - ۱۳- کرد علیوند، روح‌الدین؛ میرزایی، محمد، گونه‌شناسی جرایم سایبری با نگاهی به قانون جرایم رایانه‌ای و آمار پلیس فتا، مجله حقوقی دادگستری، سال هشتاد و دوم، شماره ۱۰۲، ۱۳۹۵
 - ۱۴- کرمی، داود، سیاست کیفری افتراقی در جرایم سایبر با تأکید بر حقوق کیفری ایران، پایان‌نامه دکترا دانشکده حقوق، ۱۳۹۴