شنود ارتباطات الکترونیک در حقوق کیفری ایران

حمید بهره‌مند،* امیرحسین جلالی فراهانی**

تاریخ دریافت ۱۳۹۲/۲/۳	تاریخ پذیرش ۱۳۹۲/۱۰/۱۰

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 دربرمی‌گیرد که در بستر مبادلات الکترونیک جریان دارند. گرچه از هنگام به رسمیت‌یافتن 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. مقاله حاضر با بررسی عناصر تشکیل‌دهنده جرم شنود و بررسی مستندات قانونی این حوزه با تأکید بر ماده (۷۳۰) قانون مجازات اسلامی، این نتیجه را اخذ می‌کند که مقررات موجود از جامعیت مناسبی برخوردارند، لکن در تعیین پاسخ‌های کیفری می‌توان با اصلاحاتی بازدارندگی قوانین را افزایش داد.

کلیدواژه‌ها: شنود؛ محتوای رایانه‌ای؛ ارتباطات غیرعمومی؛ قانون جرایم رایانه‌ای

---

* استادیار دانشکده حقوق و علوم سیاسی، دانشگاه تهران (نویسنده مسئول)؛
Email: bahrmand@ut.ac.ir
** کارشناس ارشد حقوق کیفری و جرم‌شناسی؛ دانشکده حقوق، دانشگاه امام صادق (ع)؛
Email: jalalyfarahany1979@gmail.com

مقدمه

حریم خصوصی[1] یکی از نمادهای نمایان و برجسته حقوق بنیادین[2] بشری است. هر شخص حق دارد از حریم خلوت خویش بهره‌مند باشد و اطلاعات آن را از دسترس نامحرمان دور نگاه دارد. تعرض به حریم اشخاص و تجسس و تفحص اطلاعات شخصی و خصوصی آنها می‌تواند بسیار ناگوار باشد و چه‌بسا آنان را برای همیشه از جامعه متنفر و رویگردان سازد. حریم خصوصی ملجأ و مجالی است برای با خود بودن و آنهایی که تنها می‌خواهیم با آنها باشیم و بازداشتن فرد از چنین حقی، به معنای نادیده انگاشتن آزادی اراده و از بین بردن حیثیت و حرمت اوست.

به‌طورکلی، برای حریم خصوصی پنج شاخه اصلی در نظر گرفته می‌شود: حریم خصوصی جسمانی، منزل، محل کار، اطلاعات و ارتباطات. قوانینی که به‌منظور صیانت و حمایت فراگیر از حریم خصوصی اشخاص به تصویب می‌رسند نیز همین پنج شاخه را مبنای قاعده‌گذاری خویش قرار داده‌اند.[3] لیکن در گذر زمان و به‌ویژه در نیم‌سده اخیر، در پی دستیابی بشر به فناوری‌ها و همچنین نوآوری در سبک زندگی‌اش، با دگرگونی‌های کم و بیشی در گستره و گونه‌های مشمول هریک از شاخه‌های پنج‌گانه حریم خصوصی‌اش روبه‌رو شده که از تأثیرپذیرترین آنها حریم خصوصی اطلاعات و ارتباطات اشخاص، آن هم در پی دستیابی به فناوری‌های اطلاعاتی (رایانه‌ای) و ارتباطی (مخابراتی) بوده است.

درباره حریم خصوصی ارتباطات، آگاهی ناروا از ارتباطات انسانی، از ارتباطات چهره‌به‌چهره تا پستی و مخابراتی، همواره به‌عنوان یک رفتار سرزنش‌آمیز ازسوی جوامع شناخته می‌شده، تا حدی که علاوه‌بر تأکید به آن در موازین دینی،[4] در زمره حقوق بنیادین ملت‌ها در

---

1. Privacy
2. Fundamental Rights

۳. در لایحه مسترد حریم خصوصی که پس از مدتی به‌صورت طرح ازسوی گروهی از نمایندگان مجلس هفتم به مجلس شورای اسلامی تقدیم و تاکنون مسکوت مانده، همین پنج شاخه مبنا قرار گرفته است.

۴. استراق سمع یکی از مصادیق تجسس است که قرآن کریم به حکم صریح آن را منع کرده است (حجرات: ۱۲). برای مطالعه بیشتر درخصوص مبانی فقهی منع شنود نک: بای و پورقهرمانی، ۱۳۸۸: ۲۲۲.

قانون اساسی کشورها نیز محترم شمرده شده است.[۱] ولی برخلاف چنین صراحتی در منشورهای وفاق ملی، در قوانین عادی همه کشورها، جنبه‌ها و جلوه‌های گوناگون این حق به یک اندازه تبیین و برای موارد نقض آنها ضمانت اجرایی پیش‌بینی نشده است تا شهروندان بتوانند با اطمینان برای استیفای حق خویش تظلم‌خواهی کنند و کارهای تقنینی بسیاری باید صورت گیرد تا این حق جایگاه واقعی خویش را بیابد (بهره‌مند و جلالی فراهانی، در دست چاپ).

نخستین گام برای رسیدن به چنین هدفی، شناسایی گستره و نمونه‌های مشمول حریم خصوصی ارتباطات الکترونیک است. اساساً منظور از ارتباطات الکترونیک[۲] چیست؟ آیا همان ارتباطات مخابراتی[۳] سنتی که گفتگوی تلفنی اشخاص را به شکل آنالوگ پشتیبانی می‌کردند، تعریف جامع‌الشمولی برای دوران امروزی هم به‌شمار می‌آید یا باید در مفهوم و گستره آن بازنگری کرد؟ آیا داده‌های متنی، صوتی، تصویری یا ترکیبی از آنها که با خطوط بی‌سیم یا سیمی الکترونیک ارسال می‌شوند، در زمره حریم خصوصی ارتباطی قرار می‌گیرند؟

دستاورد چنین بحثی می‌تواند حساس و تعیین‌کننده باشد. ترسیم قلمرو حریم خصوصی به

---

۱. در متمم قانون اساسی مشروطه، مصوب ۲۹ شعبان ۱۳۲۵، اصول مختلفه‌ای به جنبه‌های گوناگون حریم خصوصی اختصاص‌یافته بودند که اهمیت و حساسیت موضوع را نزد قانونگذاران مشروطه نشان می‌دهد. در اصل نهم این قانون آمده بود: «افراد مردم از حیث جان و مال و مسکن و شرف محفوظ و مصون از هرنوع تعرض هستند و متعرض احدی نمی‌توان شد، مگر به حکم و ترتیبی که قوانین مملکت معین می‌نماید». همچنین، اصل سیزدهم درباره حریم منزل اشعار می‌داشت: «منزل و خانه هرکس در حفظ و امان است، در هیچ مسکنی قهراً نمی‌توان داخل شد، مگر به حکم و ترتیبی که قانون مقرر نموده». اصول بیست‌ودوم و بیست‌وسوم این قانون نیز در حمایت از حریم ارتباطات پستی و تلگرافی چنین مقرر کرده بودند: «کلیه مراسلات پستی محفوظ و از ضبط و کشف مصون است، مگر در مواردی که قانون استثناء می‌کند». «افشا یا توقیف مخابرات تلگرافی بدون اجازه صاحب تلگراف ممنوع است، مگر در مواردی که قانون معین می‌کند». یادآور می‌شود در قانون اساسی جمهوری اسلامی ایران، اصل بیست‌ودوم حکم مشابه اصل نهم قانون اساسی مشروطه را بیان می‌دارد و اصل بیست‌وپنجم به شکل جامع‌تر و نوآورانه‌تر از حریم ارتباطاتی شهروندان حمایت می‌کند: «بازرسی و نرساندن نامه‌ها، 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».

2. Electronic Communication

3. Telecommunication

این معناست که هرگونه تعرض و دست‌یازی غیرمجاز به آن، باید با واکنش و اعمال ضمانت اجرا همراه باشد که با توجه به زیان‌بار بودن آن، عموماً ضمانت اجراهای کیفری سخت و سنگینی پیش‌بینی می‌شود. لذا نه تنها در ترسیم این قلمرو، بلکه در تعریف ویژگی‌ها و شرایط داده‌ها و اطلاعات مربوط و موجود در آن باید احتیاط بسیار کرد تا جریان آزاد اطلاعات[1] و آزادی اطلاعات[2] به خطر نیفتد و افراد به‌طور ناروا از حق بنیادی دیگر خویش، یعنی آگاهی و دانستن بازنمانند و بدتر از آن با ضمانت اجراهای سخت کیفری روبه‌رو نشوند.

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 یابند که آنها را به‌عنوان گیرنده مجاز می‌شناسد. پس از آن و درصورت ذخیره شدن اطلاعات در یک یا چند سامانه، از قلمرو حریم ارتباطی به قلمرو حریم اطلاعاتی وی راه می‌یابند که با اینکه همچنان آنها را سزاوار صیانت و احترام می‌داند، اما دیگر به اندازه حالتی نیست که مشمول حریم ارتباطی‌اش می‌شدند.[3]

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 به‌دلیل قرار گرفتن در چنین موقعیتی از مزایای محرمانگی برخوردار می‌شود. اما در حریم خصوصی اطلاعاتی، نوع اطلاعات مهم است و بنابراین کوشش می‌شود از آن

---

1. Free Flow of Information
2. Freedom of Information
۳. از جمله جرایمی که حریم اطلاعاتی اشخاص را نقض می‌کند، دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای و مخابراتی، موضوع ماده (۷۲۹) قانون مجازات اسلامی است.

تعریف روشن و مشخصی به‌عمل آید، مانند اطلاعات شخصی[1] در برابر اطلاعات عمومی[2] و تقسیم‌بندی اطلاعات شخصی به عادی و حساس[3] (انصاری، ۱۳۸۶: ۳۱۷).

به‌این‌ترتیب، روشن است که قانونگذاران کشورها برای حریم خصوصی ارتباطی شهروندانشان اهمیت به مراتب بالاتری قایل می‌شوند و با موارد نقض و تعرض به آنها به‌طور جدی‌تری برخورد می‌کنند. با توجه به اهمیت موضوع، در این نوشتار، جرم شنود غیرمجاز ارتباطات الکترونیک، مقرر در ماده (۷۳۰) قانون مجازات اسلامی برگزیده شده که از جهاتی می‌توان مهم‌ترین اقدام قانونگذار ایرانی در برخورد قاطع کیفری با انواع سوءاستفاده‌های رواج‌یافته در این عرصه به‌شمار آورد.

به همین منظور، نخست پیشینه این جرم در ادبیات تقنینی کشورمان بررسی و تحلیل می‌شود. سپس با گام نهادن در عناصر تشکیل‌دهنده این جرم، رفتاری که به‌صورت موجز و در یک کلمه ازسوی قانونگذار بیان شده، تبیین و دامنه شمول آن مشخص می‌شود. هرچند برای دستیابی به دستاورد مطلوب بنابر موضوع و شرایط و اوضاع و احوال این جرم به‌ترتیب در مطالب بعدی آمده است. پس از بررسی نتیجه‌محور یا مطلق بودن این جرم و عنصر روانی آن، به کیفر مقرر برای هریک از حالات و به‌ویژه کیفیات مشدده‌ای که می‌تواند متوجه مرتکبان باشد، اشاره می‌شود.

سرانجام در پرتو بررسی‌ها و تحلیل‌های به‌عمل آمده، میزان کامیابی قانونگذار در پاسخ‌گویی به نیازهای کاربران ارتباطات الکترونیک ایرانی در صیانت از حریم ارتباطی‌شان، ارزیابی و پیشنهادهای لازم برای رسیدن به جامعیت و بازدارندگی مطلوب مطرح می‌شود. توضیح آنکه در این نوشتار به ادبیات حقوق کیفری تطبیقی که ازسوی قانونگذار در تدوین قانون جرایم رایانه‌ای مورد استناد قرار گرفته، به‌ویژه کنوانسیون جرایم سایبر شورای اروپا، مصوب ۲۰۰۱، حسب مورد اشاره شده و نکات مربوط به آنها آمده است.

---

1. Personal Information
2. Public Information
3. Sensitive Personal Information

۱. پیشینه قانونی

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 وسائل 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. درصورت 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».[۱]

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، درصورت روزآمد شدن آن آیین‌نامه ازسوی وزارت مذکور، می‌تواند سوءاستفاده‌های نوین مخابراتی را هم دربرگیرد و مشمول ضمانت اجرای آن شود. به‌ویژه آنکه یکی از وظایف اصلی این وزارتخانه به‌موجب 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 اشخاص‌حقیقی و حقوقی طبق قانون» عنوان شده است که انتظار می‌رود وزارتخانه مقررات لازم‌الاجرا را ازسوی کمیسیون تنظیم مقررات ارتباطات به تصویب برساند.

---

۱. گفتنی است هرچند ماده (۶۶۰) قانون مجازات اسلامی هم به «استفاده غیرمجاز» از تلفن اشاره می‌کند، لکن مصادیق این ماده مربوط به جایی است که فردی «بدون پرداخت حق انشعاب و اخذ انشعاب» از خطوط تلفن متعلق به دیگری، اعم از اشخاص و شرکت مخابرات، استفاده کند، درحالی‌که در تبصره «۱» ماده (۱۴) مذکور ارتکاب جرم مربوط به وسایلی است که مرتکب «در اختیار» دارد.

پیشینه قانونی دیگر، ماده (۵۸۲) قانون مجازات اسلامی[۱] است: «هریک 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 افشا نماید، به حبس از یک سال تا سه سال یا جزای نقدی از شش تا هیجده میلیون ریال محکوم خواهد شد».[۲]

این ماده بیش از آنکه ناظر به امور پستی باشد، به امور مخابراتی مربوط می‌شود و بنابراین، با توجه به تعریف گسترده‌ای که از مخابرات در نصوص قانونی آمده، به‌خوبی شامل سوءاستفاده‌های نوین هم می‌شود و در مقام اعمال قوانین جدیدی مانند قانون جرایم رایانه‌ای، باید دامنه شمول آن را مدنظر قرار داد. این مهم در قسمت ضمانت اجراهای مقرر برای این جرم خواهد آمد.

همان‌طور که ملاحظه می‌شود، قوانین برشمرده، به‌ویژه ازلحاظ دربرگرفتن مرتکبان بالقوه این‌گونه سوءاستفاده‌ها، نارسایی‌های جدی داشتند و از جامعیت لازم برخوردار نبودند. حال باید دید ماده (۷۳۰) قانون مجازات اسلامی تا چه حد توانسته نیازهای قانونی این حوزه را در حمایت از حریم ارتباطی شهروندان برآورده کند. این ماده مقرر می‌دارد: «هرکس به‌طور غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری را شنود کند، به حبس از شش‌ماه 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».

---

۱. لازم به ذکر است این ماده جایگزینی برای ماده (۶۴) قانون مجازات اسلامی مصوب ۱۳۶۲ است که خود جایگزینی برای ماده (۱۶) قانون تشکیل شرکت پست جمهوری اسلامی ایران محسوب می‌شود.

۲. قانون رسیدگی به تخلفات اداری، مصوب ۱۳۷۲، این رفتار را تخلف اداری نیز برشمرده و برای آن تنبیه اداری در نظرگرفته است: «ماده (۸). تخلفات اداری به قرار زیر است:... ۳۱. توقیف، اختفا، بازرسی یا باز کردن پاکت‌ها و محمولات پستی یا معدوم کردن آنها و استراق سمع بدون مجوز قانونی».

۲. رفتار مجرمانه

متن ماده (۷۳۰) موجز تنظیم شده و قانونگذار از بیان عبارات توصیفی یا توضیحی پرهیز کرده است. حال باید دید در پرتو سایر قوانین و مقررات و قواعد حاکم بر تفسیر احکام کیفری، واژگان و مفاهیم این ماده را می‌توان به‌گونه‌ای تبیین کرد که رویکرد قانونگذار را تأمین کند یا خیر.

تنها واژه‌ای که در این ماده برای نمایان کردن رفتار موردنظر قانونگذار آمده، «شنود» است. 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.

قانونگذار پیش‌تر در قوانین عبارت «استراق سمع» را به‌کار برده است (ماده ۵۸۲ قانون مجازات اسلامی). فرهنگ‌های واژگان فارسی در تعریف این عبارت آورده‌اند: «شنود، پنهانی گوش‌کردن سخنان دیگران بدون آگاهی و رضایت آنها یا مستقیم و یا غیرمستقیم از راه دستگاه‌های مخابراتی» (دهخدا، ۱۳۸۹). تعریف دانشنامه‌ای این عبارت به‌خوبی مفهوم منفی شنود را بازتاب می‌دهد. لیکن پرسش اینجاست که چرا قانونگذار جرایم رایانه‌ای، همین عبارت را به‌کار نبرده و واژه شنود را جایگزین آن کرده است؟ به‌نظر می‌رسد پیدایش جنبه‌ها و ویژگی‌های فناورانه و نوآورانه در ارتکاب این جرم، قانونگذار را بر آن داشته تا از مفهوم سنتی‌اش فاصله بگیرد و واژه مناسب‌تری را جایگزین آن کند که با توجه به کاربردش در عرف، امکان تسری آن به سایر موضوعات هم وجود داشته باشد.

معادل استراق سمع در زبان لاتین، Eavesdropping است که در دانشنامه‌ها برایش معنای شنیدن پنهانی فیزیکی یا حتی به‌وسیله ابزارهای مخابراتی آمده است (همان؛ گارنر،[1] ۱۹۹۹: ۵۲۹).

1. Garner

اما در قوانین جرایم رایانه‌ای سایر کشورها و همچنین کنوانسیون جرایم سایبری شورای اروپا،[۱] واژه Interception به‌کار رفته که معنای واژگانی آن عبارت است از مانع شدن یا جلوگیری کردن از جریان یافتن یا رسیدن به مقصد خود، مانند موشک، موج رادیویی یا هواپیما. اما معنای حقوقی آن همان است که برای Eavesdropping آمده است[۲] (گارنر، ۱۹۹۹: ۸۱۵).

به‌نظر می‌رسد دلیل اصلی جایگزینی این واژه با گزینه سنتی خود، دگرگونی شیوه ارتکاب آن است. در پی یکپارچگی فناوری‌های اطلاعاتی و ارتباطاتی و تبدیل اصوات به داده‌ها و انتقال بسته‌ای آنها[۳] بین ابزارها و در شبکه‌های ارتباطی دیگر، شاید بتوان گفت در بیشتر موارد، امکان شنود آنها به شکل استراق سمع سنتی وجود ندارد و باید آن بسته‌ها را یک سامانه رایانه‌ای با کارکرد مخابراتی دریافت و به شکل درک‌شدنی تبدیل کند. به بیان دیگر، آنچه جابه‌جا می‌شود، صوت خالص نیست تا صرف به‌کارگیری حس شنوایی درک‌شدنی باشد، بلکه فناوری‌های ارتباطی به گونه‌ای دگرگون شده‌اند که در برخی بسترهای ارتباطی صوت را به مجموعه‌ای از داده‌ها تبدیل و پس از رسیدن به سامانه مقصد، دوباره پردازش و به شکل صوت بازپخش می‌کنند.[۴]

---

۱. «ماده (۳) شنود غیرقانونی[غیرمجاز]: هریک از اعضا باید به‌گونه‌ای اقدام به وضع قوانین و سایر تدابیر کنند که درصورت لزوم براساس حقوق داخلی خود، شنود عمدی و بدون حق داده‌های رایانه‌ای در حال انتقال غیرعمومی را که با ابزارهای فنی ایجاد شده‌اند و از سیستم‌های رایانه‌ای ارسال شده یا در میان آنها جریان دارند، جرم‌انگاری کنند. همچنین گسیل‌های امواج الکترومغناطیسی از یک سیستم رایانه‌ای که این‌گونه داده‌های رایانه‌ای را انتقال می‌دهند نیز دربرمی‌گیرد. اعضا می‌توانند مقرر دارند این جرم درصورتی محقق می‌شود که قصد ناروایی وجود داشته یا سیستم رایانه‌ای به سیستم رایانه‌ای دیگری متصل باشد» (جلالی فراهانی، ۱۳۸۹: ۲۸).

۲. علاوه‌بر این، واژه Wiretapping نیز در ادبیات حقوقی و قانونی نیز کاربرد دارد و به معنای استراق سمع مکانیکی یا الکترونیکی است که معمولاً به‌وسیله مجریان قانون و به‌موجب دستور مقام قضایی انجام می‌شود تا مکالمات خصوصی اشخاص شنود شود (گارنر، ۱۹۹۹: ۱۵۹۴).

3. Packet Data

۴. در آغاز، این موضوع آنچنان مورد توجه قرار گرفت که در ادبیات حقوقی کشورمان، به‌جای شنود غیرمجاز، تعبیر قطع غیرمجاز به‌کار رفت (دبیرخانه شورای عالی انفورماتیک کشور، ۱۳۷۶: ۱۳۹).

به‌این‌ترتیب، واژه شنود به‌کار رفته در این متن دلالت بر «دریافت» محتوا دارد و نه «درک شدن» آن به شکل شنیدن یا با حواس دیگر.[۱] برای «دریافت» محتوا به این شکل نیز باید آن را از مسیر اصلی خود خارج و به سامانه‌ای 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 به‌کار رفته است.[۲]

دلیل دیگر برگزیدن Interception به‌جای Eavesdropping، مطلق بودن مفهوم «محتوا»ست. محتوا تنها شامل داده‌های شنیداری نمی‌شود و همه انواع آن، مانند دیداری ـ شنیداری، نوشتاری یا ترکیبی از آنها را دربرمی‌گیرد. لذا دریافت یک محتوای نوشتاری رایانه‌ای، مانند رایانامه یا پیامک، با رعایت سایر شرایط و اوضاع و احوال می‌تواند رفتار مشمول این ماده را محقق سازد.

رفتار لازم برای تحقق جرم شنود ممکن است به‌طور آنی یا در طول زمان ارتکاب یابد. برای مثال، شخصی که در یک بازه زمانی کوتاه، داده در حال جریانی مانند یک پیامک را دریافت می‌کند، مرتکب جرمی آنی شده است. اما اگر همین دریافت داده در بازه زمانی طولانی صورت گیرد، جرم مستمری شکل خواهد گرفت؛ مانند آنکه شخصی با کارگذاشتن تجهیزات در یک بازه زمانی طولانی ارتباطات مخابراتی دیگری را شنود کند.

۳. موضوع جرم

در ماده (۷۳۰) قانون مجازات اسلامی، واژه «محتوا» به‌کار رفته است. منظور از محتوا چیست و چه نوع داده‌هایی را دربرمی‌گیرد؟ در ماده (۱) لایحه جرایم رایانه‌ای، «داده محتوا» چنین

---

۱. در لایحه قانون جرایم رایانه‌ای، در کنار شنود، دریافت نیز آمده بود (مرکز پژوهش‌های مجلس، ۱۳۸۷: ۳).

۲. برای مثال، بوینده‌ها (Sniffers) قطعه‌های سخت‌افزاری یا نرم‌افزاری‌اند که به‌طور خاص برای شنود در یک شبکه طراحی می‌شوند. نفوذگران رایانه‌ای بیشتر برای گردآوری گذرواژه‌ها این ابزار را به‌کار می‌گیرند تا بتوانند آن را در دسترسی‌های غیرمجاز خویش به‌کار برند (کیسی، ۱۳۸۶: ۴۴).

تعریف شده بود: «ب) داده محتوا: هر نمادی از موضوع‌ها، مفهوم‌ها یا دستورالعمل‌ها نظیر متن، صوت یا تصویر، چه به‌صورت در جریان یا ذخیره شده که به‌منظور برقراری ارتباط میان سیستم‌های رایانه‌ای یا پردازش توسط شخص یا سیستم رایانه‌ای به‌کار گرفته شده و به‌وسیله سیستم رایانه‌ای ایجاد شود».[۱] همچنین، لایحه داده رایانه‌ای و اطلاعات را نیز در همین ماده تعریف کرده بود: «الف) داده رایانه‌ای: هر نمادی از واقعه، اطلاعات یا مفهوم به شکلی مطلوب برای پردازش در یک سیستم رایانه‌ای یا مخابراتی است که باعث می‌شود سیستم‌های ذکر شده کارکرد خود را به مرحله اجرا گذارند ... د) اطلاعات: عبارت است از داده‌های پردازش شده قابل فهم برای انسان یا سیستم‌های رایانه‌ای یا مخابراتی».[۲] همان‌طور که دیده می‌شود، در این تعریف به پیروی از کنوانسیون جرایم سایبر شورای اروپا، ویژگی بارز داده رایانه‌ای «مناسب بودن برای پردازش» در نظر گرفته شده بود.[۳]

بااین‌حال، هنگامی که این تعاریف در کنار یکدیگر قرار گرفتند، نه تنها رافع ابهام نبودند، بلکه در کنار سایر تعاریف قانونی،[۴] بر ابهام‌های موجود هم می‌افزودند و به همین دلیل، قانونگذار آنها را حذف و تنها به مواردی بسنده کرد که ثمره عملی بر آنها مترتب

---

۱. در آیین‌نامه ساماندهی و توسعه رسانه‌ها و فعالیت‌های فرهنگی دیجیتال، مصوب مرداد ۱۳۸۹ هیئت وزیران، تعریف دیگری از محتوا ارائه شده است: «ماده (۱) ... الف) محتوا: مواد دیداری، شنیداری، نوشتاری یا ترکیبی از آنها در هر شکل و قالب».

۲. در پرتو این تعریف، ضرورتی به دیجیتالی یا صفرویکی بودن داده‌ها نیست و قالب آنالوگ آنها را نیز دربرمی‌گیرد.

۳. «ماده (۱) ... ب) «داده رایانه‌ای» هرگونه نماد حقایق، اطلاعات یا مفاهیم به شکلی مناسب برای پردازش در یک سیستم رایانه‌ای است که شامل برنامه‌ای می‌شود که برای کارکرد یک سیستم رایانه‌ای مناسب است». توضیح آنکه در این کنوانسیون، «اطلاعات» تعریف نشده است.

۴. بند «الف» ماده (۲) قانون تجارت الکترونیکی مقرر می‌دارد: ««داده پیام» (Message Data): 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». همچنین، بند «الف» ماده (۱) قانون انتشار و دسترسی آزاد به اطلاعات، مصوب ۱۳۸۸، «اطلاعات» را چنین تعریف کرده است: «هر نوع داده که در اسناد مندرج باشد یا به‌صورت نرم‌افزاری ذخیره گردیده و یا با هر وسیله دیگری ضبط شده باشد».

است. لذا می‌توان چنین نتیجه‌گیری کرد که دست‌کم سه واژه اطلاعات، داده و محتوا تفاوتی با یکدیگر ندارند و مفهوم واقعی و کاربردی آنها را باید در چارچوب بحث جستجو کرد. برای مثال، در چارچوب حریم خصوصی ارتباطی، داده‌ها به دو بخش داده محتوا و داده ترافیک تقسیم می‌شوند.

طبق تبصره «۱» ماده (۷۶۰) قانون مجازات اسلامی، داده‌های ترافیکی «هرگونه داده‌ای است که سامانه‌های رایانه‌ای در زنجیره ارتباطات رایانه‌ای و مخابراتی تولید می‌کنند تا امکان ردیابی آنها از مبدأ تا مقصد وجود داشته باشد. این داده‌ها شامل اطلاعاتی از قبیل مبدأ، مسیر، تاریخ، زمان، مدت و حجم ارتباط و نوع خدمات مربوطه می‌شود».[۱] این داده‌ها در پی جابه‌جایی محتوای ارتباطات رایانه‌ای و مخابراتی به‌طور خودکار ایجاد می‌شوند و کاربر رایانه در پیدایش آنها نقشی ندارد و سامانه در پی برقراری و انجام یک ارتباط رایانه‌ای و مخابراتی، چنین داده‌هایی را تولید و ذخیره می‌کند. برای مثال، هنگامی که یک ارتباط مخابراتی برقرار می‌شود، محتوای ارتباط، همان گفتار یا نوشتاری است که مخابره می‌شود، اما داده‌های ترافیکی شامل آن بخش از اطلاعاتی می‌شود که وضعیت آن ارتباط را نشان می‌دهد، مانند مدت ارتباط، زمان ارتباط، شماره‌های مبدأ و مقصد و حتی گره‌های[۲] ارتباطی که حسب مورد روی سامانه ارتباطی کاربر یا مسیریاب‌های[۳] ارائه‌دهنده خدمات ارتباطی تولید و ذخیره می‌شود.

دلیل اصلی جداسازی این دو گونه داده‌ها در پرتو مباحث حریم خصوصی ارتباطات، آن‌گونه که در گزارش توجیهی کنوانسیون جرایم سایبر شورای اروپا آمده، کمتر تعرض‌آمیز بودن دسترسی به داده‌های ترافیکی برخلاف داده محتواست. به همین دلیل در

---

۱. در ماده (۱) کنوانسیون جرایم سایبری شورای اروپا آمده است: «ت) «داده ترافیک» داده رایانه‌ای است که به ارتباط برقرار شده به‌وسیله سیستم رایانه‌ای مربوط می‌شود. این داده را سیستم رایانه‌ای ایجاد می‌کند که بخشی از زنجیره ارتباطی را تشکیل داده است و مبدأ، مقصد، مسیر، زمان، تاریخ، اندازه، مدت، یا نوع خدمات ارائه شده را نشان می‌دهد».

2. Nodes
3. Routers

این سند به‌جای شنود داده ترافیک، تعبیر «گردآوری زنده»[1] به‌کار رفته که به‌خوبی نگاه متفاوت تدوین‌کنندگان را به این دو گونه داده‌ها نشان می‌دهد. این موضوع به‌ویژه از باب اقدامات مجریان قانون در کشف و شناسایی جرایم و مجرمان سایبری اهمیت دارد و به همین دلیل، تفکیک مزبور در بخش شکلی کنوانسیون به‌عمل آمده است.[2]

با توجه به این توضیحات، پرسش اینجاست که آیا داده‌های ترافیک مشمول مفهوم «محتوای» برشمرده در ماده (۷۳۰) قانون مجازات اسلامی می‌شوند؟ واقعیت این است که داده‌های ترافیک در تعریف محتوای رایانه‌ای می‌گنجند و از آن بیرون نیستند و آن‌گونه که اشاره شد، مبنای تفکیک آنها، تعرض‌آمیزی کمتر دسترسی به آنها در مقایسه با محتوای در حال انتقال ارتباطات رایانه‌ای است. لذا برپایه تفسیر ادبی و فنی (مبتنی‌بر حریم خصوصی ارتباطی) می‌توان گفت داده‌های ترافیک مشمول داده محتوا می‌شوند و بنابراین

---

1. Real Time Collection

۲. در گزارش توجیهی کنوانسیون چنین آمده است: «۲۱۰. در بسیاری از کشورها، میان شنود زنده داده محتوا و جمع‌آوری زنده داده ترافیک درخصوص پیش‌شرط‌های قانونی لازم جهت صدور مجوز تدبیری مانند تحقیق و جرایمی که می‌توان برای آنها این تدبیر را به‌کار برد، تفکیک قائل شده‌اند. با اینکه نسبت به هر دو نوع داده مذکور، منافع مربوط به حریم خصوصی رسمیت یافته است، اما بسیاری از دولت‌ها به این نکته توجه کرده‌اند که منافع حریم خصوصی ناشی از داده محتوا، به‌دلیل ماهیت محتوا یا پیام ارتباطی بیشتر است. ازاین‌رو، ممکن است جمع‌آوری زنده داده محتوا در مقایسه با داده ترافیک محدودیت‌های بیشتری داشته باشد. این کنوانسیون، به‌منظور کمک به کشورهایی که چنین تمایزی را رسمیت بخشیده‌اند، هرچند ازلحاظ اجرایی اذعان می‌شود که جمع‌آوری یا ضبط داده‌ها در هر دو موقعیت امکان‌پذیر است، اما ازلحاظ هنجاری، در عنوان‌های این دو ماده برای جمع‌آوری داده ترافیک از «جمع‌آوری زنده» و برای جمع‌آوری داده محتوا از «شنود زنده» استفاده کرده است. ۲۱۱. در بعضی کشورها، قوانین موجود تفاوتی بین جمع‌آوری داده ترافیک و شنود داده محتوا قائل نشده‌اند، شاید به این دلیل که در قوانین مربوط به تفاوت‌های منافع حریم خصوصی اشاره نشده یا این‌که فنون جمع‌آوری فناورانه هر دو نوع داده بسیار مشابه‌اند. بنابراین، پیش‌شرط‌های قانونی لازم جهت کسب مجوز انجام این تدابیر و جرایمی که برای آنها می‌توان این تدابیر را اتخاذ کرد، همانند یکدیگرند. این وضعیت نیز در کنوانسیون پذیرفته شده و تعبیر «جمع‌آوری یا ضبط» در متن اصلی هر دو ماده (۲۰) و (۲۱) در مفهوم کاربردی معمول آمده است» (جلالی فراهانی، ۱۳۸۹: ۸۳).

شنود آنها پیرو شرایط ماده (۷۳۰) قانون مجازات اسلامی، جرم و قابل مجازات است.[۱]

نکته دیگری که باید درباره داده‌های رایانه‌ای تبیین شود، این است که آیا باید به شکل دیجیتالی، یعنی مبتنی‌بر صفرویک ذخیره و جابه‌جا شوند یا اینکه به شکل آنالوگ هم امکان جابه‌جایی آنها وجود دارد؟ به‌نظر می‌رسد توان سامانه‌های رایانه‌ای در پردازش دیجیتالی داده‌ها اهمیت دارد و جابه‌جایی آنها می‌تواند به دو شکل دیجیتال و آنالوگ صورت گیرد. به‌این‌ترتیب، صداهایی که با دستگاه‌های بی‌سیم موسوم به واکی‌تاکی جابه‌جا می‌شوند، می‌توانند موضوع جرم شنود قرار گیرند.

بااین‌حال، باید توجه داشت چنانچه تفسیر گسترده‌ای درباره مفهوم محتوا صورت پذیرد، ممکن است نتایج نامتعارفی حاصل شود. بر این اساس، هر صوت یا تصویری که در عالم بیرون وجود دارد، می‌تواند به‌وسیله سامانه‌های رایانه‌ای و مخابراتی دریافت، پردازش و ارسال شود. درحالی‌که آنها محتوای رایانه‌ای نیستند. لذا باید توجه داشت محتوایی داده به‌شمار می‌آید که با سامانه رایانه‌ای تولید شده و برای پردازش و ارسال مناسب است. اما درباره برون‌داد آن، هنگامی که به شکل پدیده‌ای فیزیکی نمایان می‌شود، دیگر داده نخواهد بود، مانند صوت یا تصویر یا متنی که از گوشی یا نمایشگر یا چاپگر رایانه پخش، نمایش یا چاپ می‌شود.

با توجه به این ملاحظات، در ماده (۷۳۰) قانون مجازات اسلامی علاوه‌بر محتوای رایانه‌ای، امواج الکترومغناطیسی هم موضوع شنود غیرمجاز در این ماده قرار گرفته‌اند. با توجه به تعریفی که از داده و محتوای رایانه‌ای ارائه شد، امواج الکترومغناطیسی یا رادیویی را دربرنمی‌گیرد و اینها ماهیت متفاوتی دارند. گرچه می‌توانند باعث جابه‌جایی داده‌ها و محتوای رایانه‌ای شوند و با دریافتشان می‌توان داده‌ها را بازسازی کرد (جلالی فراهانی، ۱۳۸۹: ۳۰). لذا ازآنجاکه امکان دریافت محتوا از امواج مذکور وجود دارد، بی‌آنکه آنچه دریافت شده ماهیت داده‌ای داشته باشد، قانونگذار جداگانه

---

۱. درباره زمینه‌های سوءاستفاده از داده‌های ترافیکی کاربران برای شنود ارتباطات الکترونیکی آنها، نک.: سازمان فناوری اطلاعات ایران، ۱۳۸۹، ج ۲: ۲۱۲.

و در کنار سامانه‌های رایانه‌ای و مخابراتی به آنها نیز اشاره کرده است. امواج نوری هم که ماهیتی الکترومغناطیسی دارند، باعث جابه‌جایی محتوا به‌وسیله فیبرهای نوری در شبکه‌های محدود[1] و گسترده[2] می‌شوند. لیکن در اینجا نیز به‌دلیل ناهمگون بودن این امواج با مفهوم داده رایانه‌ای، به‌طور جداگانه و در کنار آنها برشمرده شده‌اند. برای مثال، دستگاه‌های رادار نمونه‌ای از رسانه‌های الکترومغناطیسی‌اند که داده را جابه‌جا نمی‌کنند، بلکه برپایه بازگشت امواج گسیل شده، وجود اشیا را در فواصل گوناگون نشان می‌دهند. لذا دریافت آنها نیز مشمول ماده (۷۳۰) می‌شود.

شرط مهم دیگر 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 به‌عنوان 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 به‌شمار نمی‌آید 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[3] همه طرف‌های ارتباط غیرعمومی شرط است و چنانچه یکی از طرف‌ها 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.

در این خصوص، ضبط یا ذخیره‌سازی ارتباطات الکترونیک کارکنان سازمان‌ها

---

1. Local Area Network (LAN)
2. Wide Area Network (WAN)
۳. در حقوق مدنی این شکل از رضایت را اذن می‌نامند و در برابر، به رضایت پسینی اجازه گفته می‌شود.

ازسوی 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. بااین‌حال، چنین رضایتی نسبت به ارتباطات درون‌سازمانی پرسنل این مجموعه‌ها معتبر و قابل استناد خواهد بود و ارتباطات برون‌سازمانی آنها تنها درصورتی مجاز خواهد بود که پیشاپیش رضایت آن سوی ارتباط نیز گرفته شود.

برای زدودن وصف مجرمانه از چنین رفتارهایی، می‌توان پروتکلی را تعریف و اجرا کرد که برپایه آن پیش از آنکه مخاطب کلامش را آغاز کند یا محتوایش را به سامانه‌های پیام‌رسان[1] شرکت بفرستد، به‌طور خودکار پیامی پخش یا آشکار شود که هشدار دهد سامانه ارتباطی سازمان مجهز به ابزار شنود است و ادامه ارتباط ازسوی وی به‌منزله رضایتش خواهد بود. در غیر این صورت، رفتار ارتکابی با وجود سایر شرایط جرم تلقی می‌شود. لذا این فرض نیز قابل تصور است که یک یا چند تن از طرف‌های ارتباط، بدون داشتن رضایت طرف یا طرف‌های دیگر مرتکب چنین جرمی شوند.

همچنین در مواردی که شنود به ارتباطات میان دو یا چند سامانه یا اجزای یک سامانه (مانند چاپگر یا صفحه کلید با سامانه) برقرار می‌شود، رضایت مالک یا دارنده یا متصدی آنها، شرط مجاز بودن رفتار ارتکابی خواهد بود. گاهی مجوز قانونی، جای رضایت فردی را می‌گیرد و به رفتار ارتکاب‌یافته مشروعیت می‌بخشد. برای مثال، در جایی که یک مأمور قانونی ارتباط موضوع این ماده را با رعایت مقررات شنود می‌کند، نیازی به گرفتن رضایت نخواهد بود. این موضوع به‌ویژه در فنون تحقیقاتی ویژه‌ای مانند دام‌گستری[2] رواج دارد که در آن یک مأمور با معرفی خود به‌عنوان یک تبهکار یا بزه‌دیده بالقوه، با یک یا چند تن تبهکار ارتباط برقرار و هم‌زمان یک مأمور دیگر یا حتی خود وی ارتباط را شنود (دریافت) می‌کند.

---

1. Messaging System
2. Entrapment

نداشتن مجوز قانونی در امر تحقیق جرایم یا تخلفات هم می‌تواند به غیرمجاز بودن شنود بیانجامد. طبق ماده (۷۷۶) قانون مجازات اسلامی «شنود محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی مطابق مقررات راجع به شنود مکالمات تلفنی خواهد بود». دراین‌باره ماده (۱۰۴) قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور کیفری، مصوب ۱۳۷۸، قابل استناد است که مقرر می‌دارد: «در مواردی که ملاحظه، تفتیش و بازرسی مراسلات پستی، مخابراتی صوتی و تصویری مربوط به متهم برای کشف جرم لازم باشد قاضی به مراجع ذی‌ربط اطلاع می‌دهد که اشیاء فوق را توقیف نموده نزد او بفرستند، بعد از وصول آن را در حضور متهم ارائه کرده و مراتب را درصورت مجلس قید نموده و پس از امضاء متهم آن را در پرونده ضبط می‌نماید. استنکاف متهم از امضا درصورت مجلس قید می‌شود و چنانچه اشیاء مزبور حائز اهمیت نبوده و ضبط آن ضرورت نداشته باشد با اخذ رسید به صاحبش مسترد می‌شود».

۴. بستر ارتکاب جرم

در ماده (۷۳۰) قانون مجازات اسلامی، برای تبیین بستر ارتکابی شنود، واژه «ارتباطات» به‌کار رفته است. ارتباط در مفهوم عام، به معنای برقراری پیوند معنادار و هدفمند میان دو یا چند چیز است که می‌توانند انسان، سایر جانداران و اشیاء باشند. اما در مفهوم خاص، روابط پستی و مخابراتی متناظر آن شده که حسب مورد میان انسان‌ها با یکدیگر، انسان‌ها با سامانه‌ها و سامانه‌ها با یکدیگر برقرار می‌شود.

پرسشی که درباره شنود مقرر در این ماده مطرح می‌شود این است که کدام مفهوم از ارتباطات را مدنظر دارد؟ آیا هر شکل ارتباطات سامانه ـ سامانه، انسان ـ انسان و انسان ـ سامانه را دربرمی‌گیرد یا اینکه باید به مفهوم خاص آن برپایه مفهومی که از شنود ارتباطات از دیرباز در پیشینه قانونگذاری کشورمان و سایر کشورها وجود داشته بسنده کرد؟ به‌نظر می‌رسد ارتباطات بین اجزای یک سامانه را هم می‌توان مشمول این حکم دانست. برای

مثال، هنگامی که شخصی یک صفحه‌کلید بی‌سیم را برای وارد کردن داده‌های خود به‌کار می‌گیرد، آیا این ارتباط بی‌سیم مشمول این ماده می‌شود؟ حتی برخی دستگاه‌ها طراحی و تولید شده‌اند که با به‌کارگیری آنها در فاصله مناسب می‌توان تشعشعات کابل‌های سیمی را دریافت کرد و داده‌های آنها را به‌دست آورد. مؤید چنین دیدگاهی آمدن «سامانه‌های رایانه‌ای» در کنار «سامانه‌های مخابراتی» در ماده (۷۳۰) است که چنانچه تفسیری جز این داشته باشیم، آوردن آن ازسوی قانونگذار را باید کار بیهوده‌ای ارزیابی کرد.

افزون بر این کنوانسیون جرایم سایبری شورای اروپا هم به کشورهای عضو اجازه می‌دهد مفهوم ارتباطات را به وجود دو یا چند سامانه محدود کنند یا ارتباطات میان اجزای یک سامانه را نیز مشمول عنوان مجرمانه شنود بدانند.[۱] ضمن اینکه دلیلی وجود ندارد داده‌های در جریان میان اجزای یک سامانه از چنین حمایتی برخوردار نباشند. برای مثال، چنانچه شخصی در حال نگاشتن محتوای یک پیام رایانامه‌ای به‌وسیله صفحه‌کلید بی‌سیم خود باشد تا پس از پایان آن را برای گیرنده مورد نظرش بفرستد و در این اثنا دیگری آن را دریافت کند، آیا رفتار مرتکب را نباید شنود دانست و تنها باید به هنگامی محدود شود که در حال ارسال به‌وسیله سامانه پیام‌رسان الکترونیکش است؟

به‌علاوه، آنچه به این گستره به ظاهر گسترده قلمرو مشخص و معناداری می‌بخشد، قید «غیرعمومی» گنجانیده شده در ماده (۷۳۰) است. همان‌طور که در ادامه خواهد آمد، این قید به تنهایی بار معنایی مفهوم و گستره محرمانگی محتوای در حال انتقال ارتباطات در سامانه‌های رایانه‌ای و مخابراتی را دربرمی‌گیرد و خودبه‌خود دریافت محتواهایی که به‌طور عمومی پخش می‌شوند را از شمول این ماده بیرون می‌کند.[۲]

---

۱. ماده (۳) کنوانسیون جرایم سایبری.

۲. این بحث‌ها هنگامی جدی‌تر مطرح می‌شوند که این ماده در کنار ماده (۷۴۰) قانون مجازات اسلامی راجع به سرقت داده‌های رایانه‌ای مورد توجه قرار گیرند. در پرتو دیدگاه نخست، با عنایت به اینکه دو عبارت «غیرعمومی» و «غیرمجاز» یک معنا دارند، دریافت غیرمجاز هرگونه محتوای در حال انتقال رایانه‌ای را باید شنود و دریافت غیرمجاز هرگونه محتوای ذخیره ←

سرانجام، وجود حرف «در» پیش از سامانه‌های رایانه‌ای و مخابراتی، دریافت و ضبط هرگونه محتوا از محیط فیزیکی به‌وسیله ابزارهای الکترونیک را از شمول این ماده بیرون می‌کند. برای مثال، چنانچه دو یا چند نفر در حال گفتگو با یکدیگر باشند و دیگری صدای آنها را با تلفن همراه خویش دریافت کند، مرتکب شنود مقرر در ماده (۷۳۰) نشده است.[۱]

شرط لازم دیگر برای تحقق این جرم، «در حال انتقال بودن» محتوا دانسته شده است. لذا بازه زمانی شنود عبارت است از آغاز ارسال محتوا از سامانه رایانه‌ای یا مخابراتی مبدأ تا هنگام رسیدن و ذخیره شدن آن در سامانه مقصد یا با فرض پذیرش مفهوم موسع از ارتباطات، شامل زمان جابه‌جایی داده‌ها میان اجزای یک سامانه هم می‌شود. بنابراین، چنانچه مرتکب، داده‌های ذخیره شده در سامانه مبدأ یا مقصد را دریافت کند، مرتکب شنود نشده است. لیکن لزومی ندارد که ازسوی مخاطب آن دریافت و درک شده باشد. به بیان دیگر، صرف ذخیره شدن پیام و از حرکت ایستادن آن در مسیرهای ارتباطی بی‌سیم یا باسیم یا در یک سامانه، شرط لازم تحقق این جرم را از بین می‌برد.

فرض دیگر درباره در حال انتقال بودن داده‌ها، به موردی برمی‌گردد که مرتکب، دستگاه دریافت‌کننده داده‌ها از سامانه‌ها را در فاصله مناسبی قرار می‌دهد، مانند یک دوربین دیجیتال که از صفحه نمایشگر داده‌ها را ضبط می‌کند. آیا در چنین حالتی، رفتار وی می‌تواند شنود باشد؟ رسیدن به پاسخ مثبت هنگامی امکان‌پذیر است که داده‌های به نمایش درآمده بر روی نمایشگر را در حال انتقال انگاریم، البته در داخل سامانه و نه جلوه دیداری ـ شنیداری آن. در پرتو رویکرد موسع از ارتباطات، چنانچه این داده‌ها را میان

← شده را باید سرقت انگاشت. ضمن اینکه سیاق ماده (۷۴۰) چنین استدلالی را تأیید می‌کند. اما برپایه دیدگاه دوم، مبانی حمایت کیفری از حریم خصوصی ارتباطی و مالکیت از دارایی‌های رایانه‌ای و الکترونیکی اشخاص متفاوت است و بنابراین، در حال انتقال یا ذخیره بودن داده‌ها نباید مبنای ترسیم قلمرو قرار گیرد. لذا آن‌گونه که تبصره ماده (۷۷۶) تصریح دارد، شنود تنها به دریافت محتوای در حال انتقال محدود نمی‌شود و بر این اساس باید ماده (۷۳۰) اصلاح شود. ضمن اینکه سرقت نیز به داده‌های ذخیره شده محدود نمی‌شود و ممکن است نسبت به داده‌های در جریان ارتکاب یابد.

۱. این موضوع به‌ویژه در نظام حقوق رسانه‌ها و دریافت اخبار و اطلاعات اهمیت دارد. برای آگاهی بیشتر، نک.: انصاری، ۱۳۹۰: ۱۶۷.

اجزای یک سامانه در حال انتقال بدانیم، دریافت آنها می‌تواند شنود انگاشته شود؛ مگر اینکه در ماهیت داده‌ای آنها تشکیک شود. برای مثال، آیا محتوای صوتی در حال پخش از بلندگوی سامانه، داده رایانه‌ای به‌شمار می‌آید یا اینکه دیگر ماهیت داده را به‌دلیل ممکن نبودن پردازش مستقیم آن به‌وسیله سامانه‌های رایانه‌ای و مخابراتی ندارد و بنابراین، دریافت آن شنود محتوای رایانه‌ای انگاشته نمی‌شود؟ به‌نظر می‌رسد در چنین مواردی باید قایل به تفکیک شد و دریافت هر محتوایی را شنود ندانست و تنها به گزینه‌هایی بسنده کرد که محتوا ماهیت داده‌ای خویش را حفظ کرده باشد.

عنصر بسیار مهم دیگر شنود غیرمجاز، «غیرعمومی بودن» ارتباط[1] است. این شرط می‌تواند به تحدید گستره این جرم و روشن‌تر کردن مرزهای آن با سایر جرایم کمک کند. شکل‌های نخستین ابزارها و فناوری‌های مخابراتی و ارتباطی که عمدتاً در دستگاه‌های تلفن نمود یافته بودند، ارتباطات خصوصی[2] را رقم می‌زدند؛ به این معنا که تنها امکان حضور دو نفر و نه بیشتر در دو سوی خط ارتباطی فراهم بود. اما پس از پیدایش شبکه‌های ارتباطی و شکل‌گیری ارتباطات چندسویه میان افراد مختلف و حتی برگزاری گردهمایی‌ها و نشست‌های الکترونیک، این حوزه از آن جلوه خصوصی خویش فراتر رفته و شکل غیرعمومی یافته است.

به‌این‌ترتیب، ارتباط غیرعمومی به ارتباط خصوصی یا گروهی گفته می‌شود که همه اعضای شرکت‌کننده در آن نمی‌خواهند کسی بدون رضایت پیشینی از آنها از محتوای ارتباطی مبادله‌ای میان آنها آگاه شود. برای مثال، در محیط‌های گپ اینترنتی،[3] چندین نفر می‌توانند به‌طور هم‌زمان[4] یا غیرهم‌زمان با یکدیگر به گفتگو بپردازند. ورود شخص ثالث به این مجموعه و دریافت محتوای مبادله‌ای دیگران ازسوی وی باید با رضایت همگی آنها

1. Non-public Communication
2. Private Communication
3. Chat Room
4. Synchronous

همراه باشد، والا می‌تواند با جمع بودن سایر شرایط مشمول مجازات مقرر در این ماده شود.

نکته بسیار مهم درباره قید غیرعمومی بودن این است که به ارتباطات برمی گردد نه محتوا. به بیان دیگر، برای احراز این قید، باید بستر ارتباطی و نه محتوای در حال انتقال ارزیابی شود. برای مثال، در جایی که شخصی محتوای در حال پخش در تلویزیون کابلی را به طور غیرمجاز دریافت می‌کند، ممکن است مرتکب شنود شناخته شود؛ زیرا گرچه بینندگان این برنامه ها بسیارند، اما همگانی پخش نمی شوند و بنابراین واجد وصف عمومی نیستند.

۵. نتیجه جرم

همان‌طور که اشاره شد، رفتار مشمول این ماده بسیار مختصر و تنها در یک واژه نمایان شده که عبارت است از «شنود». لذا نتیجه آن نیز در خودش نهفته است، یعنی به‌محض دریافت محتوای در حال انتقال یک ارتباط غیرعمومی، شنود تحقق خواهد یافت (عالی‌پور، ۱۳۹۰: ۱۸۳). نکته حائز اهمیت این است که لزومی ندارد مرتکب در همان لحظه از مفاد محتوا آگاهی یابد و آن را درک کند. کما اینکه در شنود مکالمات تلفنی نیز عموماً ممکن است شنودگر هم‌زمان از مفاد مکالمه آگاه نشود و تنها به ضبط آن بسنده کند و در زمان دیگری برای آگاهی از آن مراجعه کند و حتی امکان دارد پیش از آگاهی تحت پیگرد قرار گرفته و دستگیر شود. همچنین ممکن است شنود به‌طور واقعی و زنده[1] صورت گیرد و مرتکب هم‌زمان از مفاد محتوای ارتباطی آگاهی یابد. لیکن آگاهی از محتوای در حال جریان شرط لازم برای تحقق نتیجه این جرم به‌شمار نمی‌آید و صرف دریافت محتوا، چه بالمباشره و چه بالتسبیب، برای تحقق نتیجه کافی خواهد بود.

1. Real Time

۶. عنصر روانی

رفتار مقرر در این ماده تنها درصورتی جرم و قابل مجازات انگاشته می‌شود که به‌طورعمدی ارتکاب یافته باشد. ممکن است دریافت محتوای در حال انتقال یک ارتباط غیرعمومی به‌طورغیرعمدی رخ دهد که درصورت اثبات چنین امری مرتکب، مجازات نخواهد شد. برای مثال، در ارتباطات بی‌سیم و حتی باسیم بسیار رخ می‌دهد که کانال‌های ارتباطی با یکدیگر آمیخته می‌شوند و فرد به‌طور ناخواسته محتوای ارتباطات دیگران را دریافت و درک می‌کند. نکته حائز اهمیت این است که از هنگام آگاهی از دریافت غیرمجاز محتوا باید فوراً آن را قطع کند والا عنصر معنوی مورد نیاز تحقق یافته است. به بیان دیگر، قصد مرتکب در ادامه دریافت داده‌های در حال انتقال یک ارتباط غیرعمومی می‌تواند عنصر روانی این جرم را محقق سازد.

۷. مجازات

طبق ماده (۷۳۰) قانون مجازات اسلامی، شنود غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی، شش‌ماه تا دوسال حبس یا جزای نقدی یا هر دو آنها را در پی دارد. آن‌گونه که پیداست، این کیفرها طیف گسترده‌ای را دربرمی‌گیرند که می‌توان چنین پنداشت قانونگذار خواسته است اختیار صلاحدیدی[1] کافی را به قاضی اعطا کند؛ چرا که این جرم برخلاف مختصر و مفید بودن، گونه‌های فراوان و گستره فراگیری را دربرمی‌گیرد که به همان نسبت می‌تواند آسیب‌ها و زیان‌های کم و زیادی را به بزه‌دیدگان وارد آورد. لذا برای تعیین یک مجازات اثربخش، متناسب و بازدارنده،[2] شرایط و ویژگی‌های طرف‌های ارتباط، محتوای در حال انتقال، آسیب‌های بالقوه یا بالفعل و انگیزه ارتکاب می‌توانند شاخص‌های مطلوب و قابل اتکایی باشند.

---

1. Judicial Discretionary Power
2. Efficient, Proportionate and Deterrent

درخصوص هم‌پوشانی کیفر مقرر در این ماده با سایر قوانین، نخست باید حکم مقرر در ماده (۷۳۱) قانون مجازات اسلامی مورد توجه قرار گیرد. چنانچه محتوای در حال انتقال شنودشده، داده‌های سری موضوع این ماده باشد، مرتکب به کیفر مقرر در آنجا محکوم خواهد شد.[۱] همچنین، ماده (۵۸۲) قانون مجازات اسلامی و بند «الف» ماده (۷۵۴) قابل توجه‌اند.[۲] بند «الف» به کارمندان و کارکنان اداره‌ها و سازمان‌ها یا شوراها یا شهرداری‌ها و مؤسسه‌ها و شرکت‌های دولتی یا وابسته به دولت یا نهادهای انقلابی و بنیادها و مؤسسه‌هایی که زیر نظر ولی‌فقیه اداره می‌شوند و دیوان محاسبات و مؤسسه‌هایی که با کمک مستمر دولت اداره می‌شوند یا دارندگان پایه قضایی و به‌طورکلی اعضا و کارکنان قوای سه‌گانه و همچنین نیروهای مسلح و مأموران به خدمت عمومی اعم از رسمی و غیررسمی اشاره دارد که به مناسبت انجام وظیفه مرتکب جرم رایانه‌ای شده باشند.

اما ماده (۵۸۲) تنها مستخدمان و مأموران دولت را مخاطب حکم خود قرار داده که برای آگاهی از دامنه شمول این مفهوم می‌توان به‌عنوان فصل سیزدهم قانون مجازات اسلامی (تعدیات مأموران دولتی نسبت به دولت) مراجعه کرد. با توجه به ماده نخست این فصل، یعنی ماده (۵۹۸)، ملاحظه می‌شود قانونگذار دقیقاً همان موارد مقرر در بند «الف»

---

۱. «ماده (۷۳۱) ـ هر کس به‌طور غیرمجاز نسبت به داده‌های سری در حال انتقال یا ذخیره شده در سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود، به مجازات‌های مقرر محکوم خواهد شد: الف) دسترسی به داده‌های مذکور یا تحصیل آنها یا شنود محتوای سری در حال انتقال، به حبس از یک تا سه سال یا جزای نقدی از بیست میلیون (۲۰،۰۰۰،۰۰۰) ریال تا شصت میلیون (۶۰،۰۰۰،۰۰۰) ریال یا هر دو مجازات».

۲. «ماده (۷۵۴) ـ در موارد زیر، حسب مورد مرتکب به بیش از دو سوم حداکثر یک یا دو مجازات مقرر محکوم خواهد شد: الف) هریک از کارمندان و کارکنان اداره‌ها و سازمان‌ها یا شوراها و یا شهرداری‌ها و مؤسسه‌ها و شرکت‌های دولتی و یا وابسته به دولت یا نهادهای انقلابی و بنیادها و مؤسسه‌هایی که زیر نظر ولی‌فقیه اداره می‌شوند و دیوان محاسبات و مؤسسه‌هایی که با کمک مستمر دولت اداره می‌شوند و یا دارندگان پایه قضایی و به‌طورکلی اعضاء و کارکنان قوای سه‌گانه و همچنین نیروهای مسلح و مأموران به خدمت عمومی اعم از رسمی و غیررسمی به مناسبت انجام وظیفه مرتکب جرم رایانه‌ای شده باشند».

ماده (۷۵۴) را برشمرده است.[۱] همچنین در آنجا قید «در غیر مواردی که قانون اجازه داده» آمده که به‌نظر می‌رسد ازلحاظ مفهوم و گستره با قید «به مناسبت انجام وظیفه» تفاوتی نداشته باشد. زیرا انتظار می‌رود همه کارکنان و کارمندان نهادهای موضوع بند «الف» برپایه قانون و البته آیین‌نامه‌های اجرایی پیرو آنها عمل می‌کنند.

لذا با توجه به شباهت موضوع و ارکان ماده (۷۳۰) و بند «الف» ماده (۷۵۴) با ماده (۵۸۲) در حوزه ارتباطات مخابراتی، به‌ویژه برپایه مفهوم فراگیری که از مخابرات به‌دست آمد، ماده (۵۸۲) در این موارد نسخ ضمنی شده و باید برپایه احکام جدید قانونگذار به موضوعات رسیدگی و حکم مقتضی را صادر کرد.

برای احراز تعدد در شنود غیرمجاز، شاخص‌های گوناگونی را می‌توان مورد توجه قرار داد: تفاوت خطوط ارتباطی، تفاوت طرف‌های ارتباط و تعداد دفعات شنود، هریک می‌توانند به احراز تعدد کمک کنند. برای مثال، چنانچه فرد در یک زمان محتوای در حال انتقال چند ارتباط غیرعمومی متعلق به یک فرد یا گروه یا افراد یا گروه‌ها یا یک محتوا را در بازه‌های زمانی یا به شیوه‌ها یا در بخش‌های متفاوت یا متعددی دریافت کند، می‌تواند مشمول احکام تعدد شود؛ زیرا طبق نص ماده (۷۳۰)، برای اینکه شنود غیرمجاز تحقق یابد، کافی است همه یا بخشی از محتوای یک ارتباط غیرعمومی در یک زمان دریافت شود و هرگونه تغییری در این شرایط می‌تواند موضوع را مشمول احکام تعدد کند.

سرانجام، مسئولیت کیفری اشخاص حقوقی در این جرم نیز باید مورد توجه قرار گیرد. این موضوع به‌ویژه از آن جهت اهمیت دارد که احتمال ارتکاب آن ازسوی مؤسسات، بنگاه‌ها و شرکت‌ها وجود دارد که به نمونه‌هایی از آنها نیز اشاره شد و

---

۱. ماده (۵۹۸) ـ «هریک از کارمندان و کارکنان ادارات و سازمان‌ها یا شوراها و یا شهرداری‌ها و مؤسسات و شرکت‌های دولتی و یا وابسته به دولت و یا نهادهای انقلابی و بنیادها و مؤسساتی که زیر نظر ولی فقیه اداره می‌شوند و دیوان محاسبات و مؤسساتی که به کمک مستمر دولت اداره می‌شوند و یا دارندگان پایه قضایی و به‌طورکلی اعضا و کارکنان قوای سه‌گانه و همچنین نیروهای مسلح و مأمورین به خدمات عمومی اعم از رسمی و غیررسمی ...».

بسیاری از کارفرمایان به دلایل گوناگون مایل‌اند ارتباطات کارکنانشان را شنود کنند. همچنین ارائه‌دهندگان خدمات مخابراتی نیز که هم‌اینک طیف بسیار گسترده‌ای از ارتباطات را برای کاربرانشان فراهم می‌آورند، در معرض ارتکاب چنین جرمی قرار دارند (فضلی، ۱۳۸۹: ۲۱۰).

به‌این‌ترتیب، با عنایت به اینکه ماده (۷۴۷) قانون مجازات اسلامی،[1] ارتکاب جرایم رایانه‌ای ازسوی اشخاص حقوقی را سزاوار کیفر دانسته و در تسری حکم ماده (۷۳۰) به این ماده تردیدی وجود ندارد، درصورت جمع بودن شرایط حاکم بر آن، کیفرهای مقرر در ماده (۷۴۸)[2] بر شخص حقوقی اعمال خواهد شد.

---

۱. «ماده (۷۴۷) ـ در موارد زیر، چنانچه جرائم رایانه‌ای به نام شخص حقوقی و در راستای منافع آن ارتکاب یابد، شخص حقوقی دارای مسئولیت کیفری خواهد بود:

الف) هرگاه مدیر شخص حقوقی مرتکب جرم رایانه‌ای شود.

ب) هرگاه مدیر شخص حقوقی دستور ارتکاب جرم رایانه‌ای را صادر کند و جرم به وقوع بپیوندد.

ج) هرگاه یکی از کارمندان شخص حقوقی با اطلاع مدیر یا در اثر عدم نظارت وی مرتکب جرم رایانه‌ای شود.

د) هرگاه تمام یا قسمتی از فعالیت شخص حقوقی به ارتکاب جرم رایانه‌ای اختصاص یافته باشد.

تبصره «۱» ـ منظور از مدیر کسی است که اختیار نمایندگی یا تصمیم‌گیری یا نظارت بر شخص حقوقی را دارد.

تبصره «۲» ـ مسئولیت کیفری شخص حقوقی مانع مجازات مرتکب نخواهد بود و درصورت نبود شرایط صدر ماده و عدم انتساب جرم به شخص خصوصی فقط شخص حقیقی مسئول خواهد بود».

۲. «ماده (۷۴۸) ـ اشخاص حقوقی موضوع ماده فوق، با توجه به شرایط و اوضاع و احوال جرم ارتکابی، میزان درآمد و نتایج حاصله از ارتکاب جرم، علاوه‌بر سه تا شش برابر حداکثر جزای نقدی جرم ارتکابی، به‌ترتیب ذیل محکوم خواهند شد:

الف) چنانچه حداکثر مجازات حبس آن جرم تا پنج سال حبس باشد، تعطیلی موقت شخص حقوقی از یک تا نُه ماه و درصورت تکرار جرم تعطیلی موقت شخص حقوقی از یک تا پنج سال.

ب) چنانچه حداکثر مجازات حبس آن جرم بیش از پنج سال حبس باشد، تعطیلی موقت شخص حقوقی از یک تا سه سال و درصورت تکرار جرم، شخص حقوقی منحل خواهد شد.

تبصره ـ مدیر شخص حقوقی که طبق بند «ب» این ماده منحل می‌شود، تا سه سال حق تأسیس یا نمایندگی یا تصمیم‌گیری یا نظارت بر شخص حقوقی دیگر را نخواهد داشت».

۸. جمع‌بندی و نتیجه‌گیری

حریم ارتباطات اشخاص، به‌ویژه ارتباطات الکترونیک آنها، از حساس‌ترین شاخه‌ها یا ارکان حریم خصوصی به‌شمار می‌آید؛ زیرا فرض بر این است که اطلاعاتی در آنها جریان دارد که درصورت دستیابی غیرمجاز به آنها، می‌تواند زیان‌بارترین آسیب‌ها را به دارنده یا موضوع اطلاعات وارد آورد. به همین منظور و برای ایجاد بازدارندگی متناسب و اثربخش در میان بزهکاران بالقوه‌ای که سودای چنین تعرضاتی را در سر می‌پرورانند، قانونگذاران به حمایت‌های قانونی و وضع احکام کیفری برای بزه‌دیدگان این سوءاستفاده‌های ناشایست پرداخته و به این وسیله صیانت از حریم ارتباطی آنها را تضمین کرده‌اند.

بااین‌حال، همانند همه احکام کیفری، پیدایش و رخ دادن شرایط گوناگون می‌تواند کارایی قوانین پشتیبان حریم ارتباطی اشخاص را به خطر اندازد. لذا نه تنها باید به هنگام تدوین چنین احکامی کوشید جامعیت آنها، ولو برای بازه زمانی متعارفی تضمین شود، بلکه پیوسته با رصد چگونگی اجرای این احکام و شناسایی به‌هنگام کاستی‌ها و نارسایی‌های پیش روی آنها، از فراهم آمدن زمینه‌های سوءاستفاده‌آمیز برای هنجارشکنان جلوگیری شود.

از جمله موضوعاتی که ضروری است به هنگام وضع قوانین، به‌ویژه قوانین کیفری راجع به حوزه‌های فناورانه، به‌ویژه فناوری‌های اطلاعاتی و ارتباطی مورد توجه قرار گیرد، رویکرد به‌اصطلاح فناوری خنثی یا بی‌طرف[1] است؛ به این معنا که قانونگذار خود را به رفتار یا ابزار یا وسیله یا فناوری خاصی محدود نمی‌کند تا چنانچه نمونه‌های نوآورانه‌ای پدید آمدند، با بن‌بست در اجرا روبه‌رو نشود. برای مثال، چنانچه برای شنود، تنها به ذکر «تلفن» بسنده می‌شد، سایر سامانه‌های پیام‌رسان الکترونیک را دربرنمی‌گرفت و نارسایی قانونی جدی پدید می‌آمد. هرچند این سخن به معنای تجویز نگاه بی‌پایان به موضوعات قانونی نیست و همان‌طور که جامعیت یک قانون ارزش به‌شمار می‌آید، مانعیت آن نیز بر اعتبارش می‌افزاید.

1. Technology Neutral

خوشبختانه قانونگذار ایرانی، خواسته یا ناخواسته تا حد زیادی به این موضوع پایبند بوده و گزافه نیست اگر گفته شود سنگ بنای این حوزه را به‌درستی گذاشته و راه قانونگذاری‌های بعدی، چه سامانده و چه سزاده را به‌خوبی هموار کرده است. ارائه تعریف درست، منطقی و جامع‌الشمولی از «مخابرات» در چهار دهه پیش، آغاز بسیار خوبی را نوید می‌داد، اما متأسفانه سایر قطعات این جورچین حمایتی تقنینی از کاربری و حریم ارتباطات الکترونیک، به همان مطلوبیت گردهم نیامدند تا اینکه سرانجام، با تصویب قانون جرایم رایانه‌ای در سال ۱۳۸۸ و الحاق آن به قانون مجازات اسلامی، این نیاز به شکل نسبتاً مطلوبی برطرف شد.

از بررسی مفاد ماده (۷۳۰) قانون مجازات اسلامی در کنار سایر احکام قانونی مرتبط و واقعیات حاکم بر ارتباطات الکترونیک و چشم‌انداز این حوزه، می‌توان امیدوار بود که کاستی یا نارسایی قانونی به آن شکل که زمینه سوءاستفاده را برای هنجارشکنان بالقوه فراهم آورد، وجود نخواهد داشت و از این لحاظ قانونگذار نمره قابل قبولی را دریافت کرده است. اما نادیده انگاشتن یا نادیده ماندن برخی موضوعات می‌تواند اجرای شایسته این حکم را با محدودیت‌هایی روبه‌رو کند.

درباره موضوع جرم، همان‌طور که دیده شد، محتوای رایانه‌ای، مورد توجه قانونگذار قرار گرفته است. با توجه به اینکه دیدگاه‌های متفاوتی درباره شمول یا عدم شمول داده‌های ترافیک در حکم این ماده وجود دارند و ضروری است از دریافت غیرمجاز این داده‌ها نیز حمایت کیفری به‌عمل آید، این‌گونه ابهام‌ها باید برطرف شوند. برای حفظ تناسب در ضمانت اجرای قابل اعمال نیز می‌توان درجه‌ای پایین‌تر از محتوای رایانه‌ای و برای مثال حداقل یک یا دو کیفر مقرر را پیش‌بینی کرد.

در حال انتقال بودن، ویژگی ذاتی جرمی مانند شنود است. اما همان‌طور که در تبصره ماده (۷۷۶) قانون مجازات اسلامی دیده شد، حساسیت این محتواها به حدی است که در مواردی باید ذخیره شده‌های آنها ولو با درجه‌ای پایین‌تر از حمایت کیفری بهره‌مند شوند و

این حکم تنها شامل ضابطان متخلف دادگستری نشود.

درباره مفهوم و گستره ارتباطات هم دیده شد که دو مفهوم بسیار گسترده و بسیار محدود قابل استنباط است. شاید مؤثرترین عنصری که می‌تواند اجرای این حکم را با چالش جدی روبه‌رو کند، همین واژه باشد. به‌نظر می‌رسد قانونگذار باید کنشگرانه عمل کرده و منتظر رویه قضایی نماند؛ زیرا ممکن است برخی به‌طور ناروا با ضمانت اجراهای سنگین کیفری روبه‌رو و برخی دیگر به‌طور ناروا از چنین ضمانت اجرای اثربخش، متناسب و بازدارنده‌ای معاف شوند.

علاوه‌بر این، ازآنجاکه امکان دریافت، ذخیره‌سازی و پردازش انواع ارتباطات انسانی به‌وسیله سامانه‌های رایانه‌ای و مخابراتی وجود دارد و می‌تواند زمینه بسیاری از سوءاستفاده‌های گوناگون را از اطلاعات به‌دست آمده فراهم آورد، به‌نظر می‌رسد ورود قانونگذار به این عرصه و جرم‌انگاری استراق سمع الکترونیک و گنجانیدن آنها به قلمرو شنود غیرمجاز، ناروا انگاشته نمی‌شود و حمایت فراگیر از حریم خصوصی ارتباطی شهروندان را نیز تضمین خواهد کرد.

غیرعمومی بودن ارتباط نیز از عناصر اصلی و تعیین‌کننده شنود دانستن یا نداستن یک رفتار به‌شمار می‌آید. سزاوار است قانونگذار دست‌کم با برشمردن نمونه‌هایی از باب تمثیل، به شناسایی سایر مصادیق متناسب ازسوی مراجع صلاحیتدار قضایی کمک کند.

سرانجام، درباره کیفر مقرر برای این جرم، پیشنهاد می‌شود قانونگذار از توانمندی کیفرهای اجتماعی برای بالاتر بردن میزان بازدارندگی این ضمانت اجراها بهره‌برداری کند. محرومیت از اشتغال در مشاغلی که امکان ارتکاب دوباره این جرایم را فراهم می‌آورند یا محرومیت از اشتراک یا کاربری خدمات ارتباطات عمومی الکترونیک، می‌تواند دستاوردهایی به مراتب بازدارنده‌تر از حبس یا جزای نقدی داشته باشد، مشروط به آنکه زمینه اجرای شایسته چنین کیفرهایی فراهم شود.

منابع و مآخذ

۱. قرآن کریم.

۲. آقایی‌نیا، حسین (۱۳۸۵). *حقوق کیفری اختصاصی؛ جرایم علیه اشخاص* (شخصیت معنوی)، تهران، میزان.

۳. انصاری، باقر (۱۳۸۶). *حقوق حریم خصوصی*، تهران، سمت.

۴. ـــــ (۱۳۹۰). *حقوق رسانه*، تهران، سمت.

۵. بای، حسینعلی و بابک پورقهرمانی (۱۳۸۸). *بررسی فقهی حقوقی جرایم رایانه‌ای*، قم، پژوهشگاه علوم و فرهنگ اسلامی.

۶. بهره‌مند، حمید و امیرحسین جلالی فراهانی (در دست چاپ). «اطلاعات شخصی و پیشگیری از جنایات سازمان‌یافته فراملی»، تهران، *مجموعه مقالات همایش ملی حقوق ثبت احوال*.

۷. جلالی فراهانی، امیرحسین (۱۳۸۸). *تفتیش و توقیف رایانه‌ها و تحصیل دلایل الکترونیکی در تحقیقات کیفری*، تهران، نشر روزنامه رسمی.

۸. ـــــ (۱۳۸۹). *کنوانسیون جرایم سایبر و پروتکل الحاقی آن*، تهران، خرسندی.

۹. دبیرخانه شورای عالی انفورماتیک کشور (۱۳۷۶). *جرایم کامپیوتری*، جلد اول، تهران.

۱۰. دهخدا، علی‌اکبر (۱۳۸۹). *لغت‌نامه دهخدا*، تهران، مؤسسه انتشارات دانشگاه تهران، ویرایش چهارم.

۱۱. سازمان فناوری اطلاعات ایران (۱۳۸۹). *مجموعه مقالات و گزارشاتی درباره امنیت فضای تولید و تبادل اطلاعات*، جلد دوم، تهران، نهضت پویا.

۱۲. عالی‌پور، حسن (۱۳۹۰). *حقوق کیفری فناوری اطلاعات*، تهران، خرسندی.

۱۳. فضلی، مهدی (۱۳۸۹). *مسئولیت کیفری در فضای سایبر*، تهران، خرسندی.

۱۴. کیسی، اون (۱۳۸۶). *دلایل دیجیتالی و جرم رایانه‌ای* (علم قانونی، رایانه‌ها و اینترنت)، ترجمه امیرحسین جلالی فراهانی و علی شایان، قم، سلسبیل.

۱۵. مرکز پژوهش‌های مجلس شورای اسلامی (۱۳۸۷). «اظهارنظر کارشناسی درباره لایحه جرایم رایانه‌ای» (متن اصلاحی)، شماره ۲-۹۱۳۸.

۱۶. میرمحمدصادقی، حسین (۱۳۸۶). *حقوق کیفری اختصاصی: جرایم علیه اشخاص*، تهران، میزان.

17. Garner, Bryan A. (1999). *Black's Law Dictionary*, United States of America, West Group Publishing, Seventh Edition.