فصلنامه علمی حقوق و مطالعات نوین، دوره ۶، شماره ۳، پیاپی ۲۰، پاییز ۱۴۰۴ www.jhvmn.ir

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

بازاندیشی در مشروعیت شنود در عصر دیجیتال با تأکید بر تقابل امنیت کیفری و حریم خصوصی

امیررضا محمودی[۱] / سحر علیپور نوشر[۲]

* نوع مقاله: پژوهشی / تاریخ دریافت: ۱۴۰۴/۰۲/۱۵ / تاریخ پذیرش: ۱۴۰۴/۰۴/۰۴

کدمقاله: JHVMN-۲۵۰۶-۱۲۹۸

چکیده

با توسعه روزافزون فناوری‌های اطلاعاتی و گسترش تعاملات دیجیتال، مفاهیمی همچون شنود الکترونیکی، مرزهای مشروعیت آن و نسبت آن با امنیت و آزادی‌های فردی، به یکی از چالش‌های اساسی در حوزه حقوق کیفری معاصر تبدیل شده‌اند. در این میان، شنود غیرمجاز سایبری که متضمن دسترسی یا ضبط غیرقانونی ارتباطات خصوصی در فضای دیجیتال است، سؤالاتی بنیادین درباره حدود و ثغور مداخله دولت، چارچوب‌های قانونی، اصول دادرسی منصفانه و صیانت از حریم خصوصی افراد مطرح می‌کند. این مقاله با رویکرد توصیفی-تحلیلی، به واکاوی جایگاه شنود غیرمجاز در ساختار جرایم سایبری پرداخته و عناصر قانونی این جرم، خلأهای تقنینی، ابهامات تفسیری و چالش‌های اجرایی آن را بررسی می‌کند. یافته‌ها نشان می‌دهد که نبود تعریف دقیق و منسجم از شنود، فقدان سازوکارهای نظارتی اثربخش و پراکندگی یا تعارض میان مقررات موجود، موجب تضعیف مشروعیت حقوقی و تردید در کارآمدی شنود در نظام کیفری ایران شده است. در پایان، پیشنهادهایی برای اصلاح قوانین، تقویت شفافیت، تضمین حقوق شهروندی و افزایش انطباق میان امنیت کیفری و حفظ حریم خصوصی ارائه می‌شود.

واژگان کلیدی: شنود غیرمجاز، جرایم سایبری، مشروعیت شنود، حریم خصوصی، سیاست کیفری ایران، امنیت اطلاعات.

[۱]. استادیار گروه حقوق، دانشکده علوم انسانی، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران. amirreza.mahmodi@gmail.com

[۲]. کارشناسی‌ارشد گروه حقوق، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران. (نویسنده مسئول) sahar.alipour۹۱۱@gmail.com

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

مقدمه

در دهه‌های اخیر، جهان با تحولات بنیادینی در عرصه فناوری اطلاعات و ارتباطات مواجه شده است؛ تحولات شتابانی که موجب دگرگونی الگوهای ارتباطی، اقتصادی، فرهنگی و امنیتی در سطوح مختلف شده‌اند. در این بستر جدید، مفهوم «ارتباط خصوصی» نیز دچار تغییراتی اساسی شده و بسترهای دیجیتال جایگزین روش‌های سنتی تعاملات انسانی گردیده‌اند. همین تحول ساختاری، بروز چالش‌های نوظهوری را در حوزه حقوق کیفری به همراه داشته است. یکی از مهم‌ترین این چالش‌ها، مسئله شنود سایبری و تبیین مرزهای مشروعیت و مقبولیت آن در مواجهه با اصول بنیادین حقوق کیفری، به‌ویژه اصل قانونی بودن جرم و مجازات، اصل حریم خصوصی و اصل تناسب اقدامات کیفری است.شنود در بستر سایبری، برخلاف شیوه‌های سنتی استراق سمع، نه‌تنها محدود به ضبط صدای مکالمات تلفنی یا فیزیکی نیست، بلکه شامل انواع روش‌های دسترسی غیرمجاز به داده‌ها، پیام‌ها، فایل‌های شخصی و حتی اطلاعات رمزگذاری‌شده در محیط‌های دیجیتال نیز می‌شود. این گستره فنی و پیچیدگی‌های فنی مرتبط، موجب شده است که اعمال شنود بدون ضوابط روشن قانونی، از یک سو، امنیت روانی و اطلاعاتی شهروندان را تهدید کند و از سوی دیگر، با تضعیف اعتماد عمومی به نهادهای دولتی، چالشی اساسی برای حکومت‌های مدرن در دستیابی به تعادل میان کارآمدی اجرایی و مشروعیت حقوقی فراهم آورد.در نظام‌های حقوقی مختلف، مواجهه با پدیده شنود الکترونیکی همواره همراه با نوعی دوگانگی مفهومی و عملی بوده است. از یک سو، نهادهای امنیتی و ضابطان قضایی نیازمند ابزارهایی برای کشف جرم و مقابله با تهدیدهای امنیتی در فضای مجازی هستند و شنود را به‌عنوان یکی از ابزارهای کلیدی در این فرآیند تلقی می‌کنند؛ و از سوی دیگر، مداخلات بدون قاعده در حریم خصوصی افراد، موجب نقض حقوق بنیادین و مغایرت با اصول دادرسی منصفانه می‌شود. بنابراین، یافتن مرز مشروعیت برای شنود، امری ضروری، اما دشوار و متضمن ملاحظات حقوقی، فنی و سیاست‌گذاری است.در ایران نیز هم‌زمان با تصویب قانون جرایم رایانه‌ای مصوب ۱۳۸۸ و توسعه روزافزون بسترهای دیجیتال، شنود غیرمجاز به‌عنوان یکی از مصادیق جرایم علیه محرمانگی داده‌ها و اطلاعات، موضوع توجه قانون‌گذار قرار گرفت. با این حال، بررسی دقیق مفاد قانونی، آیین‌نامه‌ها و رویه‌های قضایی موجود نشان می‌دهد که هنوز نظام حقوقی ایران با چالش‌هایی

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

جدی در زمینه تعریف دقیق شنود، تمایز آن از سایر اقدامات نظارتی، تعیین حدود اختیارات نهادهای مسئول و تضمین‌های حقوق شهروندان در برابر تعرضات بی‌ضابطه مواجه است.

از منظر حقوق کیفری، مشروعیت شنود صرفاً به معنای وجود حکم قانونی برای انجام آن نیست؛ بلکه این مشروعیت باید در پرتو اصول بنیادین حقوق جزا سنجیده شود. به بیان دیگر، وجود نص قانونی برای شنود، در صورتی می‌تواند مشروع تلقی شود که با اصولی چون ضرورت، تناسب، نظارت قضایی، رعایت حقوق متهم و پیش‌بینی ضمانت‌اجراهای مؤثر در صورت سوءاستفاده، همراه باشد. در غیر این صورت، حتی شنود به ظاهر قانونی نیز ممکن است ناقض حریم خصوصی و مخدوش‌کننده مشروعیت فرایندهای کیفری تلقی شود.

از سوی دیگر، ضعف در تفکیک مفهومی میان «شنود قانونی» و «شنود غیرمجاز»، یکی از موانع اصلی در سامان‌دهی نظام حقوقی ناظر به شنود سایبری در ایران است. قانون‌گذار در موارد متعددی، بدون ارائه تعریف صریح، اقدام به جرم‌انگاری کرده است، در حالی که در نظام‌های پیشرفته، تعاریف دقیق، معیارهای فنی روشن، و رویه‌های نظارتی شفاف برای شنود وضع شده‌اند. به همین دلیل، در حقوق ایران، هم برداشت نهادهای ضابط از مفهوم شنود، متشتت و گاه موسع است، و هم امکان دفاع حقوقی شهروندان در برابر شنودهای غیرمجاز، تضعیف شده است.علاوه بر این، اجرای شنود در بستر فضای مجازی، نیازمند دانش و فناوری تخصصی است که اغلب در اختیار نهادهای محدود و خاص قرار دارد. همین امر، امکان نظارت عمومی یا حتی قضایی را محدود کرده و احتمال سوءاستفاده یا اعمال شنود بدون مجوز را افزایش داده است. در حالی که در نظام‌های حقوقی پیشرو، سازوکارهای نظارتی چندلایه، گزارش‌دهی شفاف، و تعهد به پاسخگویی نهادهای مسئول، بخشی از الزامات قانونی شنود محسوب می‌شود. عدم پیش‌بینی چنین سازوکارهایی در حقوق ایران، موجب شده که اجرای شنود، با ابهامات حقوقی و شائبه‌های متعدد همراه شود.

در این مقاله تلاش شده است با تمرکز بر ابعاد کیفری شنود غیرمجاز سایبری در نظام حقوقی ایران، به تحلیل انتقادی از ساختار تقنینی و اجرایی مرتبط پرداخته شود. رویکرد مقاله، توصیفی-تحلیلی است و با استفاده از منابع قانونی، اسناد سیاست کیفری، آراء قضایی، و مطالعات تطبیقی، به بازنگری در وضعیت موجود و ارائه چارچوبی نظری برای مشروع‌سازی شنود در حقوق کیفری ایران می‌پردازد. در این چارچوب، به عناصر سه‌گانه جرم شنود غیرمجاز، چالش‌های موجود در قوانین فعلی، و

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

راهکارهایی برای بازنگری و اصلاح تقنینی پرداخته شده است.هدف اصلی این مقاله، ارائه تحلیلی نظام‌مند از وضعیت فعلی شنود غیرمجاز در ایران، نقد کاستی‌ها و پیشنهاد راهکارهایی برای ارتقای شفافیت، مشروعیت و کارآمدی این نهاد در بستر تحولات دیجیتال است. روشن است که در شرایط فعلی، نادیده‌گرفتن ضرورت شنود به‌منزله تضعیف نظام کیفری در برابر تهدیدهای سایبری است، اما اجرای آن بدون ضوابط روشن نیز به‌منزله نقض حقوق بنیادین شهروندان خواهد بود. یافتن توازن میان این دو دغدغه، مستلزم بازاندیشی در اصول سیاست کیفری، بازنگری در قوانین موجود، و حرکت به‌سوی تنظیم مقرراتی هوشمندانه، شفاف و پاسخگو است.

۱- مفهوم شنود غیر مجاز

به معنای دسترسی غیرقانونی به اطلاعات محرمانه افراد یا سازمان‌ها از طریق ابزارهای الکترونیکی است. این عمل می‌تواند شامل استراق سمع مکالمات تلفنی، دسترسی به ایمیل‌ها، پیام‌های خصوصی و سایر داده‌های دیجیتال باشد. در فضای سایبر، شنود غیرمجاز به دلیل ماهیت ناملموس و گسترده‌تر شدن فناوری‌های ارتباطی، به یکی از جرائم پیچیده تبدیل شده است. (صفاری، ۱۳۹۵، ۴۲) شنود غیرمجاز به عنوان یکی از جرایم سایبری مدرن، در سال‌های اخیر به دلیل گسترش فناوری‌های ارتباطی و دیجیتال، به یک چالش بزرگ برای حریم خصوصی افراد، سازمان‌ها و حتی امنیت ملی تبدیل شده است. این عمل که شامل دسترسی غیرقانونی به ارتباطات، اطلاعات یا داده‌های افراد بدون رضایت آن‌هاست، می‌تواند پیامدهای گسترده‌ای در سطوح مختلف داشته باشد. (احمدی، ۱۴۰۲، ۴۵) شنود غیرمجاز به معنای گوش دادن یا ضبط کردن ارتباطات خصوصی افراد بدون اجازه آن‌ها است. این ارتباطات می‌توانند شامل مکالمات تلفنی، پیام‌های الکترونیکی، یا هر نوع ارتباط دیگر باشد. شنود غیرمجاز شامل هرگونه اقدام غیرقانونی برای دسترسی به داده‌ها، اطلاعات یا ارتباطات خصوصی افراد از طریق شبکه‌های رایانه‌ای، اینترنت یا سایر ابزارهای الکترونیکی است. شنود غیرمجاز در فضای سایبر به عنوان یکی از مصادیق جرائم سایبری، در قوانین مختلفی از جمله قانون جرائم رایانه‌ای مصوب ۱۳۸۸ جرم انگاری شده است. بر اساس ماده ۷۲۹ این قانون، هرگونه دسترسی غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی جرم محسوب می‌شود و مجازات‌هایی از جمله حبس و جزای نقدی برای آن پیش‌بینی شده است. (احمدی، ۱۴۰۲، ۴۵) شنود غیر مجاز سایبری به هرگونه دسترسی غیرقانونی و بدون اجازه به ارتباطات الکترونیکی افراد اطلاق می‌شود.

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

این عمل ممکن است شامل شنود پیام‌ها، تماس‌های تلفنی، ایمیل‌ها، پیامک‌ها و حتی تماس‌های صوتی از طریق اپلیکیشن‌های مختلف باشد. در حقوق ایران، این نوع از نقض حریم خصوصی در ماده ۲ قانون جرایم رایانه‌ای و همچنین در ماده ۲۱ قانون حمایت از حقوق مصرف‌کنندگان مورد توجه قرار گرفته است.

۱-۱- انواع شنود غیر مجاز

گفتیم شنود غیرمجاز یکی از مصادیق بارز نقض حریم خصوصی افراد به شمار می‌رود که با گسترش فناوری‌های ارتباطی و توسعه فضای مجازی، اشکال پیچیده‌تری یافته و اهمیت توجه به آن در عرصه حقوق کیفری دوچندان شده است. در حقوق ایران، شنود غیرمجاز تحت عنوان کلی دسترسی غیرمجاز به داده‌ها یا اطلاعات در حال انتقال شناخته شده و بسته به نحوه ارتکاب، ابزار مورد استفاده، و هویت مرتکب، می‌تواند انواع مختلفی داشته باشد. به طور کلی، شنود غیرمجاز را می‌توان به دو نوع فیزیکی و دیجیتال تقسیم نمود.

۱. شنود فیزیکی

شنود فیزیکی شامل استفاده از ابزارهای سخت‌افزاری مانند دستگاه‌های ضبط صدا، میکروفن‌های مخفی، و سایر تجهیزات مکانیکی جهت استراق سمع مکالمات حضوری یا تلفنی افراد بدون رضایت آنان و بدون مجوز قانونی است.

۲. شنود دیجیتال

در مقابل، شنود دیجیتال که عمدتاً در بستر فضای مجازی و سیستم‌های رایانه‌ای رخ می‌دهد، شامل استفاده از نرم‌افزارها، بدافزارها یا روش‌های هکری برای دسترسی غیرمجاز به داده‌ها، چت‌ها، تماس‌های اینترنتی، ایمیل‌ها و حتی فعالیت‌های کاربران در شبکه‌های اجتماعی می‌باشد. این نوع از شنود، نه‌تنها تهدیدی جدی علیه آزادی‌های فردی و امنیت اطلاعات محسوب می‌شود، بلکه با پیچیدگی‌های فنی و چالش‌های قانونی نیز همراه است. برای مثال، شنود چت‌های خصوصی در بسترهای پیام‌رسان یا دسترسی به حساب‌های کاربری افراد در شبکه‌های اجتماعی از طریق حملات فیشینگ، نصب جاسوس‌افزار بر روی دستگاه‌های شخصی یا سوءاستفاده از ضعف‌های امنیتی

نرم‌افزارها، از مصادیق رایج شنود دیجیتال به شمار می‌روند. (کاظمی، ۱۴۰۰، ۷۸؛ اردبیلی، ۱۳۹۵، ۲۲)

از منظر حقوق کیفری، تحقق جرم شنود غیرمجاز مستلزم فراهم بودن چند شرط اساسی است: نخست آن‌که باید فعلی مثبت، اعم از فیزیکی یا دیجیتالی، صورت گرفته باشد که متضمن شنود یا دسترسی به محتوای ارتباطات خصوصی باشد؛ دوم این‌که چنین اقدامی بدون رضایت طرفین ارتباط انجام شده باشد؛ و سوم آن‌که هیچ‌گونه مجوز قانونی برای آن وجود نداشته باشد. لازم به ذکر است که برای تحقق این جرم، لزومی به ضبط کامل مکالمه یا دستیابی کامل به داده‌ها نیست، بلکه حتی شنیدن بخشی از مکالمه یا دسترسی جزئی نیز می‌تواند برای تحقق عنوان مجرمانه کافی باشد. بر اساس قانون جرایم رایانه‌ای، مرتکب این جرم ممکن است به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون تا چهل میلیون ریال محکوم شود. از دیگر مصادیق مهم شنود غیرمجاز، می‌توان به ارتکاب این جرم توسط مأموران دولتی اشاره کرد. چنان‌چه کارمندان یا مأموران دولتی، به اعتبار شغل و موقعیت اداری خود و بدون اخذ مجوز قضایی، اقدام به شنود مکالمات تلفنی یا ارتباطات الکترونیکی اشخاص کنند، نه‌تنها مرتکب جرم شنود غیرمجاز شده‌اند، بلکه ممکن است با مجازات‌هایی شدیدتر از جمله انفصال از خدمت نیز مواجه شوند. در چنین مواردی، عنصر سوءاستفاده از موقعیت شغلی، موجب تشدید مسئولیت کیفری مأموران می‌گردد. از سوی دیگر، در موارد خاصی همچون جرایم مرتبط با امنیت ملی، شنود ممکن است با مجوز قانونی و تحت نظارت مراجع ذی‌صلاح صورت گیرد؛ با این حال، هرگونه شنود خارج از محدوده مجوز یا در غیاب آن، همچنان جرم تلقی شده و قابل تعقیب کیفری خواهد بود. در واقع، صدور مجوز قانونی برای شنود در این موارد، باید در چارچوب محدود، موقت، و بر اساس اصول ضرورت و تناسب صورت پذیرد.در مجموع، شنود غیرمجاز با نقض آشکار اصل محرمانگی ارتباطات، یکی از مهم‌ترین تهدیدها علیه حقوق بنیادین شهروندان در عصر دیجیتال محسوب می‌شود. این جرم، چه در قالب فیزیکی و سنتی آن و چه در قالب‌های نوین سایبری، با توجه به آثار مخرب آن بر اعتماد عمومی، امنیت اجتماعی و حیثیت افراد، مستلزم واکنش مؤثر کیفری و نیز ارتقاء سطح آگاهی عمومی و فنی شهروندان برای پیشگیری از وقوع آن است. همچنین قانون‌گذار باید با بازنگری در مقررات موجود و لحاظ پیچیدگی‌های فنی ابزارهای نوین شنود، به تقویت نظام قانونی حمایت از حریم خصوصی در بسترهای جدید اقدام کند.

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

۱-۲- چالش‌های اجرایی و قانونی در مواجهه با شنود غیرمجاز

۱. چالش‌های اجرایی

یکی از مهم‌ترین چالش‌های اجرایی در مقابله با جرم شنود غیرمجاز، عدم شفافیت در تعریف مفاهیم مربوط به این جرم است. برای نمونه، مفاهیمی مانند «دسترسی غیرمجاز» و «حریم خصوصی» در بسیاری از موارد به‌طور دقیق در قوانین موجود تعریف نشده‌اند، که این امر می‌تواند در مراحل رسیدگی قضائی باعث مشکلات و اختلاف‌نظرهایی گردد. در این زمینه، ماده ۷۳۰ قانون جرایم رایانه‌ای (مصوب ۱۳۸۸) به طور کلی به جرم انگاری دسترسی غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای پرداخته است، اما این ماده فاقد تعریف دقیقی از مفهوم «دسترسی غیرمجاز» است (قانون جرایم رایانه‌ای، ۱۳۸۸، ماده ۷۳۰).چالش دیگری که در زمینه اجرایی این جرم وجود دارد، نبود نیروهای متخصص در زمینه جرایم سایبری است. این امر باعث می‌شود که دسترسی به شواهد دیجیتال و جمع‌آوری آن‌ها برای پیگیری و شناسایی مجرمان دشوار باشد. همچنین، نبود هماهنگی مناسب بین نهادهای امنیتی و قضائی نیز موجب کاهش کارایی در مبارزه با این نوع جرایم می‌شود. (صفاری، ۱۳۹۵، ۱۵)

۲. چالش‌های قانونی در مواجهه با شنود غیرمجاز

از منظر قانونی نیز، یکی از بزرگ‌ترین چالش‌ها در زمینه مقابله با شنود غیرمجاز، نیاز به بازنگری و اصلاح در قوانین موجود است. قوانین موجود به اندازه کافی به جنبه‌های فنی و تکنولوژیکی جرم شنود غیرمجاز نپرداخته‌اند. در این راستا، قانون حمایت از داده‌ها و حریم خصوصی در فضای مجازی (مصوب ۱۳۹۸) به مسأله حفاظت از اطلاعات شخصی و ممنوعیت دسترسی غیرمجاز به داده‌ها پرداخته است، اما نیاز به به‌روز رسانی برای تطابق با تغییرات سریع فناوری‌های جدید وجود دارد. (قانون حمایت از داده‌ها و حریم خصوصی در فضای مجازی، ۱۳۹۸)همچنین، در بسیاری از کشورهای پیشرفته، مقررات جدید برای مقابله با جرم شنود غیرمجاز به تصویب رسیده است که بر اساس آن‌ها، نه تنها مجازات‌های سنگینی برای دسترسی غیرمجاز به داده‌ها در نظر گرفته شده است، بلکه نظارت و تحلیل شواهد دیجیتال نیز به شکل تخصصی‌تر انجام می‌شود. برای نمونه، کنوانسیون بوداپست (کنوانسیون جرایم سایبری) به جرم انگاری دسترسی غیرمجاز به داده‌ها و سیستم‌های رایانه‌ای

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

پرداخته است و این امر در بسیاری از کشورهای عضو این کنوانسیون به عنوان جرم قابل پیگرد شناخته می‌شود (کنوانسیون بوداپست، ۲۰۰۱)

۲- شنود اطلاعات شخصی و چالش‌های حقوقی آن

شنود و فروش اطلاعات شخصی از جمله جرایم مهم در فضای سایبری محسوب می‌شود که به سهولت قابل ارتکاب بوده و می‌تواند منجر به بروز آسیب‌های جدی نظیر سرقت هویت گردد. این پدیده نه تنها برای قربانیان تبعات منفی فراوانی دارد، بلکه مشکلاتی را نیز برای سیستم قضایی در زمینه پیگیری و مقابله با این جرایم به همراه دارد. حریم خصوصی به عنوان یکی از مفاهیم بنیادین حقوقی، پیوند عمیقی با کرامت انسانی داشته و در راستای حفظ استقلال و آزادی افراد شکل گرفته است. در حقوق اسلامی، حمایت از حریم خصوصی به‌طور غیرمستقیم و از طریق ممنوعیت‌هایی نظیر تجسس، استراق سمع و ورود بدون اجازه به اماکن خصوصی مورد تاکید قرار گرفته است. در حقوق ایران نیز، هرچند حریم خصوصی به صراحت در قانون اساسی مطرح نشده، لیکن از طریق قوانین مختلفی همچون قانون مجازات اسلامی و قانون آیین دادرسی کیفری، برخی مصادیق آن تحت حمایت قرار گرفته‌اند. (انصاری، ۱۳۸۳، ۱)

۳- ضرورت تدوین چارچوب سخت‌گیرانه برای صدور مجوز شنود در فرآیند کیفری

شنود مکالمات خصوصی افراد، به‌عنوان یکی از مصادیق بارز و عمیق مداخله در حریم خصوصی، تنها باید در موارد خاص و ضروری، آن‌هم با رعایت الزامات قانونی و حقوقی دقیق، مجاز شناخته شود. مداخله در این سطح از زندگی خصوصی افراد بدون چارچوب سخت‌گیرانه و نظارت قضایی قوی، می‌تواند موجب نقض گسترده حقوق بشر گردد. (Wright & Kreissl, ۲۰۱٤, ۷۲) برای مشروعیت چنین اقداماتی، چهار شرط اساسی باید هم‌زمان و به‌صورت دقیق رعایت گردد.نخست، محدودسازی شنود به جرایم مهم و خطرناک است. به موجب قواعد بین‌المللی و توصیه‌های حقوق بشر، شنود فقط باید در مواردی چون جرایم تروریستی، جرایم سازمان‌یافته فراملی، قاچاق انسان، مواد مخدر و تهدیدات علیه امنیت ملی مجاز باشد. (Council of Europe, ۲۰۰۱) در غیر این صورت، نقض اصل تناسب و ضرورت در دادرسی کیفری رخ می‌دهد.دوم، احراز ضرورت شنود است. این اصل ایجاب می‌کند که پیش از توسل به شنود، نهاد تحقیقاتی نشان دهد که از دیگر ابزارهای متعارف و

کم‌هزینه‌تر، نظیر تحقیق میدانی، استعلام اسناد یا شهادت شهود، نتیجه‌ای حاصل نشده و شنود تنها گزینه باقی‌مانده است. به‌عبارت‌دیگر، این اقدام باید آخرین راه‌حل ممکن برای کشف جرم تلقی شود. (De Hert & Gutwirth, ۲۰۰۹, ۱۳۹). سوم، تعیین مدت‌زمان محدود و مشخص برای شنود از اهمیت بالایی برخوردار است. قانون باید تعیین کند که شنود برای چه مدت‌زمانی مجاز است و تمدید آن تحت چه شرایطی امکان‌پذیر خواهد بود. در صورت عدم تعیین سقف زمانی، این اقدام می‌تواند منجر به نظارت دائمی و غیرقابل‌کنترل بر زندگی افراد شود که با اصل حاکمیت قانون در تضاد است. (Murray, ۲۰۱٦,. ۲۱۷). چهارم، تأیید قضایی مجوز شنود توسط دادگاه مستقل شرطی اساسی برای اعتبار قانونی آن است. صدور مجوز از سوی بازپرس یا نهاد تحقیقاتی به تنهایی، فاقد پشتوانه نظارتی کافی است و باید دادگاهی مستقل و بی‌طرف با بررسی دلایل و مدارک موجود، نسبت به مشروعیت شنود رأی صادر کند(UN (HumanRights Committee, ۲۰۱٤, para. ٥٧. این امر مانع از سوءاستفاده احتمالی نهادهای امنیتی یا تحقیقاتی از ابزارهای شنود می‌شود. بدون رعایت این شروط چهارگانه، شنود مکالمات خصوصی به‌راحتی می‌تواند به ابزار سرکوب، نقض آزادی‌های مدنی، و زیر پا گذاشتن کرامت انسانی بدل شود. بنابراین، وجود چارچوب‌های قانونی سخت‌گیرانه، مکانیسم‌های نظارت مؤثر و تضمین حقوق دفاعی متهم، ضامن بقای عدالت کیفری در برابر پیشرفت‌های فناورانه و ابزارهای جدید نظارتی خواهد بود. (میرمحمدصادقی، ۱۳۹۸، ۹۱؛ اردبیلی، ۱۳۹۵، ۱۴۳)

۴- تحلیل قوانین کیفری و رویه قضایی درباره شنود غیرمجاز در نظام حقوقی ایران

با رشد و گسترش فناوری‌های دیجیتال، روش‌های شنود غیرمجاز نیز به‌طور قابل توجهی متحول شده‌اند و در حال حاضر از تکنیک‌های پیشرفته‌تری برای نفوذ به ارتباطات و اطلاعات بهره می‌برند. یکی از روش‌های رایج و نسبتاً پیچیده، حملات موسوم به مرد میانی است؛ در این نوع حمله، مهاجم با قرارگیری در میان دو نقطه ارتباطی، داده‌هایی را که میان طرفین مبادله می‌شود رهگیری، سرقت یا حتی دستکاری می‌کند، بدون آنکه طرفین متوجه شوند. (شریفی، ۱۴۰۲، ۴۵) این حمله به‌ویژه در شبکه‌های باز، مانند وای‌فای عمومی، بسیار شایع است و تهدیدی جدی برای کاربران ناآگاه محسوب می‌شود. از سوی دیگر، ظهور شبکه‌های ارتباطی نسل پنجم نیز گرچه فرصت‌هایی بزرگ برای سرعت و کیفیت ارتباطات فراهم کرده، اما در عین حال زمینه‌ساز نوعی جدید از آسیب‌پذیری‌ها

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

شده است. مهاجمان سایبری با بهره‌گیری از ضعف‌های امنیتی موجود در زیرساخت‌های 5G، می‌توانند به داده‌های کاربران دسترسی یابند یا حتی موقعیت مکانی آنان را ردیابی کنند. (رحیمی، ۱۴۰۱، ۷۸) این تهدیدات در محیط‌هایی چون شهرهای هوشمند یا کاربردهای صنعتی 5G، می‌تواند تبعاتی سنگین بر کارکردهای حیاتی داشته باشد. پیامدهای شنود غیرمجاز بسته به سطح هدف‌گیری، بسیار گسترده و گاه ویرانگر است. در سطح فردی، نقض حریم خصوصی، افشای اطلاعات حساس، ایجاد اختلال در روابط شخصی، سوءاستفاده‌های مالی، اخاذی و حتی تهدید به مرگ می‌تواند از نتایج مستقیم این جرم باشد. در مورد سازمان‌ها، افشای اسناد محرمانه، سرقت اطلاعات تجاری یا استراتژیک، از بین رفتن اعتماد مشتریان و وارد آمدن خسارات اقتصادی هنگفت از جمله پیامدهای مهم محسوب می‌شود. در سطح ملی نیز چنانچه اطلاعات امنیتی، نظامی یا سیاسی مورد شنود قرار گیرد، پیامدهای امنیتی آن ممکن است منافع حیاتی یک کشور را به خطر اندازد. (کمالی، ۱۴۰۰، ۹۱)

این نرم‌افزارها می‌توانند تماس‌های تلفنی، پیام‌های متنی، ایمیل‌ها و حتی موقعیت جغرافیایی فرد را رصد کنند. (رضایی، ۱۴۰۱، ۱۲۳) علاوه بر این، دستگاه‌های سخت‌افزاری مانند میکروفون‌ها و دوربین‌های مخفی نیز برای شنود استفاده می‌شوند. علاوه بر این، دستگاه‌های سخت‌افزاری مانند میکروفون‌ها و دوربین‌های مخفی نیز برای شنود استفاده می‌شوند. این ابزارها ممکن است در مکان‌های عمومی، محیط‌های کاری یا حتی منازل افراد نصب شوند و اطلاعات حساس را جمع‌آوری کنند. هرکس به طور غیر مجاز محتوای درحال انتقال ارتباطات غیرعمومی در سامانه های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری را شنود کند به حبس از ۶ ماه تا دوسال یا جزای نقدی از ۱۰میلیون ریال تا ۴۰ میلیون ریال یا هردو مجازات محکوم خواهد شد. ماده ۳ قانون جاسوسی رایانه‌ای درباره مجازات شنود محتوای سری در حال انتقال در سامانه های رایانه‌ای و مخابراتی صحبت می کند این عمل با حبس یا پرداخت جزای نقدی تا ۶۰میلیون ریال مجازات می شود. همچنین در مبحث پنجم از فصل دوم قانون مذکور در ماده ۴۸آن به دسترسی به محتوای ارتباطات غیر عمومی اشاره دارد. (امانی، ۱۳۸۹، ۵)

در ارتباط با مجازات جرم شنود غیرمجاز داده‌های رایانه‌ای به‌ویژه داده‌های نظامی، باید توجه داشت که قانون‌گذار با رویکردی سخت‌گیرانه و مبتنی بر حفظ منافع و امنیت ملی، مجازات‌های مشخص و

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

بعضاً سنگینی را در نظر گرفته است. اهمیت این مسئله از آن‌روست که داده‌های نظامی رایانه‌ای، جزء طبقه‌بندی‌شده‌ترین و حیاتی‌ترین اطلاعات در ساختار امنیتی کشور محسوب می‌شوند. هرگونه دسترسی غیرمجاز به این اطلاعات، نه‌تنها تهدیدی جدی برای نهادهای نظامی و دفاعی است، بلکه مستقیماً امنیت عمومی، تمامیت ارضی و ثبات سیاسی کشور را هدف قرار می‌دهد.در همین راستا، قانون جرایم رایانه‌ای ایران، خصوصاً در مواد ناظر بر جرایم علیه محرمانگی داده‌ها و سامانه‌های حساس، مجازات‌هایی از جمله حبس، جزای نقدی و در موارد خاص محرومیت‌های اجتماعی و حرفه‌ای را پیش‌بینی کرده است. شدت این مجازات‌ها بسته به سطح طبقه‌بندی اطلاعات، میزان خسارت وارده، و انگیزه مجرم (نظیر جاسوسی، اخاذی یا اقدامات خرابکارانه) متفاوت است. قانون‌گذار با در نظر گرفتن شرایط خاص داده‌های نظامی، در تلاش است تا با پیش‌بینی ضمانت اجراهای بازدارنده، از ارتکاب چنین جرایمی جلوگیری نموده و حداکثر حفاظت از اطلاعات حساس را تأمین نماید. (مرسی، زرنگ، ۱۴۰۲، ۱۸۱)

۵- پیامدهای شنود غیرمجاز

پیامدهای شنود غیرمجاز یک موضوع پیچیده و چندجانبه است که تأثیرات آن به‌طور مستقیم و غیرمستقیم در سطوح مختلف فردی، سازمانی و ملی احساس می‌شود. این پیامدها فراتر از تهدیدات فیزیکی و اقتصادی، می‌تواند به تغییرات در ساختار اجتماعی و روابط بین‌المللی نیز منجر شود. در این بخش، به بررسی جزئی‌تر این پیامدها خواهیم پرداخت.

۵-۱- پیامدهای فردی

شنود غیرمجاز برای افراد ممکن است به نقض شدید حریم خصوصی و تعرض به آزادی‌های فردی منجر شود. این نوع دسترسی غیرمجاز به اطلاعات شخصی می‌تواند پیامدهای گسترده‌ای داشته باشد. به‌عنوان مثال، وقتی که اطلاعات شخصی یک فرد از طریق شنود غیرمجاز به‌دست می‌آید، این اطلاعات ممکن است برای اخاذی، تهدید و یا حتی بهره‌برداری‌های غیرقانونی مورد استفاده قرار گیرد. در برخی موارد، سوءاستفاده از چنین اطلاعاتی می‌تواند منجر به تهدیدات جانی یا فیزیکی علیه فرد شود، به‌ویژه در شرایطی که اطلاعات حریم خصوصی افراد در معرض عمومی قرار گیرد یا در دست افراد با انگیزه‌های نادرست قرار گیرد. این تهدیدات می‌توانند منجر به آسیب‌های روانی، از

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

دست رفتن اعتماد عمومی، و حتی تغییرات در سبک زندگی و امنیت شخصی افراد شوند. (رحمانی، ۱۴۰۰، ۹۵)

۵-۲- پیامدهای سازمانی و کسب‌وکار

برای سازمان‌ها و کسب‌وکارها، شنود غیرمجاز به‌ویژه در دنیای دیجیتال کنونی، می‌تواند اثرات بسیار منفی به‌دنبال داشته باشد. یکی از مهم‌ترین پیامدهای این نوع شنود، سرقت اطلاعات محرمانه مانند طرح‌های تجاری، استراتژی‌های بازاریابی، داده‌های مالی و حتی اطلاعات مربوط به تحقیق و توسعه است. این نوع دسترسی غیرمجاز به اطلاعات می‌تواند آسیب‌های قابل توجهی به اعتبار، سرمایه و حتی استراتژی‌های بلندمدت سازمان‌ها وارد کند. علاوه بر این، شنود غیرمجاز می‌تواند منجر به از دست رفتن اعتماد مشتریان و شرکای تجاری شده و خسارات مالی هنگفتی را به سازمان‌ها تحمیل کند. در بسیاری از موارد، آسیب به شهرت و اعتبار شرکت ممکن است از خسارات مالی نیز جدی‌تر باشد، چرا که بر اساس تحقیقات، مشتریان به شدت به امنیت داده‌های شخصی و تجاری خود حساس هستند و در صورت بروز نقض امنیتی، به راحتی به رقبا روی می‌آورند. (محمدی، ۱۳۹۹، ۶۷)

۵-۳- پیامدهای امنیتی ملی

در سطح کلان، شنود غیرمجاز می‌تواند تهدیدات جدی برای امنیت ملی ایجاد کند. این تهدیدات به‌ویژه زمانی حادتر می‌شود که اطلاعات استراتژیک، نظامی یا اقتصادی کشورها در معرض خطر قرار گیرد. اطلاعات مربوط به سیاست‌های دفاعی، امنیتی، منابع طبیعی و انرژی، یا حتی راهبردهای اقتصادی، در صورتی که به‌طور غیرمجاز توسط کشورها یا گروه‌های تروریستی دسترسی پیدا شود، می‌تواند به تهدیداتی جدی برای ثبات سیاسی و امنیتی کشورها تبدیل شود. در این شرایط، ممکن است درگیری‌های بین‌المللی یا بحران‌های دیپلماتیک به‌دنبال دسترسی غیرمجاز به این اطلاعات ایجاد شود. بنابراین، شنود غیرمجاز در سطح ملی نه تنها تهدیدی برای حریم خصوصی افراد است، بلکه می‌تواند به تهدیدات جدی برای نظم عمومی و امنیت ملی منجر شود. (رحمانی، ۱۴۰۰، ۹۵)

۶- چالش‌های اجرایی قوانین موجود در مقابله با شنود غیرمجاز سایبری و راهکارهای تقنینی و نهادی

با وجود تصویب قوانین متعدد در راستای حمایت از حریم خصوصی و مقابله با جرایم سایبری، نظام حقوقی ایران در مواجهه با پدیده رو به گسترش شنود غیرمجاز سایبری با موانع جدی اجرایی، تقنینی و نهادی مواجه است. نخستین چالش در این زمینه، ابهام مفهومی در قوانین موجود است؛ به‌طوری‌که بسیاری از اصطلاحات بنیادین نظیر «دسترسی غیرمجاز»، «اطلاعات خصوصی»، «شنود دیجیتال» و حتی «اطلاعات طبقه‌بندی‌شده» به‌صورت دقیق، منقح و هماهنگ تعریف نشده‌اند. این خلأهای مفهومی زمینه‌ساز برداشت‌های متناقض و تفسیرهای گاه سلیقه‌ای در فرآیند رسیدگی قضایی شده و امنیت حقوقی شهروندان را به چالش کشیده است. (محمدی، ۱۳۹۸، ۹۲)

در کنار این ضعف تقنینی، ساختار فعلی اجرای قانون نیز با نارسایی‌هایی بنیادین روبه‌روست. فقدان نیروی انسانی متخصص در حوزه جرایم سایبری، نبود نظام آموزشی منسجم برای پرورش قضات و کارشناسان فنی، و همچنین فقدان هماهنگی مؤثر میان نهادهای مسئول، از جمله عواملی‌اند که کارایی نظام عدالت کیفری را در برابر شنود غیرمجاز به‌شدت تضعیف کرده‌اند. (موسوی، ۱۳۹۹، ۲۶؛ صفاری، ۱۳۹۵، ۲۵) در بسیاری از موارد، نه‌تنها نهادهای امنیتی و انتظامی از سازوکارهای پیشرفته برای کشف و مستندسازی شنود دیجیتال محروم‌اند، بلکه دادگاه‌ها نیز از امکانات و رویه‌های تخصصی برای بررسی این‌گونه پرونده‌ها برخوردار نیستند. نبود آزمایشگاه‌های تخصصی تحلیل ادله دیجیتال، کمبود استانداردهای فنی در پذیرش ادله، و نبود رویه قضائی منسجم، همگی نشان‌دهنده عقب‌ماندگی ساختاری در مقابله با این جرم است. (حسینی، ۱۴۰۱، ۷۱) افزون بر این، چالش‌های ساختاری نظام حقوقی در مواجهه با تحولات فناورانه، موجب شده است که قانون‌گذاری در این حوزه همواره عقب‌تر از واقعیت‌های اجتماعی و تکنولوژیک حرکت کند. به‌ویژه با توجه به پیچیدگی‌های روزافزون ابزارهای شنود و تنوع بسترهای دیجیتال، قوانین فعلی نه‌تنها پاسخ‌گوی اقتضائات فنی نیستند، بلکه گاه فاقد ضمانت اجرایی مؤثر نیز هستند. این وضعیت، در کنار ضعف در زمینه همکاری‌های بین‌المللی برای تعقیب مجرمان سایبری، به ایجاد نوعی «خلأ حمایتی» در برابر نقض حریم خصوصی شهروندان منجر شده است. (سلیمانی، ۱۴۰۰، ۳۳)

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

برای برون‌رفت از این وضعیت، اصلاحات بنیادینی در چند سطح ضروری به نظر می‌رسد. در سطح تقنینی، باید بازنگری جامعی در قوانین موجود صورت گیرد تا مفاهیم بنیادین به‌صورت شفاف، دقیق و هماهنگ با استانداردهای بین‌المللی تعریف شده و جرم‌انگاری‌های فعلی به‌گونه‌ای بازتنظیم شوند که تمامی اشکال نوین شنود دیجیتال را پوشش دهند. در سطح اجرایی، توسعه زیرساخت‌های فناورانه برای کشف و اثبات جرایم، تربیت نیروهای متخصص و آموزش مستمر آنان، و همچنین تأسیس نهادهای تخصصی برای رسیدگی به جرایم سایبری امری گریزناپذیر است. همچنین، گسترش همکاری‌های بین‌المللی و عضویت مؤثر در کنوانسیون‌های بین‌المللی مرتبط با جرایم سایبری، نظیر کنوانسیون بوداپست، می‌تواند ظرفیت‌های حقوقی کشور را برای مقابله با ابعاد فراملی شنود غیرمجاز ارتقا دهد. از همه مهم‌تر، ایجاد آگاهی عمومی در زمینه مخاطرات شنود دیجیتال و ارتقای سواد رسانه‌ای جامعه از طریق آموزش‌های هدفمند، ضرورتی اساسی است که هم جنبه پیشگیرانه دارد و هم به توانمندسازی شهروندان در برابر تهدیدات سایبری منجر خواهد شد.

۶-۱- قوانین و مقررات مرتبط با شنود غیرمجاز

برای مقابله با شنود غیرمجاز، بسیاری از کشورها قوانینی را وضع کرده‌اند که هدف آن‌ها حفاظت از حقوق فردی و سازمانی در برابر تهدیدات سایبری است. در ایران، همانطور که در قانون جرایم رایانه‌ای (۱۳۸۸) اشاره شده است، هرگونه دسترسی غیرمجاز به ارتباطات افراد یا سازمان‌ها به‌عنوان یک جرم شناخته می‌شود و مرتکبان آن با مجازات‌های مختلفی چون جریمه‌های مالی، حبس یا حتی محرومیت از برخی حقوق اجتماعی روبرو خواهند شد. (قانون جرایم رایانه‌ای، ۱۳۸۸، ماده ۷۴۵) این قوانین به‌طور خاص برای حمایت از حریم خصوصی و اطلاعات حساس در برابر تهدیدات سایبری طراحی شده‌اند. اما یکی از چالش‌های اساسی در اجرای این قوانین، دشواری‌های فنی در شناسایی و اثبات جرم است. به دلیل ماهیت پیچیده و پنهانی این نوع جرایم، شناسایی مهاجمان نیازمند تخصص‌های فنی و همکاری بین‌المللی است. همچنین، در حالی که قوانینی برای مقابله با شنود غیرمجاز وجود دارد، غالباً اثبات این جرایم به‌دلیل استفاده از فناوری‌های پیچیده و روش‌های پیشرفته برای مخفی کردن ردپای مجرمان، با مشکلات زیادی مواجه است. (محمدی، ۱۳۹۹، ۶۷)

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

۶-۲- ابعاد حقوقی شنود غیرمجاز سایبری

شنود غیرمجاز سایبری به عنوان یکی از مهم‌ترین چالش‌های حقوقی در عصر اطلاعات، جلوه‌ای نوین از تعرض به حقوق بنیادین بشر، به‌ویژه حق بر حریم خصوصی، محسوب می‌شود. گسترش فضای مجازی و استفاده روزافزون از فناوری‌های ارتباطی، بسترهای متنوعی را برای تبادل اطلاعات ایجاد کرده که در عین سودمندی، بستر ارتکاب جرایم نوپدیدی مانند شنود غیرمجاز را نیز فراهم آورده است. این پدیده از جنبه‌های مختلف حقوقی، اعم از کیفری، مدنی و بین‌المللی، قابل تحلیل است و بررسی جامع آن مستلزم نگاهی چندبُعدی به آثار و پیامدهای آن می‌باشد.در بُعد کیفری، شنود غیرمجاز سایبری به عنوان یک رفتار مجرمانه در بسیاری از نظام‌های حقوقی جرم‌انگاری شده است. در نظام حقوقی ایران، مطابق با ماده ۱ قانون جرائم رایانه‌ای مصوب ۱۳۸۸، هرگونه دسترسی غیرمجاز به سامانه‌های رایانه‌ای و مخابراتی جرم محسوب می‌شود. همچنین بر اساس ماده ۵ این قانون، شنود محتوای ارتباطات خصوصی کاربران بدون رضایت آنان مشمول مجازات حبس و جزای نقدی است. (قانون جرائم رایانه‌ای، ۱۳۸۸) هدف اصلی این جرم‌انگاری، حمایت از حریم خصوصی شهروندان و پیشگیری از سوءاستفاده از فناوری‌های ارتباطی است.در کنار بعد کیفری، شنود سایبری از منظر مدنی نیز واجد اهمیت است؛ چراکه ممکن است منجر به ورود خسارات مادی یا معنوی به افراد شود. بر اساس قواعد عمومی مسئولیت مدنی، از جمله ماده ۱ قانون مسئولیت مدنی ایران، هر کس بدون مجوز قانونی به حقوق دیگران لطمه وارد کند، موظف به جبران خسارت است. از این رو، چنانچه شخصی از رهگذر شنود غیرمجاز متضرر گردد، می‌تواند علیه مرتکب دعوای مطالبه خسارت مطرح نماید. (میرمحمدصادقی، ۱۳۹۸، ۴۶) این خسارات ممکن است ناشی از افشای اسرار خانوادگی، آسیب به حیثیت فردی، یا زیان‌های اقتصادی ناشی از نقض اطلاعات تجاری باشد.شنود سایبری اشکال متنوعی دارد که بسته به روش‌های فنی مورد استفاده، دامنه وسیعی از داده‌های شخصی و حرفه‌ای را در بر می‌گیرد. یکی از رایج‌ترین اشکال آن، شنود ارتباطات اینترنتی است که شامل رهگیری ایمیل‌ها، پیام‌های فوری و تماس‌های اینترنتی از طریق نرم‌افزارها یا ابزارهای تحلیل ترافیک شبکه می‌شود. در کنار آن، شنود حساب‌های کاربری در شبکه‌های اجتماعی مانند اینستاگرام، تلگرام یا توییتر نیز شکل دیگری از تعرض به حریم خصوصی افراد به شمار می‌رود. همچنین، نصب

نرم‌افزارهای جاسوسی بر روی دستگاه‌های شخصی همچون گوشی‌های همراه یا رایانه‌های شخصی از دیگر مصادیق بارز این پدیده است. (اردبیلی، ۱۳۹۵)

پیامدهای شنود غیرمجاز سایبری صرفاً محدود به فرد متضرر نیست، بلکه آثار آن در سطحی گسترده‌تر متجلی می‌شود. نخستین پیامد آن، نقض حریم خصوصی کاربران و ایجاد احساس ناامنی در جامعه است. کاربران با آگاهی از احتمال شنود، ممکن است اعتماد خود به فضای دیجیتال را از دست دهند و از بهره‌گیری آزادانه از ابزارهای ارتباطی خودداری کنند. در بُعد اقتصادی نیز، شرکت‌ها و سازمان‌هایی که اطلاعات محرمانه آن‌ها مورد دستبرد قرار می‌گیرد، متحمل زیان‌های سنگین مالی و از دست دادن اعتبار تجاری می‌شوند. افزون بر این، شنود غیرمجاز سایبری می‌تواند تهدیدی جدی برای امنیت ملی باشد؛ چراکه در مواردی، اطلاعات حساس دولتی و ارتباطات مقامات عالی‌رتبه ممکن است هدف نفوذ قرار گیرد و در اختیار دشمنان قرار گیرد. (مرکز ملی فضای مجازی، ۱۴۰۰)

در نظام‌های حقوقی مختلف، قوانین متعددی برای مقابله با شنود غیرمجاز سایبری وضع شده‌اند. به عنوان نمونه، در ایالات متحده، قانون حفاظت از حریم ارتباطات الکترونیکی هرگونه دسترسی غیرمجاز به ارتباطات الکترونیکی را جرم دانسته و مجازات‌هایی نظیر حبس و جریمه نقدی برای آن در نظر گرفته است. در اتحادیه اروپا نیز دستورالعمل ePrivacy در کنار مقررات عمومی حفاظت از داده‌ها، به حمایت از حریم ارتباطات الکترونیکی پرداخته‌اند و هرگونه پردازش یا شنود بدون رضایت داده‌محور را ممنوع اعلام کرده‌اند (European Parliament, ۲۰۱۶) .قوانین حفاظت از داده‌ها در سال‌های اخیر به عنوان ستون فقرات حمایت از کاربران در فضای مجازی عمل کرده‌اند. جی دی پی آر به عنوان پیشرفته‌ترین چارچوب قانونی در سطح جهانی، اصل رضایت آگاهانه، شفافیت در پردازش اطلاعات، و حق دسترسی به داده‌های شخصی را برای کاربران تضمین کرده است. به تبع آن، هرگونه شنود غیرمجاز سایبری، چنانچه بدون رضایت شخص صورت گیرد، نه‌تنها تخلف، بلکه جرم تلقی می‌شود.

۷- جایگاه حریم خصوصی و مقررات بین‌المللی و تبعات حقوقی شنود غیرمجاز سایبری

حریم خصوصی و محرمانگی ارتباطات، یکی از حقوق بنیادین انسان است که هم در اسناد بین‌المللی و هم در حقوق داخلی ایران مورد حمایت قرار گرفته است. مطابق اصل ۲۵ قانون اساسی جمهوری

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

اسلامی ایران، هرگونه شنود و افشای مکاتبات بدون حکم قانونی ممنوع است. (موسوی، ۱۳۹۲، ۱۴۴) همچنین ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی، مصوب ۱۹۶۶، به‌صراحت بیان می‌دارد که هیچ‌کس نباید در زندگی خصوصی، مکاتبات و ارتباطات خود مورد تعرض قرار گیرد (United Nations, ۱۹٦٦, Art. ۱۷). کنوانسیون بوداپست به‌عنوان مهم‌ترین سند بین‌المللی در حوزه جرایم سایبری، در ماده ۳ خود، بر لزوم جرم‌انگاری شنود غیرمجاز تأکید کرده و کشورها را به همکاری در جهت مقابله با این جرم فراخوانده است. (Council of Europe, ۲۰۰۱) با مقایسه این مقررات با قوانین ایران، روشن می‌شود که اگرچه قانون جرایم رایانه‌ای گام مثبتی در راستای مقابله با شنود غیرمجاز برداشته، اما هنوز با استانداردهای بین‌المللی فاصله دارد و در زمینه‌هایی مانند مصادیق دقیق جرم، حمایت از داده‌های رمزنگاری‌شده و ابزارهای اثبات، نیازمند اصلاح است (Samadi, ۲۰۱۸, ۹۲-۹۳)

حریم خصوصی یکی از ارکان اساسی کرامت انسانی و آزادی‌های فردی در جوامع مدرن به شمار می‌رود. این حق در بسیاری از اسناد بین‌المللی مانند ماده ۱۲ اعلامیه جهانی حقوق بشر و ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی مورد تأکید قرار گرفته است. در نظام حقوقی ایران نیز حریم خصوصی جایگاه ویژه‌ای دارد. ماده ۲۵ قانون اساسی جمهوری اسلامی ایران صراحتاً اعلام می‌کند که «بازرسی و نرساندن نامه‌ها، ضبط و فاش کردن مکالمات تلفنی، افشا و شنود مکاتبات تلگرافی و تلفنی و... جز به حکم قانون ممنوع است». این اصل اساسی به‌وضوح شنود اطلاعات را بدون مجوز قانونی جرم تلقی می‌کند. (قانون اساسی جمهوری اسلامی ایران، ۱۳۵۸)

در حوزه فناوری‌های نوین و ارتباطات سایبری، نقض حریم خصوصی می‌تواند آثار حقوقی و اجتماعی گسترده‌ای داشته باشد. شنود غیرمجاز داده‌ها و مکالمات افراد می‌تواند منجر به ایجاد ترس، ناامنی روانی، آسیب به اعتبار فردی و حتی تحریف یا سوءاستفاده از اطلاعات شود. از این‌رو، قوانین متعددی برای مقابله با این تهدیدها تصویب شده است. به‌ویژه قانون تجارت الکترونیکی ایران در ماده ۵۸، بر لزوم محرمانه بودن اطلاعات کاربران و ممنوعیت هرگونه افشای غیرمجاز تأکید می‌کند. همچنین، قانون حمایت از حقوق مصرف‌کنندگان خدمات ارتباطی نیز اپراتورها و ارائه‌دهندگان خدمات را موظف به حفظ اسرار مشتریان کرده است (قانون تجارت الکترونیکی، ۱۳۸۲؛ قانون جرایم رایانه‌ای،

۱۳۸۸).در مجموع، شنود سایبری نه‌تنها یک رفتار غیراخلاقی بلکه نقض یک حق بنیادین تلقی می‌شود که دارای تبعات کیفری، مدنی و حتی اداری برای متخلفان خواهد بود. (دهقان، ۱۴۰۱، ۲۵)

۷-۱- دلایل جرم‌انگاری شنود غیرمجاز

جرم‌انگاری شنود غیرمجاز در حقوق کیفری مدرن پاسخی به ضرورت حمایت از حریم خصوصی افراد در عصر اطلاعات است. شنود غیرمجاز نه‌تنها به آزادی‌های فردی و حق خلوت اشخاص تجاوز می‌کند، بلکه با آسیب رساندن به اعتماد عمومی، بنیان‌های جامعه مدنی را نیز تهدید می‌نماید. در نظام‌های حقوقی امروزی، امنیت ارتباطات، چه در سطح فردی و چه در سطح نهادی، از مؤلفه‌های بنیادین نظم عمومی به شمار می‌رود و هرگونه خدشه به آن، تهدیدی برای ثبات اجتماعی تلقی می‌شود.علاوه بر این، شنود غیرمجاز می‌تواند زمینه‌ساز ارتکاب سایر جرایم از جمله اخاذی، افشای اسرار تجاری، تهدید، یا انتشار محتوای خصوصی در فضای عمومی باشد. از منظر اقتصادی، ورود غیرمجاز به اطلاعات ارتباطی، به‌ویژه در حوزه‌های تجاری یا نظامی، ممکن است زیان‌های جبران‌ناپذیری را برای اشخاص حقیقی یا حقوقی به همراه داشته باشد. حتی در صورتی که اطلاعات شنودشده افشا نگردد، صرف آگاهی افراد غیرمجاز از محتوای ارتباطات ممکن است ارزش داده‌ها را کاهش داده یا موجب تغییر رفتار مخاطبان گردد. (دهقان، ۱۴۰۱، ۱۲) بنابراین، جرم‌انگاری شنود غیرمجاز توجیهی روشن در حفاظت از حقوق بنیادین بشر، حمایت از امنیت ملی و تضمین سلامت فضای دیجیتال دارد و از دیدگاه سیاست جنایی، ابزاری برای پیشگیری اجتماعی و حقوقی محسوب می‌شود.

۷-۲- تحلیل تطبیقی قوانین مرتبط با محتوای مستهجن، شنود غیرمجاز و حریم خصوصی در نظام حقوقی ایران

با توسعه روزافزون فناوری‌های اطلاعاتی و گسترش استفاده از سامانه‌های رایانه‌ای و ابزارهای ارتباطی، نظام حقوقی ایران نیز تلاش کرده است تا با وضع قوانین مناسب، به چالش‌های نوین در حوزه حفاظت از حریم خصوصی، مبارزه با محتوای مستهجن و کنترل شنودهای غیرمجاز پاسخ دهد. در این زمینه دو قانون کلیدی مورد توجه قرار گرفته‌اند: قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیرمجاز می‌نمایند (مصوب ۱۳۸۶) و قانون جرایم رایانه‌ای (مصوب ۱۳۸۸).

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

الف. قانون سمعی و بصری: تمرکز بر آثار فیزیکی و سنتی

قانون سمعی و بصری با هدف کنترل و مقابله با تولید و توزیع آثار مستهجن و مبتذل تصویب شده است. این قانون عمدتاً بر بسترهای سنتی مانند نوارهای ویدئویی و دی‌وی‌دی تمرکز دارد. در این قانون، رفتارهایی چون تولید، تکثیر، توزیع، نمایش و نگهداری آثار خلاف عفت عمومی جرم‌انگاری شده‌اند. تمرکز اصلی قانون بر محتوای آثار و میزان تعارض آن‌ها با ارزش‌های اخلاقی جامعه است، نه لزوماً ابزار یا فناوری مورد استفاده.با این حال، با گسترش فناوری و ظهور اینترنت، ابزارهای جدیدی برای ارتکاب این‌گونه جرایم فراهم شده‌اند که قانون سمعی و بصری در مواجهه با آن‌ها ظرفیت اجرایی محدودی دارد. به‌ویژه، این قانون قادر به پوشش‌دهی مؤثر جرایم صورت‌گرفته در بستر دیجیتال نیست و همین امر موجب شد قانون‌گذار در ادامه، قانون جرایم رایانه‌ای را تدوین کند. (آقایی‌نیا و عابد، ۱۳۹۱، ۲۲)

ب. قانون جرایم رایانه‌ای: پاسخ به تهدیدهای نوپدید در بستر دیجیتال

در پاسخ به خلأهای موجود، قانون جرایم رایانه‌ای در سال ۱۳۸۸ تصویب شد. این قانون با رویکردی فناورانه، تلاش کرده است تا دامنه وسیع‌تری از جرایم نوپدید از جمله تولید و انتشار محتوای مستهجن در بستر دیجیتال، شنود غیرمجاز، دسترسی غیرمجاز، تخریب داده‌ها و جاسوسی سایبری را مورد شناسایی قرار دهد.ویژگی برجسته این قانون در مقایسه با قانون سمعی و بصری آن است که تمرکز آن بر چگونگی ارتکاب جرم و ابزارهای الکترونیکی است. همچنین، داده‌های ترافیکی، ارتباطات رمزنگاری‌شده، سامانه‌های ارتباطی خصوصی، و حتی اطلاعات ذخیره‌شده در رایانه‌ها تحت حمایت قرار گرفته‌اند. به‌علاوه، این قانون علاوه بر تولیدکنندگان محتوای مجرمانه، به مجازات توزیع‌کنندگان و مصرف‌کنندگان آن نیز پرداخته است. (دهقان، ۱۴۰۱، ۹۴)

پ. تحلیل هم‌پوشانی‌ها، تعارض‌ها و خلأهای تقنینی

اگرچه هر دو قانون به موضوع مقابله با محتوای مستهجن و حمایت از حریم خصوصی پرداخته‌اند، تفاوت‌هایی در محدوده اجرایی، نوع ابزار، و مفهوم جرم وجود دارد. قانون سمعی و بصری قانون خاص محسوب می‌شود و در مورد آثار صوتی و تصویری در قالب فیزیکی اولویت دارد. در مقابل، قانون جرایم رایانه‌ای قانون عام‌تری است که جرایم ارتکابی در فضای دیجیتال را پوشش می‌دهد. در مواردی

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

که تعارض اجرایی یا تفسیر وجود داشته باشد، اصل "تقدم قانون خاص بر عام" اعمال می‌شود.با وجود این، برخی خلأها هنوز پابرجاست؛ از جمله عدم تعریف دقیق از مرزهای حریم خصوصی در فضای دیجیتال، نبود چارچوب روشن برای شنودهای قانونی توسط نهادهای امنیتی، و تداخل صلاحیت نهادهای نظارتی در مواجهه با محتواهای مستهجن دیجیتال. این چالش‌ها ضرورت بازنگری و به‌روزرسانی قوانین با نگاه جامع به تحولات فناورانه را نشان می‌دهد. (آقایی‌نیا و عابد، ۱۳۹۱، ۲۴)

۷-۳- مجازات‌ها و عواقب شنود غیرمجاز و بررسی در حقوق ایران

در نظام حقوق کیفری ایران، مجازات‌ها متناسب با شدت، تکرار و نتایج جرم اعمال می‌شود. در خصوص شنود غیرمجاز، قانون جرایم رایانه‌ای مصوب ۱۳۸۸، به‌ویژه ماده ۲۱، مجازات‌هایی شامل حبس و جزای نقدی را در نظر گرفته است. مجازات مقرر در این ماده از شش ماه تا دو سال حبس یا جزای نقدی از پنج تا چهل میلیون ریال تعیین شده است. با این حال، شدت مجازات در صورتی افزایش می‌یابد که شنود منجر به آسیب‌های گسترده‌تری مانند افشای اطلاعات طبقه‌بندی‌شده یا اسرار تجاری و شخصی گردد. (قانون جرایم رایانه‌ای، ۱۳۸۸) از سوی دیگر، مرتکب ممکن است علاوه بر مجازات کیفری، با عواقب مدنی نیز روبه‌رو شود؛ از جمله الزام به جبران خسارات مادی و معنوی وارد شده به شخص یا اشخاص قربانی. در مواردی که شنود توسط اشخاص حقوقی نظیر اپراتورها یا کارکنان نهادهای دولتی صورت گیرد، امکان پیگرد اداری و انضباطی نیز وجود دارد. به‌ویژه با توجه به مسئولیت اشخاص حقوقی در حفظ داده‌های کاربران، نقض این تعهد می‌تواند به توقیف فعالیت، تعلیق مجوز یا جریمه‌های سنگین بیانجامد. (بهرمند و فراهانی، ۱۳۹۳، ۴۰) به‌علاوه، از منظر سیاست جنایی تقنینی، شدت برخورد با این پدیده نشان از اهمیت حفظ امنیت اطلاعاتی و اعتماد عمومی در جامعه اطلاعاتی دارد. قانون‌گذار با پیش‌بینی ضمانت اجراهای متنوع، تلاش کرده است ضمن حمایت از حقوق افراد، زمینه سوءاستفاده از فناوری را به حداقل برساند. (دهقان، ۱۴۰۱، ۲۷)

در پاسخ به چالش‌های نوین ناشی از گسترش فناوری اطلاعات، قانون‌گذار ایرانی در قانون جرایم رایانه‌ای، تدابیری برای جرم‌انگاری و مقابله با شنود غیرمجاز در فضای سایبری پیش‌بینی کرده است. طبق ماده ۱ قانون مذکور، هرگونه دسترسی غیرمجاز به داده‌ها، اطلاعات و سیستم‌های رایانه‌ای جرم تلقی شده و مشمول مجازات خواهد بود. اما تمرکز اصلی بر ماده ۲۱ این قانون است که به‌طور خاص

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

رفتار شنود یا استراق سمع داده‌ها و ارتباطات غیرعمومی را تحت عنوان جرم جداگانه مطرح کرده است.ماده ۲۱ قانون جرایم رایانه‌ای تصریح می‌کند: «هرکس به طور غیرمجاز محتوای در حال انتقال در سامانه‌های رایانه‌ای یا مخابراتی را شنود کند، به حبس از شش ماه تا دو سال یا جزای نقدی از پنج میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد». (قانون جرایم رایانه‌ای، ۱۳۸۸) این ماده علاوه بر تأکید بر عنصر «غیرمجاز بودن»، به ماهیت خاص داده‌ها و بستر ارتکاب جرم (یعنی سیستم‌های رایانه‌ای و مخابراتی) توجه دارد.مهم‌تر از آن، اگر شنود منجر به افشای اطلاعات شخصی، تجاری یا دولتی شود، امکان دارد جرایم دیگری چون افشای اسرار شخصی (ماده ۶۴۸ قانون مجازات اسلامی)، نقض امنیت ملی یا اختلال در نظم عمومی نیز متوجه مرتکب گردد. بنابراین، قانون‌گذار ایرانی کوشیده است تا از طریق تعیین مجازات‌های متنوع، از جمله حبس، جریمه نقدی و حتی محرومیت از حقوق اجتماعی، جنبه بازدارنده‌ای برای چنین جرمی ایجاد نماید. (آقایی‌نیا و عابد، ۱۳۹۱، ۵۳)

۸- تحلیل چالش‌های قانونی شنود سایبری در ایران و ضرورت اصلاحات ساختاری

با گسترش روزافزون فناوری‌های ارتباطی، حفاظت از داده‌های شخصی و جلوگیری از شنود غیرمجاز در فضای سایبری به یکی از چالش‌های جدی حقوقی در ایران تبدیل شده است. با وجود تلاش‌های قانون‌گذار برای جرم‌انگاری دسترسی‌های غیرمجاز، به نظر می‌رسد که قوانین موجود، به ویژه در مواجهه با پدیده‌ی نوظهور شنود سایبری، با خلأها و ابهامات قابل توجهی روبرو هستند.ماده ۷۲۹ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ مقرر کرده است:هرکس به طور غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات محکوم می‌شود.این ماده، گرچه به دسترسی غیرمجاز به سامانه‌های حفاظت شده می‌پردازد، اما به طور صریح ارتباطی با شنود ارتباطات در حین انتقال یا رهگیری داده‌های جاری در شبکه برقرار نمی‌کند. این ابهام، تفاسیر گوناگون قضایی را ممکن می‌سازد و در نهایت ممکن است به تضییع حقوق قربانیان بیانجامد. (اردبیلی، ۱۳۹۵، ۱۸۷)

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

ماده ۵۸۲ قانون مجازات اسلامی نیز هرچند به ضبط یا انتشار صوت و تصویر بدون رضایت اشخاص اشاره دارد، اما در خصوص شنود داده‌های متنی یا شنود همزمان مکالمات آنلاین، صراحت قانونی ندارد (مرکز ملی فضای مجازی، ۱۴۰۰). در نتیجه، این نارسایی‌ها در متن قوانین سبب می‌شود که دعاوی مرتبط با شنود سایبری عمدتاً بر پایه تفاسیر موسع و برداشت‌های قضات از قواعد کلی جرم‌انگاری مورد رسیدگی قرار گیرد.نگاهی به رویه عملی نیز نشان‌دهنده برخوردهای متفاوت محاکم قضایی است. برای نمونه، در سال ۱۳۹۷ در دادگاه کیفری استان اصفهان، فردی که بدون اجازه به حساب ایمیل دیگران دسترسی یافته و ارتباطات آنان را شنود کرده بود، به دو سال حبس و پرداخت جریمه نقدی محکوم شد (گزارش پلیس فتا، ۱۳۹۷). همچنین در سال ۱۳۹۹، فردی که اقدام به نصب نرم‌افزار جاسوسی بر گوشی‌های دیگران کرده بود، با مجازات پنج سال حبس و جریمه نقدی روبرو شد. (گزارش پلیس فتا، ۱۴۰۰) این احکام، ضمن آنکه اهمیت موضوع را برجسته می‌سازند، ضرورت تدوین مقررات ویژه و شفاف در این زمینه را بیش از پیش آشکار می‌کنند.

۸-۱- بررسی قوانین ناظر بر شنود مکالمات در حقوق کیفری ایران

شنود مکالمات، چه در قالب سنتی آن و چه در قالب‌های نوین دیجیتالی، در حقوق کیفری ایران مورد توجه قانون‌گذار قرار گرفته و به‌طور خاص و عام، مقررات متعددی در مورد آن وضع شده است. قانون اساسی جمهوری اسلامی ایران، به‌عنوان سند بالادستی نظام حقوقی کشور، در اصل ۲۵ به صراحت اعلام می‌دارد که «بازرسی و نرساندن نامه‌ها، ضبط و افشای مکالمات تلفنی، افشا و تجسس، مگر به حکم قانون، ممنوع است». این اصل ضمن تأکید بر لزوم احترام به حریم خصوصی ارتباطات، هرگونه ورود به آن را مشروط به تصویب و رعایت دقیق قواعد قانونی می‌داند. بر این اساس، شنود مکالمات به‌مثابه نوعی از تجسس در ارتباطات خصوصی افراد، صرفاً در صورتی قابل پذیرش است که مستند به مجوز قانونی باشد؛ در غیر این صورت، ناقض حقوق شهروندی و مستوجب مجازات خواهد بود. در امتداد این رویکرد، قانون مجازات اسلامی نیز به‌طور صریح به جرم‌انگاری شنود غیرمجاز پرداخته است. بر اساس ماده ۵۸۲ این قانون، هرگاه مأموران دولتی یا وابسته به نهادهای عمومی، بدون مجوز قانونی، اقدام به شنود مکالمات تلفنی یا افشای آن‌ها نمایند، به مجازات حبس از یک تا سه سال یا جزای نقدی محکوم خواهند شد. این ماده، به‌طور خاص متوجه مأموران دولتی است و نشان می‌دهد که قانون‌گذار برای تخطی‌کنندگان از درون دستگاه حاکمیتی، ضمانت اجرای کیفری

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

خاصی در نظر گرفته است. این در حالی است که چنان‌چه افراد عادی نیز مرتکب چنین رفتاری شوند، می‌توان از طریق عمومات قانون جرایم رایانه‌ای یا سایر مقررات کیفری با آن‌ها برخورد کرد.

در همین راستا، قانون آیین دادرسی کیفری مصوب ۱۳۹۲ با اصلاحات بعدی نیز به‌طور دقیق‌تری به موضوع شنود مکالمات پرداخته و در ماده ۱۵۰ اعلام کرده است که «کنترل ارتباطات مخابراتی، مکاتبات، محتوای پیام‌ها و داده‌های رایانه‌ای، صرفاً در مواردی که به امنیت داخلی یا خارجی کشور مربوط باشد یا برای کشف جرایم سازمان‌یافته، تروریسم یا جرایم مهم دیگر ضرورت داشته باشد، آن هم با اجازه مقام قضایی ممکن خواهد بود». بدین ترتیب، اصل بر ممنوعیت مطلق هرگونه نظارت و شنود است و تنها در شرایط استثنایی و بر اساس اصول ضرورت، تناسب، و با مجوز قضایی می‌توان به این اقدامات مبادرت ورزید. از منظر حقوق تطبیقی نیز چنین اصل و رویه‌ای در نظام‌های حقوقی توسعه‌یافته پذیرفته شده و تنها با رعایت شرایط خاص، امکان شنود مجاز فراهم می‌گردد. علاوه بر این‌ها، قانون جرایم رایانه‌ای مصوب ۱۳۸۸ با هدف تنظیم مقررات کیفری متناسب با فناوری‌های نوین ارتباطی به تصویب رسید و در مواد مختلف خود به جرم‌انگاری شنود غیرمجاز پرداخت. بر اساس ماده ۲ این قانون، هرکس به طور غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی دسترسی پیدا کند، مجرم شناخته می‌شود. همچنین ماده ۴ قانون یادشده به‌طور خاص، شنود اطلاعات در حال انتقال از طریق سامانه‌های رایانه‌ای یا مخابراتی را جرم دانسته و برای آن مجازات تعیین کرده است. مهم‌ترین ویژگی این قانون آن است که برخلاف قوانین پیشین، صراحتاً به ابزارها و بسترهای دیجیتالی اشاره کرده و شنود را از قالب سنتی و فیزیکی آن فراتر برده است. در ماده ۴۸ این قانون و تبصره آن، شنود مجاز نیز تعریف شده و شروط قانونی برای انجام آن، نظیر وجود مجوز قضایی و ضرورت امنیتی یا کیفری، به‌روشنی بیان شده است.قانون جرایم رایانه‌ای، با الهام از اسناد بین‌المللی مانند کنوانسیون جرایم سایبری شورای اروپا (موسوم به کنوانسیون بوداپست)، تلاش کرده است تا ضمن برخورد با رفتارهای نوپدید مجرمانه، از حقوق بنیادین شهروندان در فضای سایبری نیز حمایت کند. با این حال، به‌رغم رویکرد نوآورانه قانون یادشده، برخی چالش‌ها نظیر شفاف‌نبودن معیارهای ضرورت امنیتی یا نبود سازوکار نظارتی مؤثر بر اجرای شنود مجاز، همچنان باقی است و نیازمند اصلاحات تکمیلی است.

۸-۲- راهکارهای مقابله با شنود غیرمجاز

مقابله با شنود غیرمجاز در دنیای دیجیتال امروزی نیازمند رویکردهای جامع و مؤثری است که بتواند ابعاد مختلف این تهدید را پوشش دهد. از آنجا که شنود غیرمجاز نه تنها به تهدیدی برای حریم خصوصی افراد، بلکه برای امنیت ملی و بین‌المللی تبدیل شده است، ضرورت اتخاذ تدابیر پیشگیرانه، قانونی، فنی و آموزشی بیش از پیش احساس می‌شود.

۸-۲-۱- تدوین و تقویت چارچوب‌های قانونی بین‌المللی

یکی از مهم‌ترین گام‌ها در مقابله با شنود غیرمجاز، ایجاد چارچوب‌های قانونی بین‌المللی است. برای جلوگیری از گسترش این پدیده در سطح جهانی، کشورها باید در همکاری با نهادهای بین‌المللی مانند پلیس بین‌الملل و سازمان ملل متحد، قوانین و مقرراتی را تدوین کنند که علاوه بر مقابله با شنود غیرمجاز، به جلوگیری از استفاده غیرمجاز از داده‌ها و اطلاعات شخصی نیز بپردازد. (جعفری، ۱۴۰۲، ۱۱۲) این قوانین باید شامل استراتژی‌های مشترک برای شناسایی و تعقیب مجرمان سایبری و همچنین تبادل اطلاعات به‌روز در مورد تهدیدات امنیتی باشد. به این ترتیب، علاوه بر تقویت امنیت سایبری، اعتماد عمومی نسبت به فضای دیجیتال نیز افزایش خواهد یافت.

۸-۲-۲- ارتقاء فناوری‌های امنیتی و ابزارهای رمزنگاری

یکی دیگر از راهکارهای مؤثر در مقابله با شنود غیرمجاز، توسعه و پیاده‌سازی ابزارهای امنیتی پیشرفته است. شرکت‌های فناوری باید مسئولیت‌پذیری بیشتری در برابر امنیت اطلاعات کاربران خود داشته باشند و محصولات خود را با استفاده از آخرین استانداردهای رمزنگاری و امنیتی روانه بازار کنند. ابزارهای رمزنگاری، به‌ویژه رمزنگاری end-to-end برای پیام‌رسان‌ها و ارتباطات آنلاین، می‌توانند مانع از دسترسی غیرمجاز به داده‌های کاربران شوند. (نوروزی، ۱۴۰۱، ۴۵) همچنین، استفاده از فناوری‌هایی چون بلاک‌چین برای تضمین امنیت اطلاعات و جلوگیری از دستکاری آن‌ها می‌تواند راهی مؤثر در این زمینه باشد. شرکت‌ها باید به‌طور مداوم به‌روزرسانی‌های امنیتی را برای رفع آسیب‌پذیری‌ها ارائه دهند و کاربران را از خطرات موجود آگاه کنند.

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

۸-۲-۳- آگاهی‌بخشی و آموزش عمومی

افزایش آگاهی عمومی در خصوص تهدیدات شنود غیرمجاز و شیوه‌های حفاظت از اطلاعات، یکی از اساسی‌ترین ارکان مقابله با این پدیده است. آموزش‌های امنیت سایبری باید از طریق رسانه‌ها، شبکه‌های اجتماعی و کارگاه‌های آموزشی در دسترس عموم قرار گیرد. به‌ویژه، سازمان‌ها و نهادهای دولتی می‌توانند با برگزاری کمپین‌های آموزشی، کاربران را از روش‌های ایمن برای حفظ حریم خصوصی‌شان آگاه کنند. این آموزش‌ها باید به گونه‌ای طراحی شوند که تمامی اقشار جامعه، از جمله افرادی که به تکنولوژی دسترسی محدودی دارند، بتوانند از آن بهره‌مند شوند. (موسوی، ۱۴۰۱، ۸۳) این امر می‌تواند به کاهش آسیب‌پذیری‌ها و ارتقاء سطح امنیت دیجیتال در جامعه منجر شود.

۸-۲-۴- تقویت همکاری‌های بین‌المللی و ملی در مبارزه با جرایم سایبری

همکاری میان کشورها و نهادهای بین‌المللی در زمینه تبادل اطلاعات و بررسی تهدیدات سایبری، اهمیت بسیاری دارد. کشورها باید معاهدات و توافق‌نامه‌های بین‌المللی برای تسهیل دسترسی به اطلاعات امنیتی، شناسایی و تعقیب مجرمان سایبری ایجاد کنند. علاوه بر این، همکاری با آژانس‌های امنیتی مانند پلیس بین‌الملل و اف‌بی‌آی می‌تواند در تسریع فرآیند پیگیری مجرمان سایبری مؤثر باشد. (کرمانی، ۱۴۰۲، ۵۷) همچنین، کشورهای مختلف باید برای پیشگیری از شنودهای غیرمجاز، قوانین هماهنگ و همگن در سطح ملی تدوین کنند که به صورت شفاف و دقیق به مقابله با این تهدیدات پرداخته و همزمان، به حقوق کاربران نیز احترام بگذارد.

۸-۲-۵- پیشگیری از آسیب‌پذیری‌ها در دستگاه‌های اینترنت اشیا (IoT)

یکی از روش‌های نوین شنود غیرمجاز که به‌ویژه در سال‌های اخیر شایع شده، استفاده از آسیب‌پذیری‌های دستگاه‌های اینترنت اشیا است. این دستگاه‌ها به دلیل اتصال به اینترنت و عدم توجه کافی به امنیت، به هدفی جذاب برای مهاجمان تبدیل شده‌اند. به همین دلیل، توسعه استانداردهای امنیتی برای دستگاه‌های IoT و استفاده از پروتکل‌های رمزگذاری در داده‌های منتقل‌شده، ضروری است. همچنین، نظارت و پیگیری آسیب‌پذیری‌ها در این دستگاه‌ها می‌تواند به جلوگیری از سوءاستفاده‌ها و شنودهای غیرمجاز کمک کند. (موسوی، ۱۴۰۱، ۸۳)

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

۸-۲-۶- تقویت زیرساخت‌های امنیتی در سطح دولتی و خصوصی

دولت‌ها و سازمان‌ها باید زیرساخت‌های امنیتی خود را تقویت کرده و از فناوری‌های نوین در مدیریت اطلاعات و داده‌های حساس استفاده کنند. این امر به‌ویژه در سازمان‌هایی که اطلاعات حیاتی و حساس را مدیریت می‌کنند، از اهمیت ویژه‌ای برخوردار است. همچنین، همکاری میان نهادهای دولتی و خصوصی در توسعه و اجرای سیستم‌های امنیتی می‌تواند موجب تقویت دفاع سایبری و کاهش آسیب‌پذیری‌های اطلاعاتی شود.در مجموع، راهکارهای مقابله با شنود غیرمجاز نیازمند رویکردی چندجانبه است که به‌طور همزمان با ابعاد فنی، قانونی، آموزشی و همکاری‌های بین‌المللی به تهدیدات مربوطه پاسخ دهد. اجرای این راهکارها به طور مؤثر می‌تواند زمینه‌ساز ایجاد یک محیط دیجیتال امن‌تر و حفاظت‌شده‌تر برای تمامی کاربران باشد.

۹- راهکارهای پیشگیرانه برای جلوگیری از شنود غیرمجاز سایبری

با توجه به پیچیدگی‌ها و گسترش جرایم سایبری، به‌ویژه پدیده شنود غیرمجاز، اتخاذ راهکارهای پیشگیرانه در ابعاد فنی، حقوقی، آموزشی و فرهنگی از اهمیت بالایی برخوردار است. هدف این راهکارها، کاهش مخاطرات ناشی از شنود غیرمجاز و ارتقای امنیت اطلاعات در فضای دیجیتال است.یکی از مهم‌ترین اقدامات پیشگیرانه، تقویت زیرساخت‌های امنیتی است. این اقدام شامل استفاده از فناوری‌های نوین مانند رمزنگاری پیشرفته، فایروال‌ها، سیستم‌های تشخیص و پیشگیری از نفوذ و مکانیزم‌های احراز هویت قوی می‌شود. ایجاد ساختارهای فنی مستحکم می‌تواند مانع دسترسی غیرمجاز به اطلاعات و ارتباطات خصوصی شود. (مرکز ملی فضای مجازی، ۱۴۰۰؛ اردبیلی، ۱۳۹۵، ۵۶) آموزش و آگاهی‌بخشی عمومی نیز نقش اساسی در پیشگیری از شنود غیرمجاز دارد. شهروندان باید با مخاطرات موجود در فضای مجازی و روش‌های حفاظت از اطلاعات شخصی آشنا شوند. این آموزش‌ها باید از طریق رسانه‌های جمعی، برنامه‌های درسی در مدارس و دانشگاه‌ها، و کارگاه‌های آموزشی برای اقشار مختلف جامعه ارائه شود. (میرمحمدصادقی، ۱۳۹۸، ۶۰-۴۵) افزایش سواد دیجیتال، توانایی کاربران برای محافظت از خود در برابر تهدیدات سایبری را افزایش می‌دهد.در بعد حقوقی، اصلاح و به‌روزرسانی قوانین موجود با هدف تطبیق با تحولات فناوری ضروری است. قوانین باید تعریف دقیق‌تری از جرایم سایبری، از جمله شنود غیرمجاز، ارائه دهند و با در نظر گرفتن شدت

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

آسیب‌های ناشی از این جرایم، مجازات‌های متناسبی تعیین کنند. این امر نه تنها موجب ارتقای بازدارندگی می‌شود، بلکه امنیت حقوقی کاربران را نیز تضمین می‌کند. (قانون جرایم رایانه‌ای مصوب ۱۳۸۸؛ قانون مجازات اسلامی مصوب ۱۳۹۲)

از دیگر راهبردهای ضروری، افزایش همکاری بین‌المللی در مبارزه با شنود غیرمجاز سایبری است. باتوجه به ماهیت فراملی فضای مجازی، کشورها باید از طریق نهادهایی چون پلیس بین‌الملل و کنوانسیون‌هایی مانند بوداپست (۲۰۰۱)، به تبادل اطلاعات، آموزش نیروهای تخصصی و اجرای عملیات‌های مشترک امنیت سایبری بپردازند. (Budapest Convention, ۲۰۰۱) همکاری‌های فرامرزی می‌تواند موانع اجرای عدالت در جرایم سایبری را کاهش دهد.از منظر فنی، استفاده از نرم‌افزارهای امنیتی مانند آنتی‌ویروس‌ها، ضدجاسوس‌افزارها و ابزارهای رمزنگاری پیشرفته، از دیگر ابزارهای مقابله با شنود غیرمجاز به شمار می‌رود. این نرم‌افزارها با شناسایی و حذف تهدیدات احتمالی، نقش مؤثری در پیشگیری از نفوذ به سامانه‌های ارتباطی دارند (مرکز ملی فضای مجازی، ۱۴۰۰). همچنین، نظارت و کنترل دسترسی‌ها به اطلاعات و سیستم‌های ارتباطی باید با دقت اعمال شود. استفاده از روش‌هایی مانند احراز هویت دو مرحله‌ای، محدودسازی سطح دسترسی کاربران، و ثبت فعالیت‌های سیستمی، از راهکارهای کارآمد برای کاهش احتمال نفوذ است.در نهایت، بررسی و ارزیابی مستمر امنیتی سیستم‌های اطلاعاتی، از طریق تست نفوذ، شناسایی آسیب‌پذیری‌ها و به‌روزرسانی مداوم نرم‌افزارها و زیرساخت‌ها، ضرورتی اجتناب‌ناپذیر در ارتقای امنیت سایبری محسوب می‌شود. این فرایندهای ارزیابی، امکان شناسایی نقاط ضعف را فراهم می‌کند و از بروز مخاطرات احتمالی پیشگیری می‌نماید. (اردبیلی، ۱۳۹۵، ۵۶) مجموع این راهکارها در قالب یک سیاست کلان پیشگیری سایبری می‌تواند زمینه‌ساز کاهش وقوع جرایم شنود غیرمجاز در فضای مجازی و ارتقای امنیت ملی، فردی و نهادی در حوزه سایبری شود.

دومین محور، نهادینه‌سازی فرهنگ امنیت سایبری در سطح عمومی جامعه و نهادهای اجرایی است. آموزش‌های مستمر درباره تهدیدات سایبری، روش‌های ایمن‌سازی ارتباطات دیجیتال، و ترویج مسئولیت‌پذیری کاربران از مراحل ابتدایی آموزش رسمی گرفته تا ساختارهای اداری، از ملزومات مقابله مؤثر با شنود غیرمجاز محسوب می‌شود. (میرمحمدصادقی، ۱۳۹۸، ۵۲) کاربران آگاه، خود نخستین خط دفاعی در برابر تهدیدات سایبری هستند.در گام سوم، تحول قانون‌گذاری در حوزه

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

جرایم سایبری باید با سرعت و دقت انجام گیرد. قوانین فعلی مانند قانون جرایم رایانه‌ای ۱۳۸۸ و قانون مجازات اسلامی ۱۳۹۲ پاسخ‌گوی تمامی ابعاد شنود سایبری نیستند. جرم‌انگاری مستقل شنود اینترنتی، تعیین مرزهای مشروع برای نظارت قانونی، پیش‌بینی ضمانت‌اجراهای خاص برای نقض حریم خصوصی در فضای مجازی و تشدید مجازات‌ها در موارد سازمان‌یافته، از جمله اقدامات تقنینی ضروری است (اردبیلی، ۱۳۹۵، ۱۴). با توجه به ماهیت فراملی جرایم سایبری، تحکیم همکاری‌های بین‌المللی چهارمین ضرورت اساسی محسوب می‌شود. پیوستن به اسناد بین‌المللی مانند کنوانسیون بوداپست، تبادل داده‌ها، آموزش نیروهای متخصص، و انجام عملیات‌های مشترک از جمله ابزارهای مؤثر در مقابله جهانی با شنود غیرمجاز است.(Council of Europe, ۲۰۰۱) . در کنار این راهکارها، استفاده گسترده از نرم‌افزارهای امنیتی، مانند آنتی‌ویروس‌ها، ضدجاسوس‌افزارها و ابزارهای رمزنگاری، نقش بسزایی در جلوگیری از نفوذ غیرمجاز و استراق سمع ایفا می‌کند. (اردبیلی، ۱۳۹۵، ۱۴) بهره‌گیری از نرم‌افزارهای بومی و مطمئن می‌تواند آسیب‌پذیری سامانه‌ها را در برابر تهدیدات خارجی به حداقل برساند.نظارت مستمر بر دسترسی‌ها به سامانه‌های اطلاعاتی و کنترل‌های دقیق مدیریتی، گام بعدی در این مسیر است. اجرای احراز هویت چندمرحله‌ای، محدودسازی دسترسی‌های غیرضروری و ثبت دقیق فعالیت کاربران می‌تواند از بروز سوءاستفاده‌ها و شنود غیرمجاز جلوگیری کند (مرکز ملی فضای مجازی ایران، ۱۴۰۰). در نهایت، انجام ارزیابی‌های امنیتی مستمر شامل تست‌های نفوذ، تحلیل آسیب‌پذیری‌ها و به‌روزرسانی منظم سیستم‌ها، از ارکان اساسی برای حفظ پویایی و تاب‌آوری ساختارهای سایبری است. بی‌توجهی به این امر می‌تواند حتی امن‌ترین زیرساخت‌ها را نیز در معرض خطر قرار دهد.در مجموع، مقابله مؤثر با شنود غیرمجاز در فضای سایبری نیازمند رویکردی چندلایه و نظام‌مند است. تنها از طریق ترکیب سیاست‌گذاری‌های حقوقی، اقدامات فنی، فرهنگ‌سازی عمومی و تعاملات بین‌المللی می‌توان امنیت پایدار اطلاعات و حفظ حریم خصوصی را تضمین کرد.

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

نتیجه‌گیری

در مواجهه با پدیده روزافزون شنود غیرمجاز در فضای سایبری، اتخاذ راهکارهای بنیادین و چندبُعدی ضرورتی انکارناپذیر برای تضمین امنیت اطلاعات و صیانت از حریم خصوصی افراد به شمار می‌رود. این اقدامات باید ابعاد فنی، حقوقی، فرهنگی و بین‌المللی را در بر گیرد تا بتوانند کارایی لازم را در برابر این تهدید پیچیده فراهم سازند. نخستین و بنیادی‌ترین اقدام، بازآرایی زیرساخت‌های فنی امنیت اطلاعات است. استفاده از فناوری‌های نوین رمزنگاری، احراز هویت چندمرحله‌ای، شبکه‌های خصوصی مجاز، و سامانه‌های پیشرفته شناسایی نفوذ، باید به‌عنوان ارکان اصلی طراحی و پیاده‌سازی سامانه‌های اطلاعاتی و مخابراتی مورد توجه قرار گیرد. بدون این تمهیدات فنی، حتی سخت‌گیرانه‌ترین قوانین نیز ناکارآمد خواهند بود.

شماره مجوز انتشار: ۸۷۰۱۹ ISSN: ۲۷۸۳-۱۳۲۹

منابع

۱. اردبیلی، م. (۱۳۹۵). حقوق جزای عمومی (جلد دوم). تهران: میزان.
۲. اردبیلی، م.ع. (۱۳۹۵). جرایم سایبری و حقوق کیفری ایران. تهران: انتشارات میزان.
۳. انصاری، ب. (۱۳۸۳). حریم خصوصی و حمایت از آن در حقوق اسلام تطبیقی و ایران. مجله دانشکده حقوق و علوم سیاسی، ۶۶، ۴۹–۵۲۰.
٤. موسوی‌تبریزی، علی‌محمد. (۱۳۸۷). فقه جزایی تطبیقی. قم: نشر مجتهد. ص ۷۹.
٥. میرمحمدصادقی، ح. (۱۳۸۷). جرائم علیه اشخاص (چاپ دوم). تهران: نشر میزان.
٦. میرمحمدصادقی، ح. (۱۳۹۸). جرایم رایانه‌ای و حقوق کیفری سایبری. تهران: جنگل.
۷. میرمحمدصادقی، حسین. (۱۳۹۵). حقوق کیفری اختصاصی: جرائم علیه اشخاص و امنیت. تهران: نشر میزان. ص ۱۴۷.
۸. نوروزی، ف. (۱۴۰۱). چالش‌های امنیتی در فضای مجازی. شیراز: انتشارات دانش.
۹. کاظمی، ا. (۱۴۰۲). حریم خصوصی در عصر دیجیتال. تهران: نشر آگاه.
۱۰. جعفری، م. (۱۴۰۲). همکاری بین‌المللی در مقابله با جرایم سایبری. تهران: نشر بین‌الملل.

۱۱. Council of Europe. (۲۰۰۱). Convention on Cybercrime (Budapest Convention). Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/۱۸۵

۱۲. European Parliament. (۲۰۱٦). Regulation (EU) ۲۰۱٦/٦۷۹ of the European Parliament and of the Council (General Data Protection Regulation). Official Journal of the European Union. Retrieved from https://eur-lex.europa.eu/eli/reg/۲۰۱٦/٦۷۹/oj

ISSN: ۲۷۸۳-۱۳۲۹
شماره مجوز انتشار: ۸۷۰۱۹

۱۳. Kerr, O. S. (۲۰۱۸). Cybercrime's Scope: Interpreting the "Access" and "Authorization" Elements of the Computer Fraud and Abuse Act. NYU Law Review, ۹۳(٦), ۱۵۹۰–۱٦۲٤. Retrieved from https://www.nyulawreview.org/issues/volume-۹۳-number-۶/cybercrimes-scope/

۱۴. Shackelford, S. J. (۲۰۱٦). Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace. Cambridge University Press. https://doi.org/۱۰,۱۰۱۷/CBO۹۷۸۱۱۳۹۹٤۱۳٥٤

۱۵. Wright, D., & Kreissl, R. (Eds.). (۲۰۱٤). Surveillance in Europe. Routledge. https://doi.org/۱۰,٤۳۲٤/۹۷۸۰۲۰۳۷٦۷۳۰۱

۱۶. De Hert, P., & Gutwirth, S. (۲۰۰۹). Privacy, Data Protection and Law Enforcement: Opacity of the Individual and Transparency of the State. In E. Claes, A. Duff & S. Gutwirth (Eds.), Privacy and the Criminal Law (pp. ٦۱–۱۰٤). Intersentia.

۱۷. U.S. Congress. (۱۹۸٦). Electronic Communications Privacy Act of ۱۹۸٦, Pub. L. No. ۹۹–٥۰۸, ۱۰۰ Stat. ۱۸٤۸. Retrieved from https://www.congress.gov/bill/۹۹th-congress/senate-bill/۲۸۷۳

ISSN: ۲۷۸۳-۱۳۲۹
شماره مجوز انتشار: ۸۷۰۱۹

Rethinking the Legitimacy of Surveillance in the Digital Age: Emphasizing the Tension between Criminal Security and Privacy

Amirreza Mahmoudi[۱] / Sahar Alipour Noshar [۲]

Article Number: JHVMN-۲۵۰۶-۱۲۹۸

Abstract

With the advancement of information technologies and the expansion of digital interactions, electronic surveillance and its boundaries of legitimacy have become one of the most challenging issues in contemporary criminal law. Cyber eavesdropping, as an intrusion into private communications within the digital sphere, has raised fundamental questions regarding the limits of state intervention, legal requirements, and citizens' rights. This article, through a descriptive-analytical approach, reexamines the status of the offense of unauthorized eavesdropping within the framework of cybercrimes and analyzes the legal elements, as well as the existing gaps and ambiguities in legislation, interpretation, and enforcement. The findings indicate that conceptual ambiguities, the absence of effective oversight mechanisms, and inconsistencies among existing laws have undermined the legal legitimacy of surveillance in Iran’s criminal justice system. In conclusion, the study proposes legislative reforms and measures to enhance the clarity, efficiency, and legitimacy of cyber surveillance within the framework of Iran’s criminal policy.

Keywords: Unauthorized eavesdropping, cybercrime, surveillance legitimacy, privacy, Iran’s criminal policy, information security.

[۱]. Assistant Professor, Department of Law, Faculty of Humanities, Lahijan Branch, Islamic Azad University, Lahijan, Iran. amirreza.mahmodi@gmail.com

[۲]. . Master of Law, Department of Law, Lahijan Branch, Islamic Azad University, Lahijan, Iran. (Corresponding Author) sahar.alipour۹۱۱@gmail.com