ارزیابی سیاست کیفری تقنینی ایران در مقابله با نقض حریم خصوصی توسط فناوری‌های نوین اطلاعاتی و ارتباطاتی

زهرا احمدی ناطور*
دکتر حسین آقابابایی**

چکیده: امروزه، حریم خصوصی افراد به واسطه ظهور فناوری‌های نوین اطلاعاتی و ارتباطاتی در معرض تهدید قرار گرفته است. این فناوری ها، امکان دسترسی به محتوای داده‌های شخصی افراد، ردیابی، تحریف و تخریب آن‌ها و انتشار این اطلاعات در جهت اهداف غیر مجاز را فراهم می‌سازند. لیکن، همگام با ظهور این فناوری‌ها و علیرغم تاثیر آنها بر نقض حریم خصوصی، قواعد ناظر بر حمایت از زندگی خصوصی افراد، آنچنان که باید مورد توجه قرار نگرفته است. این مقاله با هدف ارزیابی سیاست کیفری تقنینی ایران در جهت مقابله با نقض حریم خصوصی افراد توسط فناوری‌های نوین اطلاعاتی و ارتباطاتی و نمایاندن نواقص و کاستی‌های آن تدوین شده است.

واژگان کلیدی: فناوری‌های نوین اطلاعاتی و ارتباطاتی، حریم خصوصی، سیاست کیفری تقنینی ایران.

* دانشجوی کارشناسی ارشد حقوق جزا و جرمشناسی دانشگاه گیلان، نویسنده مسئول مقاله ahmadi.papers@gmail.com
**. مدیر گروه حقوق و دانشیار دانشگاه گیلان

مقدمه

حریم خصوصی را می‌توان یکی از بنیادی ترین و اساسی ترین حقوق بشری تلقی کرد که با شخصیت وی ارتباط مستقیم و تنگاتنگی دارد. حق انسان در تنها بودن و با خود بودن، به وسیله دیگران مورد احترام قرار گرفتن و به دور از چشم و نگاه کنترل کننده دیگران و رها از تجسس و تفتیش دیگران زیستن، حقی است که لازمه یک شخصیت مستقل به شمار می‌آید و اساسا شخصیت انسان در پرتو این مفاهیم معنا می‌یابد. نکته مهم در مورد حریم خصوصی آن است که مفهوم و قلمرو این بعد از حق انسان، به دنبال تحولات و پیشرفت هایی که به مرور زمان در عرصه‌های مختلف صورت گرفته تحت تاثیر قرار گرفته است (رحمدل، ۱۳۸۴، ص ۱۲۰). امروزه، با توجه به ظهور فناوری های نوین اطلاعاتی و ارتباطاتی و امکان افشاء کردن اطلاعات افراد در گستره شبکه اینترنت و فراگیر شدن دامنه جرم، تعریف جدید از حریم خصوصی و رابطه جرم و مجازات بسیار مهم و متفاوت با معیارهای سنتی است (محسنی، ۱۳۸۹، ص ۱۲). ظهور این فناوری‌ها سبب شده است که حتی اشخاص عادی با امکان دسترسی به بسیاری از وسایل پیشرفته به جمع آوری، ضبط و نگهداری حجم انبوهی از اطلاعات مربوط به حریم خصوصی افراد اقدام کنند. همچنین ممکن است در خانه یا در اماکن عمومی یا در محل کار، گفتار یا رفتار یک شخص به انحاء مختلف مورد نظارت سمعی یا بصری قرار گیرد. افراد خصوصی و صاحبان بسیاری از مشاغل به دلایل متعددی متمایل به استفاده از وسایل فنی نظارت های سمعی و بصری هستند، به طوری که استفاده از تلویزیون های مدار بسته و دوربین های ویدئویی در بانک‌ها و فروشگاه‌ها و اماکن کار به یک امر رایج تبدیل شده است (گروه مطالعات حقوق عمومی، ۱۳۸۴، ص ۱). به عبارت دیگر، با ظهور این فناوری ها، جهان به دهکده‌ای کوچک تبدیل گشته که در آن هر شخصی به راحتی می‌تواند از آخرین تحولات علمی، صنعتی، سیاسی، اقتصادی، فرهنگی و غیره مطلع شود و ارتقاء سطح دانش و آگاهی‌ها امکان تسریع در پیشرفت و رشد درخت تنومند علم بشری و ایجاد رفاه و

آسایش در زندگی انسان‌ها را فراهم آورده است، اما در عین حال عدم استفاده صحیح از این فناوری‌های ارزشمند، پیامدهای نامطلوبی را نیز به دنبال داشته که یکی از آن‌ها نقض «حریم خصوصی» افراد با استفاده از این فناوری‌ها توسط برخی از اشخاص، سازمان‌ها و یا حتی دولت هاست که با اهداف مختلف صورت می‌گیرد. نفوذ به شبکه بی سیم T-Mobile و برداشت مکاتبات و فایل‌های شخصی مشتریان این شرکت معروف که در سال ۲۰۰۶ به مدت ۷ ماه ادامه داشته است (محسنی و قاسم زاده، ۱۳۸۵، ص ۲۱) و صدها مثال و پرونده دیگر حاکی از نقض حریم شخصی افراد توسط گروه‌های مختلف با استفاده از فناوری‌های نوین اطلاعاتی و ارتباطاتی است. بنابراین باتوجه به تهدیدهای فزاینده‌ای که از جانب افراد عادی جامعه، بخش خصوصی و دولت علیه حریم خصوصی وجود دارد، ضرورت حمایت از حریم داده‌های خصوصی افراد به عنوان یکی از جلوه‌های اصلی حریم خصوصی در عصر حاضر که از ارکان اساسی حقوق بشر محسوب می‌شود بیش از پیش احساس می‌شود (جلالی فراهانی، ۱۳۸۳، ص ۸۸). علم حقوق به عنوان تنظیم کننده روابط انسان‌ها در تمام سطوح ناچار است که تحولات جامعه را درک کند و برای ایفای نقش موثر خود ملزم به همگامی با این تغییرات است. لازمه داشتن جامعه‌ای متعادل، ایجاد توازنی مستمر میان حقوق افراد و حقوق جامعه می‌باشد که دو کفه این ترازو در چند سال اخیر همواره تحت تأثیر فناوری‌های نوین بوده است. ملاحظه توأمان تحولات علمی چند سال گذشته و تحولات علم حقوق گویای این امر است که علم حقوق همواره چندین گام عقب‌تر بوده است و تا به امروز یارای همگامی را نداشته است (حسنی، ۱۳۸۵، ص ۸).

در نظام حقوقی ایران با آنکه قوانین و مقررات کنونی تا حدی از برخی مصادیق مهم حریم خصوصی حمایت کرده اند اما این حمایت‌ها کافی و کارآمد نیستند. از جنبه‌های مختلف حریم خصوصی، علی الخصوص حریم اطلاعات شخصی، حریم ارتباطات اینترنتی و حریم خصوصی افراد در قبال افشاگری‌های رسانه‌ای یا هیچ حمایتی صورت نگرفته است یا اگر حمایتی وجود دارد با توجه به در دسترس بودن انواع فناوری‌های قابل استفاده برای نقض حریم خصوصی، کافی و کارآمد نیست. از آنجا که قوانین سنتی به ویژه پایبندی به عناصر تشکیل دهنده

جرم در قوانین کیفری مانع تسری این گونه قوانین در موضوعات و مسائل موجود در جامعه اطلاعاتی می‌باشد، لذا تصویب قوانین خاص در این حیطه ضروری می‌باشد. در برخی کشورها قوانین خاص برای این موضوع تصویب گردیده است. در ایران قانون جامع و یا قوانین متعدد با موضوعات متنوع وجود ندارد و لذا باید مطالب مرتبط با آن را از برخی مواد قانون مجازات و قوانین متفرقه دیگر جستجو کرد. این قوانین پراکنده نیز بدون ابتناء بر مبانی و اصول متناسب با تحولات ناشی از ظهور فناوری‌های نوین نمی تواند راهگشای کامل مشکلات باشد و اگر تدبیر قانونی جامع و مناسب در این زمینه ظهور نکند دیری نخواهد پایید که حریم خصوصی افراد تبدیل به صحنه سوء استفاده عمومی شده و روی سیاه فناوری اطلاعات، هویدا شده و باعث انتقاد همگانی به پیشرفت‌های بشری از یکسو و بی اعتمادی عمومی به دولت و قانونگذار در حفظ حریم خصوصی افراد از سوی دیگر خواهد شد.[1]

مقاله حاضر در صدد پاسخگویی به این پرسش است که در سیاست کیفری تقنینی ایران، چه راهکارهایی برای مقابله با نقض حریم خصوصی افراد در نتیجه توسعه فناوری‌های اطلاعاتی و ارتباطاتی پیش بینی شده است؟ در پاسخ به این سوال، قوانین و مقررات جاری را در دو گروه بررسی خواهیم کرد. ابتدا به بررسی اصول کلی قانون اساسی در رابطه با حریم خصوصی خواهیم پرداخت، سپس به تفکیک موضوع، قوانین و مقررات عادی مرتبط با نقض حریم خصوصی توسط فناوری‌های نوین اطلاعاتی و ارتباطاتی را بررسی خواهیم کرد. بررسی سیاست کیفری تقنینی فعلی ایران در بحث حاضر از دو جنبه حائز اهمیت است. اول برای تبیین زمینه‌ها و پتانسیل‌های موجود در حقوق کشور برای ورود به مسئله حمایت از حریم خصوصی افراد به صورت جامع و دوم برای مشخص کردن حدود حمایت فعلی از این امر و ارزیابی کفایت و یا عدم کفایت آن و بررسی نقاط ضعف قوانین جاری. ارائه چنین تحلیل هایی می‌تواند پیشنهادهایی برای فعالیت‌های آتی قانونگذار ارائه نماید.

۱- البته شایان ذکر است که در کشور ما قوانین مختلفی به صورت لایحه و طرح در مراجع قانونی مطرح رسیدگی است از جمله لایحه حمایت از حریم خصوصی که هم اکنون جهت تصویب در دستور کار مجلس قرار دارد.

۱) ارزیابی قانون اساسی در رابطه با نقض حریم خصوصی توسط فناوری‌های نوین

بررسی اصول قانون اساسی ایران نشانگر این است که عبارت «حریم خصوصی» در هیچ یک از اصول قانون اساسی به صراحت ذکر نشده است. اما به طور کلی حق بر حریم خصوصی در این قانون به رسمیت شناخته شده است. یکی از اصولی که نقض حریم خصوصی افراد با استفاده از فناوری های اطلاعاتی و ارتباطاتی را جرم انگاری کرده است اصل ۲۵ می باشد[۱]. در این اصل ضبط و فاش نمودن مکالمه‌های تلفنی و استراق سمع و هرگونه تجسس ممنوع اعلام شده است که با جامعیت کم نظیری تمامی شنودهای مجاز و غیرمجاز توسط دستگاه‌های دولتی و افراد و دستگاه‌های غیر دولتی یا عمومی را شامل می‌شود. ازاین‌رو همواره با پیشرفت فن‌آوری‌ها هماهنگ بوده و جامعیت خود را از دست نمی‌دهد. اصل مذکور به عنوان شالوده و اساس قانون‌گذاری‌های عادی همواره باید مورد توجه قرار گیرد. متأسفانه تا قبل از تصویب قانون جرایم رایانه‌ای بسیاری از شنودهای غیرمجاز تلفنی و نظایر آن از ناحیه‌افراد غیر دولتی جرم به حساب نمی‌آمد؛ در حالی که بر ممنوعیت آنها در این اصل تصریح شده بود.

همانطور که گفته شد، در حقوق ایران تعریف مشخصی از اصطلاح حریم خصوصی وجود ندارد. با این حال در ماده ۲ لایحه حمایت از حریم خصوصی که متعاقبا به صورت طرح به مجلس شورای اسلامی ارائه گردیده است این اصطلاح به این نحو تعریف شده است: «حریم خصوصی قلمرویی از زندگی هر شخص است که آن شخص عرفا یا با اعلان قبلی در چارچوب قانون، انتظار دارد تا دیگران بدون رضایت وی به آن وارد نشوند یا بر آن نگاه یا نظارت نکنند و یا به اطلاعات راجع به آن دسترسی نداشته یا در آن قلمرو وی را مورد تعرض قرار ندهند. جسم، البسه و اشیاء همراه افراد، اماکن خصوصی و منازل، محل‌های کار، اطلاعات شخصی و ارتباطات خصوصی با دیگران «حریم خصوصی» محسوب می‌شوند.»

۱- اصل ۲۵: «بازرسی و نرساندن نامه ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آن ها، استراق سمع و هرگونه تجسس ممنوع است مگر به حکم قانون».

۲) ارزیابی سیاست کیفری ایران در خصوص شنود و استراق سمع

در خصوص شنود تلفن و محتوای سیستم‌های مخابراتی به طور کلی، در سیستم حقوقی ایران در قوانین مجازات اسلامی، آیین دادرسی کیفری، قانون تأسیس شرکت مخابرات ایران و قانون جرائم رایانه‌ای، مقرراتی پیش بینی شده است. قاعده کلی این موضوع در تبصره ماده ۱۰۴ قانون آیین دادرسی کیفری بیان شده است: «کنترل تلفن افراد جز در مواردی که به امنیت کشور مربوط است یا برای احقاق حقوق اشخاص به نظر قاضی ضروری تشخیص داده شود، ممنوع است. چنانچه ملاحظه، تفتیش و بازرسی مراسلات مخابراتی 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، مراتب را در صورت مجلس قید نموده، پس از امضاء متهم آن را در پرونده ضبط می‌نماید. استنکاف متهم از امضاء در صورت مجلس قید می‌شود و چنانچه اشیاء مزبور حائز اهمیت نبوده، ضبط آن‌ها ضرورت نداشته باشد با اخذ رسید به صاحبش مسترد می‌شود.» لازم به ذکر است که امر تفتیش نمی تواند منحصر در وسایل خاصی باشد و به نظر می‌رسد در لایحه اصلاحی قانون مربوطه که در دست انجام است، لحاظ وسایل نوین فناوری اطلاعات و ارتباطات در این ماده، قابلیت کارآیی مواد را افزایش می‌دهد.

همچنین در این تبصره به کنترل تلفن «افراد» اشاره شده نه «فقط متهمان» یا «افراد مرتبط با پرونده» که این امر می‌تواند در بر دارنده کنترل مکالمات افراد خارج از موضوع پرونده نیز باشد. از دیگر ایرادات وارد به این تبصره این است که قانونگذار به مقتضای اطلاق این تبصره، هرگونه احقاق حقی را مجوز استراق سمع تلفنی دانسته است. عنوان «احقاق حق» آنقدر عام است که هرگونه دعوای کیفری و یا حتی دعوای مدنی را هم در بر می‌گیرد؛ مگر اینکه گفته شود، با توجه به ذکر این تبصره در قانون آیین دادرسی کیفری، مقصود قانونگذار تنها دعاوی کیفری است. با آنکه نقض حریم خصوصی تنها در موارد کاملا ضروری، آن هم در قالب فرآیندهایی شفاف و نظارت پذیر امکان دارد، قانونگذار دست مقامات اجرایی را کاملا باز گذاشته و هیچ گونه فرایند عملی برای کنترل تلفن افراد پیش بینی نکرده

است. ضمن اینکه حتی برای تعدی از حدودی که خود پیش بینی کرده نیز هیچ گونه ضمانت اجرایی در نظر نگرفته است. این در حالی است که ضبط و فاش کردن مکالمات تلفنی و استراق سمع از نظر قانون اساسی چندان مهم بوده است که قانونگذار اصلی را در فصل مربوط به حقوق ملت (اصل ۲۵) به آن اختصاص داده است. چنین رویکردی یک بار دیگر نشانگر این دیدگاه است که قانونگذار ما در تعارض حقوق و آزادی‌ها با دیگر ارزش‌ها یا منافع، به حقوق و آزادی‌ها چندان اهمیت نمی دهد.

همچنین در لایحه جدید قانون آیین دادرسی کیفری که در دست بررسی است، ماده‌ای مجزا به این مسئله اختصاص داده شده است. ماده ۲۸- ۱۲۴ این لایحه مقرر می‌دارد: «کنترل مکالمات تلفنی افراد ممنوع است، مگر در مواردی که به امنیت کشور مربوط باشد یا برای کشف و شناسایی جرائم موضوع بند «الف»، «ب» و «ج» ماده ۶-۱۳۱ این قانون (جرایم مستوجب مجازات سلب حیات، جرایم مستوجب مجازات قطع یا قصاص عضو، جرایم مستوجب مجازات حداکثر بیش از سه سال حبس و حبس ابد) لازم تشخیص داده شود. در این صورت با موافقت رئیس حوزه قضایی و با تعیین مدت و دفعات کنترل، اقدام می‌شود. کنترل مکالمات تلفنی اشخاص و مقامات موضوع مواد ۱۰-۱۳۱ و ۱۱-۱۳۱ و نیز متهمان جرائم موضوع بند «د» ماده ۶-۱۳۱ این قانون (جرائم سیاسی و مطبوعاتی)، منوط به تأیید رئیس کل دادگستری استان است.» در کنار قیودی که در این لایحه برای تحقق امر کنترل مکالمات تلفنی افراد به قیود ماده ۱۰۴ اضافه شده است، قید ممنوعیت کنترل تلفن افراد جز در مواردی که برای احقاق حقوق اشخاص به نظر قاضی ضروری تشخیص داده شود، حذف شده است.

ماده ۵۸۲ قانون مجازات اسلامی نیز ضمن جرم تلقی کردن استراق سمع غیر قانونی ضمانت اجرای کیفری آن را تعیین می‌کند: «هر یک از مستخدمین ومأمورین دولتی، مراسلات یا مخابرات یا مکالمات تلفنی اشخاص را در غیر موارد مجاز در قانون استراق سمع کند یا بدون اجازه صاحبان آن‌ها مطالب آن‌ها افشاء نماید به حبس از یک سال تا سه سال یا جزای نقدی از شش تا هجده میلیون ریال محکوم خواهد شد». نقد وارد بر این ماده این است که این ماده ناظر به ارتکاب این

جرم توسط مستخدمین و مأمورین دولتی است و در مورد ارتکاب این جرم توسط شخص ثالث ساکت است. نظریه ۷/۳۴۷۲ -۱۳۷۷/۸/۱۶ اداره حقوقی قوه قضاییه در این خصوص اعلام داشته: «ضبط کردن یا استراق سمع مذاکرات تلفنی توسط مستخدمین ومأمورین دولتی جرم و مشمول ماده ۵۸۲ قانون مجازات اسلامی است، لکن چنانچه شخص ثالثی که مرتکب اعمال مذکور شده از مأمورین یا مستخدمین دولت نباشد قابل تعقیب کیفری نیست مگر این که ارتکاب این اعمال مستلزم مزاحمت تلفنی یا استفاده غیر مجاز از تلفن باشد که در این صورت به جهات اخیر قابل تعقیب کیفری خواهد بود».

به عبارت دیگر تخلف مأمورین و مستخدمین دولتی از موارد مصرح در قانون جرم تلقی شده و برای آن مجازات در نظر گرفته شده است. اگر اصل را بر مصونیت مکاتبات و مرسولات از تعرض قرار دهیم، پس استثنائات وارد بر آن باید دقیقاً مشخص شده و تخلف از آن مجازات در بر داشته باشد.

مبحث دوم قانون جرائم رایانه‌ای (مصوب ۱۳۸۸) نیز تحت عنوان «شنود غیر مجاز» به این موضوع اختصاص دارد و مقرر می‌دارد: «هر کس به طور غیر مجاز محتوای در حال انتقال ارتباطات غیر عمومی در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری را شنود کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد». به نظر می‌رسد به کارگیری اصطلاح «هر کس» در ماده فوق با هدف برطرف نمودن خلاء موجود در ماده ۵۸۲ قانون مجازات اسلامی است که تنها ناظر به ارتکاب این جرم توسط مأمورین و مستخدمین دولتی بوده و در مورد اشخاص ثالث ساکت است. بدین ترتیب شنود غیر مجاز ارتباطات غیر عمومی در سیستم‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری، صرف نظر از موقعیت و شغل مرتکب آن، جرم محسوب شده و مجازات به دنبال خواهد داشت. اما نکته مهم در اینجاست که این ماده در حوزه سیستم‌های رایانه‌ای و سایر موارد مصرح در آن به جرم‌انگاری پرداخته و امکان نقض حریم خصوصی خارج از این حیطه برای افراد عادی همچنان وجود دارد.

ماده ۴۸ این قانون نیز در تبصره خود اشعار می‌دارد: «دسترسی به محتوای

ارتباطات غیرعمومی ذخیره شده، نظیر پست الکترونیکی یا پیامک، در حکم شنود و مستلزم رعایت مقررات مربوط است.» مهم ترین مساله درباره ی این مقررات، لزوم وجود دستور کتبی مقام ذیصلاح قضایی برای هرگونه شنود است. بنابراین حتی در صورتی که از لحاظ تکنولوژیکی امکان دسترسی به محتوای پست‌های الکترونیکی میسر باشد، از لحاظ قانونی بدون حکم مقام مجاز قضایی نمی توان این محتواها را کنترل و مطالعه کرد.

در ماده۱۱ قانون استفاده از بی‌سیم‌های اختصاصی و غیر حرفه‌ای (آماتوری) که در تاریخ ۲۵ بهمن ۱۳۴۵ به تصویب رسیده نیز ۹ مورد به عنوان جرم احصا شده است. بند هفتم آن اختصاص به افرادی دارد که پیام رادیویی مربوط به اشخاص دیگر را دریافت نموده و آن را مورد استفاده قرار می‌دهند. قانون‌گذار برای مجازات این عمل پرداخت غرامت از دو تا بیست هزار ریال تعیین کرده که اگرچه در زمان تصویب قانون متناسب بوده؛ اما با افزایش تورم ظرف چند سال گذشته این مجازات جنبه بازدارندگی خود را از دست داده است. البته ابتکار جالبی که در این قانون به کار رفته، ماده۱۲ آن است. به موجب این ماده در صورتی که اعمال مذکور در این قانون مشمول مجازات‌های شدیدتری در سایر قوانین باشد، مجازات شدیدتر اجرا خواهد شد. بنابراین با تصویب قانون جرایم رایانه‌ای در سال ۱۳۸۸ و تصریح به سامانه‌های مخابراتی و امواج الکترومغناطیسی در آن و به استناد ماده ۱۲ قانون استفاده از بی‌سیم‌های اختصاصی، مجازات مذکور در ماده ۱۱ قابلیت اعمال نداشته و باید به قانونی که مجازات آن اشد است، عمل شود.

لایحه حمایت از حریم خصوصی نیز در این زمینه طی موادی اقدام به جرم انگاری نموده است. ماده ۶۰ این لایحه مقرر می‌دارد: «رهگیری ارتباطات از راه دور نظیر ارتباطات از طریق تلفن، تلگراف، تلکس، فکس، انواع بی‌سیم و سائر وسایل و یا پایش ارتباط کلامی – حضوری افراد ممنوع است مگر با رعایت قانون». بند ۹ ماده ۲ این لایحه «رهگیری» را دستیابی به محتوای ارتباطات کلامی – حضوری یا کتبی یا الکترونیکی یا سیمی با استفاده از هر نوع وسیله الکترونیکی، مکانیکی یا سایر وسایل مشابه بدون اطلاع طرف برقرار کننده ارتباط نظیر بازرسی، شنود و ضبط ارتباطات تعریف می کند.

در برخی موارد ضرورتی برای استماع مکالمات افراد وجود ندارد بلکه صرفاً اطلاع از برقراری تماس بین دو نفر و یا با شماره‌ای خاص مد نظر است. در چنین مواردی مجوز کنترل صادر خواهد شد نه رهگیری. در این صورت فقط شماره‌هایی که با فرد مورد نظر در تماس بوده‌اند و در صورت لزوم طول مدت مکالمه یا هویت صاحب شماره تلفن بررسی خواهد شد. در بسیاری موارد حتی در متون قانونی کلمه کنترل با هدف انجام شنود بدون توجه به تفاوت شرایط و ضوابط و عملیات کنترل و شنود به کار می‌رود که این عدم دقت، منجر به نقض حریم خصوصی ارتباطی خواهد شد. به عنوان مثال هدف قانونگذار از کلمه «کنترل» در تبصره ماده ۱۰۴ قانون آیین دادرسی کیفری، «شنود» بوده است.

ماده ۶۱ لایحه مقرر می‌دارد: «در صورتی که مقام قضایی موضوع ماده ۵۷ بنا به در خواست وزارت اطلاعات و سایر مراجع ذیصلاح در محدوده وظایف قانونی خود و در مورد جرائم مذکور در ماده ۵۷ بر مبنای ظن قوی تشخیص دهند که رهگیری ارتباطات از راه دور یا ارتباطات کلامی – حضوری به جلوگیری از وقوع جرائم مذکور، کشف ادله جرائم در حال وقوع یا واقع شده کمک مؤثر خواهد کرد، اختیار دارد مجوز کتبی رهگیری با اوصاف زیر صادر کند:

۱.مشخصات شخص یا اشخاصی که باید ارتباط‌شان رهگیری شود.

۲.مشخصات دقیق شخص یا سازمانی که باید ارتباطات مورد نظر را رهگیری کند.

۳.مدت زمان مجوز رهگیری

۴.موضوعی که باید اطلاعات راجع به آن از طریق رهگیری تحصیل شود .

۵. استفاده کنندگان از اطلاعات تحصیل شده».

همان طور که مشاهده می‌شود، رهگیری ارتباطات مذکور در این ماده به عنوان استثنایی بر اصل آزادی ارتباطات و با شرایط مقرر در قانون پیش بینی شده است. به عنوان مثال، لزوم صدور مجوز کتبی از سوی مقام قضایی که سایر ضوابط باید در آن قید شود. نکته قابل ذکر در این جا رضایت یک طرف مکالمه با قصد همکاری برای شنود و کنترل است. در این صورت رهگیری نقض حریم خصوصی وی نخواهد بود اما برای سایرین باید مجوز صادر شود. دیگر این که فقط شنود

مکالمات تلفنی افراد مرتبط با پرونده مجاز است که تعیین آن نیز با مقام قضایی صالح است. همان طور که ذکر شد ماده ۱۰۴ قانون آیین دادرسی کیفری به کنترل تلفن «افراد» اشاره کرده نه «فقط متهمان» یا «افراد مرتبط با پرونده» که می‌تواند در بر دارنده مکالمات و افراد خارج از موضوع پرونده نیز باشد.

اساساً مجوز شنود مکالمات نباید امکان سوء استفاده برای مأمورین اجرا کننده دستور را ایجاد کند که کلیه مکالمات فرد موضوع قرار را در مورد هر موضوعی استماع نمایند. به عنوان مثال، استماع و ضبط مکالمات خانوادگی شخصی که اتهامش جاسوسی است مجاز نمی‌باشد. این موضوع لزوم ذکر اتهام در قرار را توجیه می‌کند. مدت اعتبار مجوز نیز به جهت حفظ حریم خصوصی متهم باید مشخص شود.

در مورد رهگیری مکالمات حضوری افراد، گاهی نیاز به نصب ابزار و آلات ضبط و یا شنود مکالمات در منزل یا مکان خصوصی افراد ضروری می‌شود، در این مورد جواز ورود به این اماکن با ذکر جدود واختیارات مأمورین برای نصب این وسایل نیز باید صادر شود. بنابراین صدور هر مجوز باید اقدامات را به موارد ضروری و موضوع خاص محدود سازد.

انواع دیگر برقراری ارتباط مانند بی‌سیم و مکالمات تلفنی از طریق اینترنت نیز تابع همین ضوابط خواهد بود[1]. در مورد تعارض میان حق حریم خصوصی و منافع عمومی، تعدی نسبت به حریم خصوصی در مواردی خاص و معدود و به نحوی بسیار ضابطه‌مند مجاز شمرده می‌شود. یکی از مصادیق آن تعیین مقام استفاده کننده از اطلاعات جمع‌آوری شده از طریق رهگیری و کنترل است. ماده ۶۴ لایحه حمایت از حریم خصوصی مقرر می‌دارد: «هر گونه افشای اطلاعات حاصل از رهگیری قانونی به اشخاص و مراجع غیر قانونی جرم تلقی شده و به مجازات مربوطه محکوم می‌شود». ماده ۶۳ لایحه نیز مقرر کرده است: «ارائه دهندگان خدمات پستی یا از راه دور و کارمندان، کارگران و متخصصان فنی آنان که در اجرای ماده فوق با مأموران دولت همکاری می‌کنند حق افشای وسایل به کار رفته

۱- مثال بارز این مورد جرم انگاری دریافت پیام رادیویی متعلق به دیگران در ماده ۱۱ قانون استفاده از بی‌سیم های خانگی مصوب ۴۵/۱۱/۲۵ است که عمل هر کس که پیام رادیویی مربوط به اشخاص دیگر را دریافت نموده و مورد استفاده قراردهد، جرم و مستوجب مجازات می‌داند.

برای رهگیری ارتباطات رهگیری شده و اطلاعات جمع‌آوری شده را ندارند.»

مفهوم این دو ماده همان اصل رازداری حرفه‌ای است و افشاء چنین اسراری طبق ماده ۶۴۸ مجازات اسلامی جرم و مستوجب کیفر است.

به طور کلی بر موادی که ذکر گشت چند نقص وارد است و این نواقص، جزء مهم ترین مواردی هستند که با وجودشان نمی توان با استفاده کنندگان دستگاه های استراق سمع و عاملان خرید و فروش برخورد کرد. از جمله اینکه در حقوق ایران استراق سمع افراد عادی هنوز جرم محسوب نمی شود و همچنین مشخص نیست که در چه نوع جرائمی می توان استراق سمع کرد و مدت زمان آن چه مدتی است یا کیفیت ثبت مذاکرات اشخاص، قطع مذاکرات تلفنی و قطع و افشای دیگر وسایل مخابراتی از جمله اینترنت، کامپیوتر و موبایل و... مشخص نیست. البته در قوانین متفرقه از جمله ماده ۱۶ قانون پست و مواد ۱۲ و تبصره ۳ ماده ۱۳ و ماده ۱۴ قانون نیروهای مسلح مصوب ۷۱/۵/۱۸ و قانون نیروهای انتظامی مصوب ۶۹/۴/۲۷ و ماده ۲۱۳ آیین نامه زندان‌ها و بند ۱۱ ماده ۸ قانون رسیدگی به تخلفات اداری و قوانین استفاده از بی سیم های اختصاصی و غیرحرفه ای و... اشاره هایی در خصوص این امر کرده اند ولیکن همه این قوانین مشمول نیروهای دولتی می شوند و سخنی از افراد عادی به میان نیاورده اند و این در حالی است که در این خصوص در اکثر قوانین جزایی کشورهای جهان برای حمایت از افراد عادی قوانینی همچون حبس یا جزای نقدی پیش بینی شده است. ولیکن در قوانین ما افراد عادی در جرم استراق سمع به حیطه فراموشی سپرده شده اند و هیچ ماده یا تبصره ای را به خود اختصاص نداده اند. در حالیکه جرم استراق سمع یک جرم عمومی است و در رابطه با حقوق عمومی و نظم و امنیت جامعه و آسایش عمومی دارای چنان اثر عمیق نامطلوب و فزاینده ای است که ایجاب می کند دادستان و قضات دادگاه‌ها عمومی مرتکبان آن را بدون الزام به وجود شاکی خصوصی تعقیب و کیفر کنند. ولیکن متاسفانه شکایت شاکی خصوصی در این خصوص امری است الزامی که در صورت فقدان آن هیچ گونه برخوردی با متخلف عادی در جرم استراق سمع امکان پذیر نخواهد بود. حال با توجه به فقر و فقدان قانون در این خصوص چگونه می توان با افراد عادی که مرتکب چنین عملی می شوند، برخورد کرد؟ عده ای از صاحب نظران معتقدند از آنجا که تجهیزات استراق سمع جزء

وسایل رادیویی محسوب می شود، سازمان ارتباطات رادیویی و همچنین مخابرات می توانند از تبلیغ کنندگان، و فروشندگان و خریداران تجهیزات استراق سمع شکایت کنند و مانع تبلیغات و خرید و فروش آنها شوند. البته با توجه به اینکه استراق سمع تنها در موارد خاص و آن هم به دستور قاضی و اجرای آن از سوی ماموران نیروهای انتظامی امکان پذیر است، می توان نتیجه گرفت خرید و فروش و استفاده از دستگاه های استراق سمع به نوعی دخالت در وظیفه قانونی نیروهای انتظامی محسوب می شود و فردی که بدون سمت قانونی و دستور قاضی اقدام به تبلیغ و خرید و فروش دستگاه های استراق سمع کند به طور خودسرانه در وظیفه یک ارگان دولتی دخالت کرده و طبق موارد مشابه، آن ارگان می تواند از فرد مورد نظر شکایت و درخواست مجازات وی را کند و این امر را قانون جدید نیروی انتظامی نیز تقویت می کند چرا که طبق این قانون از ۸۷/۹/۱۰ با هرگونه تبلیغ و خرید و فروش دستگاه های استراق سمع از سوی نیروهای انتظامی برخورد شدید خواهد شد و بدین ترتیب برای پیگیری و مجازات تبلیغ کنندگان، فروشندگان و خریداران دستگاه های استراق سمع دیگر نیازی به شاکی خصوصی برای اقدام به رسیدگی و محاکمه آنها نخواهد بود و نیروهای انتظامی هر زمان که متوجه وقوع چنین عملی شوند، مستقیماً می توانند به موضوع رسیدگی و بدون هیچ گونه اتلاف وقتی فرد یا افراد متخلف را دستگیر و به مجازات عمل خود رسانند و شاید بتوان از این طریق عدم توجه قانونگذار یکی از مهم ترین مسائل حساس جامعه را جبران کرد. قانونگذار نباید فراموش کند در عصر ارتباطات تصمیم گیری بیش از گذشته از اهمیت برخوردار است و جامعه ای که با تحول و دگرگونی سریع امروز نتواند خود را هماهنگ کند دچار سردرگمی و عدم توانایی در حل مشکلات و معضلاتی که برایش پیش می آید خواهد شد که بخش اعظم آنها مربوط به اموری می شود که در گذشته وجود نداشته و حال نیازمند تدبیری نو هستند. لذا نیاز است که قوانین کشور بنا به مسائل و رویدادهای جدید جامعه بشری مورد بررسی و بازنگری مجدد قرار گیرند و موادی نو در خصوص مسائل و مشکلات جدید جامعه در قوانین ما لحاظ شود.

در سال ۱۹۸۶ در آمریکا قانونی تحت عنوان قانون حریم خصوصی ارتباطات

الکترونیکی[1] به تصویب مجلس رسید که حریم خصوصی در استفاده و شنود تلفنی بر اساس آن مورد بررسی قرار گرفت. در این قانون مفاد مکالمات تلفنی بر دو قسمت شناخته شده است که تحت عنوان تلفن‌های شرکتی و تلفن‌های خصوصی شمرده شده است. بر اساس این قانون اجازه شنود مکالمات به تمامی تلفن‌های شرکتی (تلفن هایی که موضوع آنها در رابطه با مسائل شرکت می‌باشد) داده شده است. چنانچه در حین شنود، فرد متوجه شود که در حال کنترل یک مکالمه خصوصی است، می‌بایست فورا شنود را قطع نموده و از ادامه کنترل جلو گیری کند. در جایی که کارفرما منافع شغلی مشروعی برای توجیه کنترل مکالمات تلفنی کارکنان دارد، استثنائا می‌تواند تلفن‌های رد و بدل شده در جریان کار توسط کارکنانش را از طریق توسعه یکی از خطوط تلفنش کنترل کند (Oncidi, Mckenna, Kathleen, ۲۰۰۶: ۲۰). در پرونده Arias v. Mutual Central Service Inc. دادگاه مقرر کرد علیرغم شخصی بودن برخی از آن مکالمات، کارفرمایان دلایل مشروع شغلی برای ضبط تمامی مکالمات ورودی و خروجی را داشته اند. زیرا شرکت به دلیل نکهداری اطلاعات محرمانه مشتری نیاز به نگهداری دقیق تلفن‌های ضروری داشت. در پرونده Briggs v. American Air Filter Inc. دادگاه مقرر نمود اقدام کارفرما نسبت به ضبط تلفن کارمند به منظور تشخیص انتقال اطلاعات محرمانه به رقیب شرکت، قانونی است.

مطابق بخش فرعی (d)، (c)۲۵۱۱ قانون حریم خصوصی ارتباطات الکترونیکی ۱۹۸۶، یک کارفرما می‌تواند مکالمات تلفنی یا دیگر ارتباطات شفاهی کارکنان را با رضایت آنان کنترل کند.

همچنین بر اساس ماده ۲۰۱ قانون جزای آلمان، ضبط بدون مجوز سخنانی که در برابر عموم بیان نشده است، استفاده بدون مجوز و یا قرار دادن آن در اختیار دیگری در صورتی که با هدف ایراد صدمه به حقوق ذینفع باشد مستوجب مجازات است. همچنین شنود این سخنان به وسیله میکروفن نیز ممنوع شده است و مجازات این جرم پرداخت جریمه یا حبس تا ۳ سال می‌باشد. همچنین ماده ۷ قانون ۱۹۸۲ اسپانیا، تهیه و استفاده از هر نوع وسیله شنود، فیلمبرداری، دید یا هر وسیله دیگر که

1- Electronic Communication Privacy ACT (ECPA) 1986.

امکـان آگـاهی یـافتن از حـریم خـصوصی اشـخاص و اشـکال مختلـف بیانـات یـا مکاتبات محرمانه آنـان را فـراهم مـی‌سـازد و همچنـین ضـبط یـا تکثیـر آ نهـا را از تعرضات غیر قانونی به حریم خصوصی افراد بر می‌شمارد.

۳) ازریابی سیاست کیفری ایران در خصوص مزاحمت تلفنی و سوء استفاده از تلفن

مزاحمت تلفنی یکی از روش‌های نقض حریم خصوصی دیگـران اسـت. مبنـای رسیدگی به مزاحمت‌های تلفنی تا قبل از سال ۱۳۷۵ قواعد عمومی، آیـین‌نامـه‌هـای امور خلافی و سایر قوانین عام بود. تحول مهم در این زمینـه بخـشنامه ۱۳۴۱ وزارت دادگستری در مورد مزاحمـت‌هـای تلفنـی بـود کـه موجـب آسـیب‌هـای روحـی و جسمی و حتی مرگ شنونده شده بود. جرم‌انگاری مزاحمت تلفنی به صورت یـک عنوان مستقل از سال ۱۳۷۵ در قوانین کیفـری ایـران شـکل گرفتـه اسـت (محـسنی، ۱۳۹۰: ۵۱۸). ماده ۶۴۱ قانون مجازات اسلامی مزاحمت از طریق تلفن یا هر دستگاه مخابراتی دیگر و حتی پیامک را جرم انگاشته و ضـمانت اجـرای کیفـری بـرای آن تعیین کرده است. ماده ۱۴ قانون تأسیس شرکت مخابرات ایران (مصوب ۱۳۵۰) نیز ناظر به سوء استفاده از تلفن در جهت نقض حریم خصوصی دیگران است که بـرای آن مجازات‌هایی از اخطار کتبی تا قطع اشتراک تلفن پیش بینی کرده است.

مـاده ۶۴۱ قـانون مجـازات اسـلامی مقـرر مـی‌دارد: «هرگـاه کـسی بـا تلفـن یـا دستگاه‌های مخابراتی دیگر برای اشخاص ایجاد مزاحمت نماید، عـلاوه بـر اجـرای مقررات خاص شرکت مخابرات، به حبس از یک تا شش ماه محکوم خواهد شد.»

تعقیب مزاحم مانند سایر جرایم از طریـق مراجعـه بـه دادسـرا و تـسلیم شـکوائیه است. بنابراین امکان درخواست مستقیم از شـرکت مخـابرات بـرای معرفـی مـزاحم وجود ندارد.

ماده ۱۴ قانون تأسیس شرکت مخابرات مقـرر مـی‌دارد: «اشـخاص حقیقـی و یـا حقوقی با توجه به مواد ۲ و ۳ این قانون بـدون موافقـت وزارت پـست و تلگـراف و تلفن حق ندارند در تأسیس و توسعه و بهره‌برداری شبکه‌هـای مخـابرات اختـصاصی اقدام نمایند و در صورت تخلف، مقامات و مأموران انتظامی مکلفند بـه درخواسـت وزارت پست و تلگراف و تلفن و یا شرکت از احداث و توسـعه و بهـره‌بـرداری آن جلوگیری نمایند.

تبصره ۱: هر کس از وسایل مخابراتی عمومی یا اختصاصی که در اختیار دارد به طور غیر مجاز استفاده کند، در نوبت اول به او کتباً اخطار می‌شود و در نوبت دوم به مدت پانزده روز ارتباط او قطع یا از استفاده ممنوع خواهد شد. در صورت تکرار، اشتراک و یا اجازه استفاده او لغو می‌شود و یا تجدید تقاضای اشتراک با استفاده پس از انقضای شش ماه با رعایت امکانات فنی پذیرفته خواهد شد. موارد استفاده غیر مجاز در آئین نامه‌ای که از طرف شرکت تهیه و به تصویب وزیر پست و تلگراف و تلفن خواهد رسید تعیین می گردد.

تبصره ۲: هر کس وسیله مخابراتی در اختیار خود را، وسیله مزاحمت دیگری قراردهد یا با عمد و سوء نیت ارتباط دیگری را مختل کند، برای بار اول پس از کشف، ارتباط تلفنی او به مدت یک هفته همراه با اخطار کتبی قطع و تجدید ارتباط مستلزم پرداخت هزینه‌های مربوط خواهد بود. برای بار دوم پس از کشف، ارتباط تلفنی او به مدت سه ماه همراه با اخطار کتبی قطع و تجدید ارتباط مستلزم تقاضای مشترک و پرداخت هزینه‌های مربوطه خواهد بود و برای بار سوم، شرکت ارتباط تلفنی وی را بطور دائم قطع و اقدام به جمع‌آوری منصوبات تلفن نموده و ودیعه مربوط به مشترک را پس از تسویه حساب مسترد خواهد نمود.»

دادگاه‌ها در مقام عمل در برخورد با جرایم مزاحمت تلفنی، اغلب حکم به پرداخت جزای نقدی می‌دهند و چنانچه مبادرت به صدور حکم حبس کنند، نهایتا به مدت سه ماه یا سه ماه و یک روز می‌باشد که معمولا با توجه به ماده ۲۲ قانون مجازات اسلامی تبدیل به جزای نقدی می‌شود.

ماده ۶۴۱ از حیث ارزیابی زمینه‌های قانونی برای جرم انگاری، ماده قابل استفاده‌ای است. این ماده می‌تواند بستری برای جرم انگاری فعالیت‌های مزاحمت آمیز در فضای سایبر[1] و نیز Spamming باشد. متاسفانه در لایحه جدید قانون مجازات اسلامی نه تنها از مواد فوق سخنی به میان نیامده است، بلکه در آن هیچ ماده یا تدبیر نوینی در جهت حمایت از حق حریم خصوصی افراد که هر روزه توسط فناوری‌های نوین اطلاعاتی و ارتباطاتی در حال پایمال شدن است اندیشیده نشده است و این مسئله جای بسی تاسف و تامل دارد.

1- Cyber Harassment

۴)ارزیابی سیاست کیفری ایران در خصوص نظارت‌های ویدیویی و استفاده از دوربین‌های مداربسته

از جمله اطلاعات مربوط به شخص که تضمین‌های مناسبی را می‌طلبد، تصاویر و فیلم‌های مربوط به اشخاص است. در خصوص حمایت از حریم خصوصی افراد در برابر نظارت‌های ویدیویی با دوربین‌های مدار بسته که اغلب در محیط‌های کار توسط کارفرمایان برای کنترل بر محیط رخ می‌دهد، متاسفانه ماده خاصی در قوانین فعلی ما وجود ندارد. تنها مواد موجود در این خصوص، مواد ۲۳ تا ۲۷ لایحه حمایت از حریم خصوصی است که ناظر به حریم خصوصی در محل کار است. ماده ۲۳ مدیران و کارفرمایان را فقط در صورت وجود دلایل متعارف و ظن قوی مبنی بر ارتکاب فعالیت‌های مجرمانه در ارتباط با محیط کار از قبیل سرقت یا تخریب اموال محل کار یا سوء استفاده از آن‌ها و یا برای تامین امنیت و بهداشت محل کار یا کارکنان و مستخدمان مجاز به اعمال نظارت بر محیط کار می‌نماید. علاوه بر این مطابق تبصره ۱ ماده ۲۳، نظارت الکترونیکی اعم از ویدیوئی و انواع دیگر باید به عنوان آخرین راه کار یا در فقدان روشهای دیگر به کار گرفته شود. ماده ۲۵ راجع به نظارت ویدیوئی است و مقرر می‌دارد: «تجهیزات تصویر برداری که به قصد نظارت الکترونیکی به کار می‌رود، باید کاملا قابل روئیت باشد و همچنین در محلی که نظارت در آنجا صورت می گیرد علائمی به کار رفته باشد که به کارکنان، مستخدمان و ارباب رجوع توجه دهد که محل مذکور تحت نظارت الکترونیکی قرار دارد. شنود و ضبط اصوات تابع مقررات مربوط به فصل ششم این قانون خواهد بود.» ماده ۲۴ نیز ناظر بر نحوه اطلاع رسانی در مورد اعمال نظارت است: «در اجرای ماده فوق مدیر و کارفرما باید پیش از اقدام به نظارت، دلایل آن، زمان نظارت، اشخاص، پست ها، مکان‌های مورد نظر، روش‌ها و وسایل بکار رفته برای نظارت و اطلاعاتی که قرار است درباره آن نظارت شود را کتبا به اطلاع آنان برساند. افرادی که به این امر اعتراضی داشته باشند می‌توانند اعتراض خود را به مقامات موضوع ماده ۲۶ ارائه نمایند.» بنابراین همانگونه که مشاهده می‌شود، لایحه حمایت از حریم خصوصی تنها نظارت ویدیوئی آشکار و با اطلاع قبلی را به رسمیت شناخته و در مورد پایش بصری مخفیانه ساکت است.

برخی از ایالت‌های آمریکا از جمله ماساچوست، کانکتیکت و کالیفرنیا با تصویب قوانین ناظر بر پایش در محل کار، سعی در حمایت از این جنبه از حریم شخصی داشته اند. اما در میان آنها کانکتیکات، بیشترین میزان حمایت از حریم خصوصی در محل کار را به ویژه در رابطه با ممنوعیت استفاده از پایش‌های الکترونیکی برای نظارت بر فضاهای تعبیه شده به منظور استفاده شخصی کارکنان، مانند اتاق‌های استراحت، فراهم نموده است. کانکتیکات تنه ایالتی است که بر اساس قانون ایالتی شماره ۴۸۶ -۳۱ سال ۱۹۸۷، ضبط صدا و فیلم برداری را منوط به اطلاع قبلی کارمندان آن سازمان نموده است. بر ایای همین قانون نصب دوربین‌های مدار بسته در اماکن خصوصی شرکت‌ها نظیر رختکن، توالت و حمام، منع و پیگرد قانونی دارد[1].در سیستم حقوقی ایالت متحده آمریکا در خصوص نظارت ویدیوئی دو نکته قابل ذکر است:

۱- توجه واقناع قبلی: بدین معنی که در صورت اطلاع قبلی کارکنان نسبت به وجود نظارت ویدیوئی از طریق یاد داشت یا اطلاع رسانی مناسب، دلیلی برای ادعای حریم خصوصی توسط کارکنان وجود ندارد و شرایط اعلام رضایت قبلی بر این وضعیت حاکم است.

۲- نظارت در فضاهای باز و مسطح و یا با دوربین‌های در دید آشکار: حتی در موارد عدم اطلاع رسانی و اخذ رضایت قبلی، کارکنان در فضاهای باز و عمومی دارای انتظار معقولی از حریم خصوصی نمی باشد (Oncidi, Mckenna, Kathleen, ۲۰۰۶: ۲۲). در پرونده L.R.Wilson v. OSHRC، فعالیت‌های کارگاه ساختمانی توسط یک بازرس از پشت بام هتل کنار آن به صورت ویدیوئی ضبط شد. دادگاه مقرر کرد که انتظار معقولی از حریم خصوصی برای کارفرما در کارگاهش وجود ندارد. زیرا هر کس در آن قسمت از هتل قادر به دیدن فعالیت‌های کارگاه ساختمانی بوده است (http://www.findlaw.com).

یکی از مباحث مهم در مورد نظارت ویدیوئی، «نظارت بدون دلیل» است. کارفرما باید از نصب دوربین در فضاهایی که منجر به نقض حریم خصوصی افراد

1- Gomez, Cynthia, Video Surveillance Laws in the Workplace, 2010, in: http://www.ehow.com.

می‌شود یا ضرورتی برای آن وجود نـدارد، اجتنـاب کنـد. در دعـوای Hawaii v. Bonnell، کارفرما اقـدام بـه نظـارت ویـدیوئی کارکنـان پـست در اتـاق اسـتراحت می‌نمـود. دادگـاه ایـالتی مقـرر نمـود کـه کارکنـان دارای انتظـار معقـولی از حـریم خصوصی در اتاق استراحتی که اقداماتی برای تامین حد معینی از حـریم خـصوصی در آن صورت گرفته، می‌باشند.

یکی دیگر از مـوارد اسـتفاده از نظـارت ویـدیوئی، کـه منجـر بـه اقامـه دعـاوی بسیاری در دادگاه‌های آمریکا گشته، کنترل خطاهای کارکنان است. یـک کارفرمـا در صورت تحقـق دو شـرط مـی‌توانـد از نظـارت ویـدیوئی بـرای «کـشف» خطـای ارتکابی یک کارمند استفاده کند:

۱) منفعت ادعـایی کارفرمـا بـرای ارجحیـت نـسبت بـه منـافع حـریم خـصوصی کارکنان به حد مهم کافی باشد.

۲) کارفرما تضمین کند که نقـض حـریم خـصوصی کارمنـد بـه ضـعیف تـرین شکل ممکن صورت می‌گیرد (محسنی، ۱۳۸۹: ۴۰۵).

همچنین به موجب ماده ۸-۲۲۶ قانون جزای فرانسه، اقدام به تهیه فیلم یـا تـصویر شخص یا انتشار آن بدون رضایت وی به هر شیوه‌ای که باشد، مستوجب یـک سـال حبس و پانزده هزار یورو جزای نقدی است. ماده ۳-۹۰۳ قانون جزایی ایالت مریلند نیز استفاده از دوربین و دیگر وسایل الکترونیکی برای تصویر برداری از فـرد بـدون رضایت وی را جرم دانسته است.

۵) ارزیابی سیاست کیفری ایران در خصوص انتشار تصاویر و فیلم‌های خصوصی افراد

یکی از مصادیق مهم حریم خصوصی، حق فرد نسبت بـه تـصویر خـود اسـت و عکس و تصویر هر فرد جزء شخـصیت اوسـت. چـاپ و انتـشار تـصویر فـرد بـدون رضایت و اجازه او نقض حریم خصوصی محسوب شده و ممنـوع اسـت. از ایـن رو هر فرد می‌تواند از انتشار عکس و تـصویر خـود حتـی اگـر بـدون سـوء نیـت باشـد جلوگیری نماید. اهمیـت و حـساسیت ایـن موضـوع بـه حـدی اسـت کـه برخـی از کشورها با هدف قاعده‌مند نمودن این قسم از فعالیت رسانه‌ای و ایجـاد تعـادل میـان حریم خصوصی افراد و حق آزادی بیان رسانه‌ها، اقـدام بـه تـدوین قـوانین و تنظـیم

آیین‌نامه‌های تخصصی تحت عنوان «حقوق عکسبرداری»[1] نموده‌اند. البته ممنوعیت چاپ و انتشار عکس و تصویر افراد مطلق نیست بلکه در مواردی که نفع عمومی اقتضا کند می‌توان علی‌رغم ناراضی بودن صاحب عکس آن را منتشر نمود. شرایط انتشار تصویر افراد بر خلاف رضایت‌شان، در هر مورد با توجه به معیارهایی مانند ماهیت فعالیت انجام شده، شهرت مثبت یا منفی سوژه، نفع عمومی، تأثیر آن بر جامعه، عرف، انتظار معقول از حریم خصوصی و ... متفاوت است. ماده ۱۶ و ۱۷ قانون جرایم رایانه‌ای به این مسئله اشاره دارد.

ماده ۱۶ در این خصوص مقرر می‌دارد: «هرکس به وسیله سیستم‌های رایانه‌ای یا مخابراتی، فیلم یا صوت یا تصویر دیگری را تغییر دهد یا تحریف کند و آن را منتشر یا با علم به تغییر یا تحریف منتشر کند، به نحوی که عرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

تبصره: چنانچه تغییر یا تحریف به صورت مستهجن باشد، مرتکب به حداکثر هر دو مجازات مقرر محکوم خواهد شد.»

این جرم که در حقیقت معادل توهین در دنیای واقعی است با نقض عامدانه اصل کیفیت داده‌های شخصی در مرحله پردازش و اصل پردازش صادقانه با تغییر داده‌های درست یا تولید داده‌های نادرست صورت می‌گیرد. بنابراین این تصاویر یا فیلم‌ها یا صداها ممکن است واقعی باشند و از روی نسخه واقعی به این شکل درآمده باشند یا غیر واقعی بوده ولی کاملا شبیه به تصویر فیلم و صدای یک یا چند شخص معین باشند و اگر صدا یا تصویر یا فیلم با یکدیگر جمع شوند، تغییر یا تحریف یکی از آن‌ها برای تحقق موضوع مجرمانه با تحقق سایر شرایط کافی است (عالی پور، ۱۳۸۴: ۲۵۲). البته این جرم یک جرم مقید به نتیجه است و این عمل حتما باید به صورت عرفی موجب هتک حیثیت شخص بشود تا قابل مجازات باشد. هرچند عموما ناظران این صحنه‌ها این محتویات را به صاحبان اصلی آن‌ها منتسب نمی دانند اما این گونه محتویات موجب اهانت به اشخاص و تزلزل حرمت شخص می‌شود. فضای سایبر در این زمینه به اندازه‌ای مساعد است که اکنون هر تصویری

1- Photography Law

را که در ذهن انسان می‌گنجد می‌توان در آن یافت (همان: ۲۵۳). اشکالی که می‌توان به این ماده وارد کرد محدود بودن دامنه این جرم است که صرفا فیلم یا صوت یا تصویر دیگری را تحت حمایت قرار می‌دهد و سایر داده‌های افراد مانند اسناد شخصی را شامل نمی شود. به نظر می‌رسد این جرم انگاری به دلیل اقتضائات فعلی جامعه و برخی وقایعی باشد که اخیرا اتفاق افتاده است نه با یک رویکرد جامع برای حفظ حریم خصوصی شهروندان، زیرا این ماده شمول کافی را ندارد. با اینحال می‌توان آن را یک قدم مثبت ارزیابی کرد زیرا عمده تجاوزات به حقوق فردی شهروندان در فضای سایبر در کشور ما به صورت تحریف نگاری شخصیت انجام می‌شود.

ماده ۱۷ قانون جرائم رایانه‌ای (مصوب ۱۳۸۸) نیز در این خصوص مقرر می‌دارد: «هر کس به وسیله سامانه‌های رایانه‌ای یا مخابراتی، صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او منتشر کند یا در دسترس دیگران قرار دهد، به نحوی که منجر به ضرر یا عرفا موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.»

در پیش نویس‌های لایحه این قانون، دامنه مصادیق اسرار شخصی گسترده تر بود که در متن قانون از شمول حمایت خارج شده اند و فقط صوت، تصویر و فیلم مشمول مواد فوق قرار گرفته اند. گزارش توجیهی این لایحه علت این امر را به صورت زیر بیان داشته است:

«در ماده ۱۷ اسرار دیگری در متن‌های نخستین پیش نویس وجود داشته که در متن نهایی حذف شده است، زیرا افشای سر به صورت عام در مقررات کیفری پیش بینی شده و ذکر مجدد آن در این ماده نه تنها ضروری نبود بلکه ماهیت سر نیز مشخص نبود و اینکه آیا همگان باید حافظ اسرار یکدیگر باشند؟ حال آنکه در حالت عادی فقط سر نسبت به اشخاصی مصداق دارد که افراد با توجه به وظایف و شغلشان، اسرارشان را نزد آن‌ها بازگو می کنند مثل پزشک یا وکیل وگرنه اگر قرار باشد حفظ سر نسبت به کلیه افراد سرایت داشته باشد، مفهوم آن کلا مبهم و مغشوش می گردد.»

به نظر می‌رسد که این توجیه قابل پذیرش نیست و به راحتی می‌توان حداقل، داده‌های شخصی حساس را احصا و تعریف کرد و حدود مبهم لفظ «سر» را با این تعاریف روشن ساخت. موضوع این جرم در هر حال باید واقعی باشد یعنی نسبت به آن شبیه سازی یا دخل و تصرف یا تغییر صورت نگرفته باشد. در غیر اینصورت حسب مورد جعل، تخریب یا تحریف نگاری یا هرزه نگاری هویت خواهد بود. منظور از در دسترس دیگران قرار دادن، ارائه محتویات ذکر شده به هر شکل دیگری است اعم از خرید و فروش، به امانت سپردن، بخشیدن و غیره. از نص این ماده نیز بر می‌آید که شخص منتشر کننده بایستی رضایت شخص را قبل از انتشار صوت یا تصویر یا فیلم خصوصی یا خانوادگی وی به دست آورد و این رضایت بایستی در زمان انتشار یا افشاء حاصل شده باشد و این تکلیف بر عهده منتشر کننده اطلاعات فوق است و نباید تصور شود که صاحب اسرار باید عدم رضایت خود را در انتشار یا در دسترس قرار دادن اسرار خصوصی به منتشر کننده اعلام نماید. این جرم نیز جرمی مقید است و باید ایراد ضرر یا هتک حیثیت عرفی در آن صورت گیرد.

همچنین بر اساس ماده ۴ قانون نحوه مجازات کسانی که در امور سمعی و بصری فعالیت غیر مجاز دارند (مصوب ۸۶/۱۰/۱۹): «هر کس با سوء استفاده از آثار مبتذل و مستهجن تهیه شده از دیگری، وی را تهدید به افشاء و انتشار آثار مزبور نماید و از این طریق با وی زنا نماید به مجازات زنای به عنف محکوم می‌شود ولی اگر عمل ارتکابی غیر از زنا و مشمول حد باشد، حد مزبور بر وی جاری می‌گردد و در صورتی که مشمول تعزیر باشد به حداکثر مجازات تعزیری محکوم خواهد شد.»

ماده ۵ قانون فوق مقرر می‌دارد:

«مرتکبان جرائم زیر به دو تا پنج سال حبس و ده سال محرومیت از حقوق اجتماعی و هفتاد و چهار ضربه شلاق محکوم می‌شوند:

الف) وسیله تهدید قرار دادن آثار مستهجن به منظور سوء استفاده جنسی ، اخاذی ، جلوگیری از احقاق حق یا هر منظور نامشروع و غیر قانونی دیگر.

ب) تهیه فیلم یا عکس از محل‌هایی که اختصاصی بانوان بوده و آنها فاقد

پوشش مناسب می‌باشند مانند حمام‌ها و استخرها و یا تکثیر و توزیع آن.

ج) تهیه مخفیانه فیلم و عکس مبتذل از مراسم خانوادگی و اختصاصی دیگران و تکثیر و توزیع آن.»

بر اساس ماده ۶ همین قانون:

«رابطه زوجیت مانع از اعمال مجازات مرتکب جرم تکثیر، انتشار و یا توزیع آثار مستهجن نمی‌باشد.»

در ایالات متحده آمریکا، به منظور حفاظت از تصاویر و فیلم‌های ویدیویی اشخاص، علاوه بر نظارت بر رسانه ها، قانون حفاظت از فیلم‌های ویدیویی اشخاص (۱۹۸۸)[1]، ناظر بر عرضه فیلم‌های ویدیویی اجاره‌ای و قابل فروش است. به موجب این قانون، ارائه دهندگان خدمات فیلم‌های ویدیویی که خدمات خارج از روند معمول حرفه‌ای خود و در جهت انتشار فیلم‌های ویدیویی خصوصی افراد ارائه دهند، به حداکثر ۲۵۰۰ دلار جریمه محکوم خواهند شد (عنوان ۱۸ از مجموعه قوانین ایالات متحده).

۶) ارزیابی سیاست کیفری ایران در خصوص استفاده از فناوری دروغ سنجی

به لحاظ ارزیابی اقدامات صورت گرفته در نظام قضایی ایران در حمایت از حق حریم خصوصی افراد در برابر استفاده از ابزارهایی همچون دروغ سنج باید خاطر نشان کرد که متاسفانه در قوانین ما استفاده از چنین تکنولوژی هایی صراحتا مورد جرم انگاری قرار نگرفته است. لذا، ناگزیر باید با توسل به مواد و قوانین پراکنده و عام، به حمایت از حقوق افراد در مواجهات احتمالی با این مسئله پرداخت. از جمله اصول و موادی که می‌توان در این زمینه به آن‌ها استناد نمود، اصل ۲۳ قانون اساسی و مواد ۶۹، ۵۷۸ و ۵۷۹ قانون مجازات اسلامی می‌باشد. همانگونه که در مباحث پیشین ذکر شد، یکی از مصادیق نقض حریم خصوصی در آزمون‌های دروغ سنجی، «تفتیش عقیده» است که به طور کلی، بر اساس مبانی حقوق بشر و نیز قوانین اساسی کشورهای مختلف ممنوع می‌باشد. زیرا عقیده یکی از جلوه‌های

1- Video Privacy Protection Act (1988), in: http://www. Privacy.gov.au/act

روشن حریم خصوصی است و لذا یکی از جنبه‌های حمایت از حریم خصوصی، مورد حمایت قرار دادن افکار و عقاید انسان هاست. بدین معنا که انسان‌ها اختیار دارند افکار و مکنونات خود را فقط با میل و اراده خود، به هر نحو و به کسانی که می‌خواهند اظهار کنند. اصل ۲۳ قانون اساسی، به نحوی بیانگر حمایت از داده‌های شخصی حساس است. عقاید مذهبی، فلسفی و سیاسی از مهمترین داده‌های شخصی حساس به شمار می‌روند و لزوم تفتیش عقاید، شکنجه و کسب مستقیم اطلاعات از خود شخص نیست. جستجوی غیر قانونی پایگاه‌های داده و جمع آوری و پردازش داده‌های مربوط به عقاید شخصی با استفاده از ابزارهایی همچون دستگاه دروغ سنج می‌تواند موثرترین و خطرناک ترین نوع تفتیش عقاید باشد. این اصل مقرر می‌دارد: «تفتیش عقاید ممنوع است و هیچ کس را نمی‌توان به صرف داشتن عقیده‌ای مورد تعرض و مؤاخذه قرار داد» (محسنی، ۱۳۸۹: ۲۹۲).

همچنین، یکی از اساسی ترین موضوعات حقوق کیفری، تحصیل دلیل است که طی آن نباید تمامیت جسمانی شهود و متهم مورد تعرض قرار بگیرد. در صورت نقض این اصل، دلیلی که با این روش کسب شده است ارزش قضایی ندارد و ضمانت اجرای کیفری و انتظامی نیز به دنبال دارد. در نظام قضایی کشور ما قانون گذار در فصل دهم قانون مجازات اسلامی در مواد ۵۷۸ و ۵۷۹ در قبال تعرض مامورین دولتی به تمامیت جسمانی متهم یا شهود واکنش کیفری از خود نشان داده است. لذا دلایل اثباتی حاصل از روش‌های غیر قانونی مانند: اقرار مبتنی بر شکنجه، سلب قوه اختیار یا توسل به هیپنوتیزم و استفاده از ابزارهایی همچون «دستگاه دروغ سنج» مطرود است. دکترین حقوقی با اعمال هر گونه اکراه، اجبار، فریب و خدعه نسبت به بزهکاران مخالف است. کسب اقرار، اطلاع، شهادت یا سوگندی که از راه اجبار شکنجه و تهدید تحصیل شود فاقد اعتبار قانونی بوده و محکومیت مستند به چنین اقراری در معرض بطلان است و دادگاه‌ها ملزم اند که به آن ترتیب اثر ندهند (گلدوزیان، ۱۳۶۵: ۱۴۵).

پاره‌ای از دلایل، صرفنظر از نوع و ساختار کسب آن، غیر قانونی و نامعتبر می‌باشند. برخی از دلایل با وجود شرایطی وجهه قانونی دارند، ولی به محض از بین رفتن آن شرایط، اعتبار و مشروعیت خود را از دست می‌دهند. استفاده از دروغ

سنج و هیبنوتیزم از دلایلی است که در نظام عدالت کیفری ایـران جایگـاه قـانونی و شرعی ندارند. اقرار از دلایلی است که بـا رعایـت شـرایطی مـی‌توانـد دارای اعتبـار باشد. در صورتی که اقرار با اراده موقر صورت گیـرد، دارای اثـرات قـانونی اسـت. ماده ۶۹ قانون مجازات اسلامی در این خصوص صـراحت دارد: «اقـرار در صـورتی نافذ است که اقرار کننده دارای اوصاف بلوغ، عقل و اختیار و قـصد باشـد». لـذا در مواردی که اقرار مبتنی بر عدم وجود اختیار و یا قصد باشد و در شرایط فشار کسب گردد از نظر قانونی مورد قبول نیست (انصاری، ۱۳۸۰: ۲۷۹).

مباحث فوق بیانگر این است که در حقوق ایران (بـا اسـتنباط از اصـول و قـوانین کلی و عام)، استفاده از ابزارهایی همچون دروغ سنج، به دلیل فقـدان اراده و اختیـار شخص مورد آزمایش، مورد پذیرش قرار نگرفته است. اما این عدم پذیرش بیشتر به دلیل قانونی نبـودن دلیـل اثبـاتی حاصـل از ایـن آزمایـشات یـا قـانونی نبـودن روش تحصیل دلیل می‌باشد و به مـسئله نقـض احتمـالی حـریم خـصوصی افـراد در نتیجـه انجام چنین آزمایشاتی و جرم انگاری آن توجهی ننموده اند. به نظر می‌رسد با توجه به اینکه گاها در کشور ما نیز علیرغم عـدم انعکـاس موضـوع در رسـانه‌هـا از چنـین ابزاری جهت کمک به روند کشف جـرم اسـتفاده مـی‌گـردد (صـرفنظر از تـاثیر یـا قابلیت اطمینان و اعتبار نتایج آن)، قانونگذار باید همانند سایر کـشورها، بـا ممنـوع، محدود یا مشروط کردن انجام چنین آزمایـشاتی، تـدابیری را در جهـت حمایـت از حریم خصوصی افراد در هنگام اجرای آزمایش پیش بینی کند. بـه عنـوان مثـال، تـا حد امکان از متصدیان متخصص و خبره برای انجام آزمـایش اسـتفاده گـردد یـا در هنگام انجام آزمایش، ناظری بی طرف در جلسه حضور داشته باشد تا سـوالاتی کـه از آزمودنی پرسیده می‌شود صرفا در راسـتای موضـوع آزمـایش باشـد نـه سـوالات متفرقه دیگر مانند عقاید مذهبی، فلسفی، سیاسی، جنسی، قومی- نژادی یا هر سوالی در حیطه حریم خصوصی فرد. لذا لازم است در جهت حمایت از حقوق شـهروندان در این موارد، اقدام به تدوین قوانینی جامع و مناسب گردد. زیرا اگـر تـدبیر قـانونی جامع و مناسب در این زمینه ظهور نکند، دیری نخواهد پایید کـه حـریم خـصوصی افراد تبدیل به صحنه سوء استفاده شده و باعث انتقاد همگانی به پیشرفت‌های بـشری از یکسو و بی اعتمادی عمومی بـه دولـت و قانونگـذار در حفـظ حـریم خـصوصی افراد از سوی دیگر خواهد شد.

۷) ارزیابی سیاست کیفری ایران در خصوص رهگیری ارتباطات الکترونیکی و حمایت از داده پیام‌های شخصی

یکی از بحث‌های عمده در تجارت الکترونیک بحث حمایت از داده‌های شخصی است. اطلاعات همواره در تجارت نقش بسیار مهمی دارد. بازاریابی، تعیین زمان و مکان خرید و فروش اجناس و تمام فعالیت‌های مرتبط با تجارت رابطه نزدیکی با اطلاعات دارد. بخشی از این اطلاعات، داده‌های شخصی طرف‌های تجاری و نیز مصرف کنندگان می‌باشد. برای انجام مبادلات تجاری بین المللی، کشورهای پیشرو اقتصادی، چنین داده هایی را به کشورهایی که فاقد سطح حمایت کافی هستند انتقال نمی دهند و این امر می‌تواند باعث تحریم اطلاعاتی و کاهش توان بازیابی و ارزیابی‌های دیگر تجار در کشورهای تحت تحریم اطلاعاتی شود. حمایت از داده‌های شخصی حتی در تجارت‌های داخلی نیز حائز اهمیت است. از این رو مقنن در ماده ۱ قانون جرایم رایانه‌ای و چند ماده از قانون تجارت الکترونیکی به بحث «حمایت از داده ها» پرداخته است.

ماده ۱ قانون جرایم رایانه‌ای در زمینه حمایت از داده‌ها مقرر می‌دارد: «هر کس به طور غیر مجاز به داده‌ها یا سامانه‌های 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 خواهد شد.»

این ماده با هدف حمایت همه جانبه از اقدام اشخاص در اتخاذ تدابیر امنیتی برای سیستم یا داده‌های خود، دسترسی غیر مجاز را به صورت ساده جرم انگاری کرده است. در این راستا از آنجایی که هکرها و کراکرها دارای امکانات هستند و جزای نقدی صرف قدرت پیشگیری ندارد مجازات حبس نیز پیش بینی شده است (گزارش توجیهی لایحه جرایم رایانه ای، ص ۵).

در مواد ۵۸، ۵۹، ۶۴، ۷۱، ۷۲، ۷۳، ۷۵ و ۷۸ قانون تجارت الکترونیکی نیز به بحث حمایت از داده‌ها پرداخته شده است.

در ماده ۵۸، قانونگذار ذخیره، پردازش و یا توزیع داده پیام شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی مذهبی، خصوصیات اخلاقی و داده

پیام‌های راجع به وضعیت جسمانی، روانی و یـا جنـسی اشـخاص را بـدون رضـایت صریح آن‌ها غیر قانونی می‌داند.

در ماده ۵۹، قانونگذار در صورت رضایت شخص موضوع داده پیام نیز به شرط آن که محتوای داده پیـام بـر وفـق قـوانین مـصوب مجلـس شـورای اسـلامی باشـد، ذخیره، پردازش و توزیع داده پیـام‌هـای شخـصی در بـستر مبـادلات الکترونیکـی را مشروط به شرایط ذیل نموده است:

الف: اهداف آن مشخص بوده و به طور واضح شرح داده شده باشند.

ب: داده پیام باید تنها به اندازه ضرورت و متناسب با اهدافی که در هنگام جمـع آوری برای شخص موضوع داده پیام شرح داده شده جمع آوری گردد و تنها بـرای اهداف تعیین شده مورد استفاده قرار گیرد.

ج: داده پیام باید صحیح و روزآمد باشد.

د: شخص موضوع داده پیام باید به پرونـده‌هـای رایانـه‌ای حـاوی داده پیـام‌هـای شخصی مربوط به خود دسترسی داشته و بتواند داده پیام‌های ناقص و یا نادرسـت را محو یا اصلاح کند.

ه: شخص موضوع داده پیام باید بتواند در هر زمـان بـا رعایـت ضـوابط مربوطـه درخواست محو کامل پرونده رایانه‌ای داده پیام شخصی مربوط به خود را بنماید.

ماده ۶۴: به منظور حمایت از رقابـت‌هـای مـشروع و عادلانـه در بـستر مبـادلات الکتریکی، تحصیل غیرقانونی اسرار تجاری و اقتـصادی بنگـاه‌هـا و موسـسات بـرای خود و یا افشای آن برای اشـخاص ثالـث در محـیط الکترونیکـی جـرم محـسوب و مرتکب به مجازات مقرر در این قانون خواهد رسید.

ماده ۷۱: هرکس در بـستر مبـادلات الکترونیکـی شـرایط مقـرر در مـواد (۵۸) و (۵۹) این قانون را نقض نماید مجرم محسوب و به یک تـا سـه سـال حـبس محکـوم می‌شود.

ماده ۷۲: هرگاه جرایم راجع به «داده پیام»هـای شخـصی توسـط دفـاتر خـدمات صدور گواهی الکترونیکی و سایر نهادهای مسئول ارتکاب یابد، مرتکب به حداکثر مجازات مقرر در ماده (۷۱) این قانون محکوم خواهد شد.

ماده ۷۳: اگر به واسطه بی مبالاتی و بی احتیاطی دفاتر خـدمات صـدور گـواهی

الکترونیکی جرایم راجع به «داده پیام»های شخصی روی دهد، مرتکب به سه ماه تا یک سال حبس و پرداخت جزای نقدی معادل ۵۰ میلیون ریال محکوم می‌شود.

ماده ۷۵: متخلفین از ماده (۶۴) این قانون و هرکس در بستر مبادلات الکترونیکی به منظور رقابت، منفعت و یا ورود خسارت به بنگاه‌های تجاری، صنعتی، اقتصادی و خدماتی با نقض حقوق قراردادهای استخدام مبنی بر عدم افشای اسرار شغلی ویا دستیابی غیر مجاز، اسرار تجاری آنان را برای خود تحصیل نموده و یا برای اشخاص ثالث افشا نماید به حبس از شش ماه تا دو سال و نیم و جزای نقدی معادل ۵۰ میلیون ریال محکوم خواهد شد.

ماده ۷۸: هرگاه در بستر مبادلات الکترونیک در اثر نقص یا ضعف سیستم موسسات خصوصی و دولتی، به جز در نتیجه قطع فیزیکی ارتباط الکترونیکی، خسارتی به اشخاص وارد شود موسسات مزبور مسئول جبران خسارت وارده می‌باشند مگر اینکه خسارات وارده ناشی از فعل شخصی افراد باشد که در این صورت جبران خسارات بر عهده این اشخاص خواهد بود.

مرور و ارزیابی این مواد، چند انتقاد مهم را بر آنها وارد می‌سازد:

برای «تجارت الکترونیک» که اصولا قانون به نام آن تصویب شده است در هیچ جا تعریفی ارائه نشده و مشخص نیست که آیا ظبق تعاریف متداول این قانون شامل زیر شاخه‌های تجارت الکترونیکی نظیر بانکداری الکترونیکی، پزشکی الکترونیکی و غیره نیز می‌شود یا برای هر یک از این شاخه‌ها باید قانون جداگانه‌ای مشابه همین قانون وضع و تصویب کرد (محسنی و قاسم زاده، ۱۳۸۲، ص ۴).

فصل سوم از این قانون به عنوان حمایت از «داده پیام»های شخصی اختصاص یافته است. در حالی که اساسا لفظ «حریم شخصی» که رکن اساسی در تجارت الکترونیکی است در این قانون مشخصا تعریف نشده و حمایت از حقوق اشخاص در خصوص اطلاعات شخصی شان مورد بحث و حمایت قرار نگرفته است.

این مواد دامنه شمول عام ندارند و بر اساس ماده ۷۱ مذکور، منحصر به بستر مبادلات الکترونیکی شده اند درحالی که اصول مدنظر مقنن به صورت عام نوشته شده اند. لیکن، تنها زمانی نقض این اصول منجر به مجازات می‌شود که در بستر مبادلات الکترونیکی صورت گرفته باشند. این امر در ماده ۵۹ قانون مذکور نیز تصریح شده است.

اصول جرم انگاری در موارد مذکور مراعات نشده است. از آنجایی که ماده ۷۱ در جرم انگاری مستقیما به مواد ۵۸ و ۵۹ ارجاع می‌دهد، دو ماده بایستی طوری نوشته شوند که تعریف و محدوده دقیق جرم مشخص باشد. درحالی که این امر اتفاق نیافتاده است. شرطی مانند «محتوی داده پیام موافق قوانین مصوب مجلس باشد» دارای ابهام است. تکلیف داده‌های معمولی معلوم نیست و در قبال داده‌های حساس نیز مقنن با بلاتکلیفی مواجه است در حالی که پردازش داده‌های حساس را در ماده ۵۸ مقید به رضایت موضوع داده‌ها کرده است، در ماده ۵۹، خود شروط دیگری را نیز اضافه کرده است که اگر این مقررات برای بستر مبادلات الکترونیک باشند، دخالت دولت با وجود رضایت طرفین فاقد وجاهت است. درباره داده‌های اشخاص حقیقی و حقوقی در حالی که در بخش تعاریف، مقنن، شخص را اعم از شخص حقیقی و حقوقی و حتی سیستم‌های رایانه‌ای تحت کنترل آنان می‌داند، داده‌های شخصی را صرفا ناظر به داده‌های شخص حقیقی می‌داند. ضمن اینکه این مواد هیچ استثنایی را در مورد پذیرش داده‌های حساس حتی موارد امنیتی، سلامت عمومی، تغییر جرائم کیفری یا حفظ حقوق مهم و حیاتی دیگری مقرر نکرده اند که اصلا معقول نیست. قابل گذشت بودن جرایم تصریح نشده است درحالی که بیشتر جرایم حمایت از داده بیش از آنکه جنبه عمومی داشته باشد ناظر بر روابط میان شهروندان است.

الزامات اساسی حمایت از داده اعم از اصول بکارگیری داده‌ها یا حقوق موضوع داده‌ها ناقص و حتی نادرست ذکر شده اند. حق بر درخواست امحاء کامل پرونده بدون شرط و در هر زمان در هیچ قانونی پیش بینی نشده است. ضمن اینکه حق دسترسی مستقیم به داده‌های شخصی و اصلاح یا محو آنها از سوی موضوع داده‌ها معقول نیست و معمولا حق دسترسی به اطلاعات راجع به داده‌های جمع آوری شده و درحال پردازش و حق بر اعتراض برای موضوع داده‌ها پیش بینی می‌شود و در مقابل آن تکلیف بر اطلاع رسانی و اصلاح موارد موجه اعتراض بر شخص کنترل گر تحمیل می‌شود (حسنی، ۱۳۸۵: ۱۱۲)[1].

۱- برای اطلاعات بیشتر درباره انتقادات وارد بر این قانون ر. ک: اصلانی، حمید رضا، حقوق فناوی اطلاعات، صص ۱۱۱، ۱۶۸، ۱۷۰، ۱۷۲، ۱۸۹، ۱۹۴، ۲۰۴، ۲۱۱، ۲۳۵، ۲۵۵، ۲۷۴، ۲۸۱.

یکی از کمبودهای مهم این قانون، سکوت در مورد لزوم رعایت تدابیر امنیتی توسط پردازشگر برای جلوگیری از نفوذ غیر مجاز و سایر اعمال ممنوع یا مجرمانه در بستر مبادلات الکترونیکی و بالاتر از آن عدم ذکر و تعیین اعمال ممنوع و مجرمانه در قانون است. همچنین بی توجهی به انتقال داده‌ها اعم از اینکه انتقال، داخلی یا خارجی و یا به بخش خصوصی یا دولتی باشد، یکی دیگر از کاستی‌های این قانون است. این سکوت را می‌توان به معنای فقدان چنین حمایتی از داده‌ها و عدم ممنوعیت انتقال آن‌ها و مسئول شناختن مرتکب تعبیر کرد. هرچند تصویب این قانون (علی رغم نواقص و کاستی‌های آن) نوید بخش آغاز قانونمند شدن فعالیت‌های اینترنت در تجارت الکترونیکی و جامعه ما بوده است، برای بهبود و پیشرفت و ارتقاء آن باید تلاش نمود و توجه داشت که بستر قانونی برای توسعه اینترنت و تجارت الکترونیکی به قوانین متعددی که با جامع نگری و توجه به سایر قوانین موجود در کشور تهیه شده باشند و نیز اصلاح قانون مصوب موجود نیاز دارد.

مقررات و ضوابط شبکه‌های اطلاع رسانی(مصوبات جلسات ۴۸۲ الی ۴۸۸ شورای عالی انقلاب فرهنگی) نیز که مشتمل بر ۳ آیین نامه است، طی موادی اقدام به جرم انگاری نقض حریم خصوصی افراد توسط ارائه کنندگان خدمات اینترنتی نموده است. از جمله، بند ج پاراگراف ۶ آیین نامه نحوه اخذ ضوابط فنی نقطه تماس بین المللی مقرر می‌دارد: « ج- دایر کننده نقطه تماس بین المللی موظف است بانک فعالیت‌های اینترنتی کاربران خود را قابل دسترسی وزارت ارتباطات و فناوری اطلاعات قرار دهد تا بر اساس ضوابط و مصوبات شورای عالی امنیت ملی با حکم قاضی ذیربط حسب درخواست در اختیار وزارت اطلاعات قرار گیرد». وضع ماده در چنین شکل عامی مغایر با حریم خصوصی شهروندان است. نوع داده هایی که باید ذخیره شود، موارد افشاء و شرایط افشاء بایستی دقیقا تشریح شود. ضمن آنکه مدت نگهداری نمی تواند نامحدود باشد و تاحد امکان باید صرفا داده‌های مربوط به مبداء و مقصد ارتباط ذخیره شود. بایستی و تنها در صورتی اطلاعات بیشتری از ارتباطات جمع آوری و افشاء شود که با وجود ادله قابل قبول و با تشخیص دادگاه صالح موارد علیه امنیت ملی رخ داده باشد. استثنائات و شرایط دیگر هم بایستی صریحا پیش بینی شود.

در آیین نامه واحدهای ارائه کننده خدمات اطلاع رسانی و اینترنتی (ISP)[1] نیز با توجه به اینکه رساها (ISP)، امکان اتصال به شبکه اطلاع رسانی و اینترنت را فراهم می‌آورند و جزء ضروری دسترسی و اتصال افراد به شبکه اینترنت می‌باشند و با داشتن امکانات ویژه می‌توانند راحت تر از دیگران حریم خصوصی اطلاعاتی شهروندان را نقض کنند و از طرف دیگر فعالیت نظام مند آن‌ها مبتنی بر تدابیر امنیتی می‌تواند از ارتکاب بسیاری از جرایم علیه داده‌های شخصی پیشگیری کند، مقررات مهمی در رابطه با حریم خصوصی شهروندان در بند ۵ این آیین نامه و ذیل آن آورده شده است که عبارتند از:

الف) هر رسا موظف است اطلاعات کلی کاربران را ثبت کند. بایستی در این آیین نامه مقرر می‌شد که ثبت اطلاعات جزئی تنها با اجازه قانون یا مقام صالح قانونی امکان پذیر است و در ضمن اینکه رساها موظف به ثبت فعالیتهای اینترنتی کاربران شده اند، بایستی نوع اطلاعات، حدود آن و شرایط مرتبط با آن صریحا اعلام می‌شد. در غیر این صورت این بند می‌تواند علیه حریم خصوصی کاربران باشد.

ب) رسا می‌تواند با عقد قرارداد با مشترکین خود حدود تکالیف خود و حقوق کاربر را مشخص کند. عقد چنین قراردادهایی در راستای کاربرد حقوق کیفری به عنوان آخرین راه حل مفید خواهد بود.

ج) از نکات بسیار جالب توجه این آیین نامه تلاش آن برای ایجاد یک رویه معقول در استفاده از سیستم رمزنگاری است. رمزنگاری ضمن اینکه می‌تواند از تدابیر حفظ امنیت و حریم خصوصی اطلاعاتی شهروندان باشد در عین حال می‌تواند به عنوان ابزاری قوی در تبادل اطلاعات مجرمان خصوصا جرایم سازماندهی شده و تروریستی باشد. بنابراین آیین نامه به دلیل کاربرد مشروع آن حکم بر ممنوعیت استفاده از آن نداده است. ضمن اینکه کاربرد آن را مقید به اطلاع رسانی به مراجع صالح و کسب موافقت از این مراجع صالح نموده است.

۱- ISP برگرفته از کلمه Internet Service Provider یعنی شرکت خدمات سرویس های اینترنت است. یک ISP توسط یک خط تلفن از شرکت مخابرات و یا امکانات ماهواره ای می تواند اینترنت را به User خود سرویس دهد.

مشخصات متقاضی استفاده از فناوری رمز نگاری در دبیرخانه شورای عالی اطلاع رسانی ثبت می‌شود(حسنی، پیشین، ص ۱۱۷).

د) رساها موظف به حمایت فنی از حقوق کاربران نیز شده اند. ضمن اینکه رساها موظفند که حقوق کاربران را به ایشان اطلاع دهند و نحوه حفاظت از حریم خصوصی اطلاعات و ارتباطات را به ایشان آموزش دهند. این تکالیف با یک رویکرد حمایتی درصدد پیشگیری از تجاوزات به حقوق کاربران و مخصوصا حریم خصوصی ایشان است.

ه) آیین نامه ضمن تاکید بر مصونیت حریم خصوصی کاربران در بندهای ۵-۳-۱۵ و ۶-۱۳، آیین نامه در بند ۹، تجاوز به حریم خصوصی کاربران را مقید به یک سری ضمانت اجراهای اداری کرده است. ضمن اینکه این ضمانت اجراها مانع طرح مورد در دادگاه‌ها و اعمال حقوق کیفری نخواهد بود. این بند آیین نامه فاقد شفافیت و وضوح کافی در تعیین ضمانت اجراهاست. ضمن اینکه در بند ۶ مصادیق مهمی از تجاوز به حریم خصوصی مانند شنود یا دسترسی غیر مجاز تخلف شمرده شده اند درحالیکه هنوز این موارد غیر از ضمانت اجراهای اداری این ماده مشمول هیچ حکم کیفری نمی شوند.

و) مرجع رسیدگی به این تخلفات، کمیسیون راهبردی است که مهمترین کمیسیون شورای عالی اطلاع رسانی است.

در عرصه بین المللی نیز، اکثر کشورهای غربی به وضع مقررات و قوانین داخلی درباره‌ی حمایت از داده‌ها پرداخته اند:

۱) در اتریش، قانون فدرال شماره ۵۶۵ درباره‌ی حمایت از داده‌های شخصی، مصوب هجدهم اکتبر ۱۹۷۸ (که مربوط به بخش‌های دولتی و خصوصی بوده و اساساً دربرگیرنده مجوز اداری گردش فرامرزی داده‌ها است)؛

۲) در کانادا، قانون فدرال دسترسی به اطلاعات و قانون فدرال حریم خصوصی، در تاریخ بیست و هشتم ژوئن ۱۹۸۲ تصویب شده و در تاریخ اول ژوئیه ۱۹۸۳ لازم الاجرا شدند (این قوانین صرفاً درخصوص بخش‌های دولتی قابل اعمال بوده و فاقد مقرراتی درباره‌ی گردش فرامرزی داده‌ها هستند)، نیز در سطح ایالتی «قانون ایالت کبک، مربوط به دسترسی به اسناد نگهداری شده به وسیله ارگان‌های عمومی و

حمایت از اطلاعات شخصی» که در تاریخ بیست و سوم ژوئن ۱۹۸۲ به تایید دربار رسید (و فقط درخصوص بخش دولتی قابل اعمال است)؛

۳) در فرانسه، قانون شماره ۱۷-۷۸ درباره‌ی داده پردازی، فایل‌های داده و آزادی‌های فردی مصوب ششم ژانویه ۱۹۷۸ (که درخصوص بخش‌های دولتی و خصوصی قابل اعمال بوده و مطابق آن باید گردش فرامرزی داده‌ها به کمیته ملی داده پردازی و آزادی‌ها اعلام شود)؛

۴) در آلمان غربی، قانون فدرال حمایت از داده ها، مصوب بیست و هفتم ژانویه ۱۹۷۷ که از تاریخ اول ژانویه ۱۹۷۹ لازم الاجرا شد (و درخصوص بخش عمومی فدرال و بخش خصوصی قابل اعمال بوده و مطابق آن در مواردی که انتشار داده‌ها در آلمان غربی مجاز است، گردش فرامرزی آن را مجاز می‌داند)، نیز قوانین ایالتی مختلفی درخصوص حمایت از داده‌ها (که درخصوص بخش عمومی ایالتی قابل اعمال هستند)؛

در ایالات متحده آمریکا، قانون حاکم بر نظارت بر ارتباطات الکترونیکی، قانون حریم خصوصی ارتباطات الکترونیکی مصوب ۱۹۸۶[1]، فصل ۱۸ از مجموعه قوانین ایالات متحده، بخش‌های فرعی ۲-۲۵۱۰ ، ۲۵۱۱ و ۱۱-۲۷۰۱ می‌باشد. این قانون (ECPA)، رهگیری غیر مجاز و عمدی در ارتباطات سیمی، شفاهی و الکترونیکی را منع می‌کند. بخش فرعی ۲۵۱۱ این قانون «ایجاد دسترسی» غیر مجاز به یک ارتباط سیمی یا الکترونیکی را نیز منع می‌کند. برای جبران خسارت در صورت نقض این قانون، هر شخص می‌تواند ضرر و زیان‌های واقعی یا قانونی، هزینه وکلا، و برای اقسام خاصی از تخلف، خسارات تنبیهی (کیفری) دریافت کند. متخلفین نیز بر حسب اینکه ارتباطات در حال انتقال رهگیری شده یا چند دقیقه، چند روز، یا چند هفته پس از ذخیره شدن در یک کامپیوتر یا دستگاه دیگر دسترسی به آن حاصل شده باشد، با مجازات‌های متفاوتی روبه رو می‌شوند. تخلف از بخش ۲۵۱۱، که رهگیری را ممنوع می‌کند، تا سقف ۱۰۰۰۰ دلار جریمه و یا حداکثر ۵ سال زندان در بر دارد. تخلف از بخش ۲۷۰۱ که دسترسی به ارتباطات ذخیره شده را ممنوع می‌سازد، تا سقف ۱۰۰۰۰ دلار جریمه و یا حداکثر یک سال

1- Electronic Communication Privacy Act (ECPA) 1986.

حبس در بر دارد. با این حال یک کارفرما می‌تواند ارتباطات سیمی، الکترونیکی یا شفاهی را در صورت اخذ رضایت قبلی فقط یکی از طرفین ارتباط رهگیری نماید[1]. رضایت صریح می‌تواند از طریق امضاء یک برگه اعراض از حق یک شرط استخدام ،که به کارفرما اجازه کنترل مکالمات تلفنی را می‌دهند، تضمین گردد.

در ایالات متحده اکیداً سفارش شده است که افراد، آیین نامه حریم خصوصی[2] مربوط به شرکتی که در آن مشغول هستند را به طور کامل مطالعه نماید تا از نحوه کنترل و شنودها اطلاع داشته باشند. در این آیین نامه‌ها تمام ضوابط نظارت ذکر شده است. علاوه بر آن برای حصول اطمینان از آگاهی تمام افراد از سیستم کنترل، این ضوابط، دائما از طریق جلسات، تذکرات، دفترچه‌های کارمندی[3] یا حتی بر چسب هایی که گوشه کامپیوتر نصب می‌شود و به کارمندان منتقل می‌شوند).http://www.usatoday.com)

۸) سایر قوانین و مقررات

۸-۱- قانون مسئولیت مدنی

این قانون ۲ ماده بسیار مهم در حمایت مدنی از عنوان کلی «حیثیت» و نیز «اعتبارات شخصی یا خانوادگی» دارد. ماده ۱ این قانون مقرر می‌دارد: «هر کس بدون مجوز قانونی عمدا یا در نتیجه بی احتیاطی به جان یا سلامتی یا مال یا آزادی یا حیثیت یا شهرت تجارتی یا به هر حق دیگر که به موجب قانون برای افراد ایجاد گردیده لطمه‌ای وارد نماید که موجب ضرر مادی یا معنوی دیگری شود مسئول جبران خسارت ناشی از عمل خود می‌باشد».

ماده ۱۰ این قانون نیز راه حل‌های قابل توجهی در موارد لطمه به حیثیت افراد پیش بینی می کند:

«کسی که به حیثیت و اعتبارات شخصی یا خانوادگی او لطمه وارد شود می‌تواند از کسی که لطمه وارد آورده است جبران زیان مادی و معنوی خود را بخواهد. هرگاه اهمیت زیان و نوع تقصیر ایجاب نماید دادگاه می‌تواند در صورت

1- Electronic Communication Privacy Act (ECPA) 1986.
2- Privacy Policy
3-. Employee Handbook

اثبات تقصیر علاوه بر صدور حکم به خسارت مالی، حکم به رفع زیان از طریق دیگر از قبیل الزام به عذرخواهی و درج حکم در جراید و امثال آن نماید».

این مواد در حمایت از حریم خصوصی اطلاعاتی و ارتباطاتی افراد نیز نقش مهمی دارند زیرا در اکثر موارد، نقض این حق همراه با لطمه به«حیثیت و اعتبارات شخصی یا خانوادگی» فرد است. با این حال می‌توان مصادیقی از نقض حریم خصوصی یافت که صرفا آسایش فرد را به هم بزند بدون اینکه حیثیت یا اعتبار شخص را از بین ببرد.

نتیجه گیری

حق اشخاص در مصون ماندن حریم خصوصی ایشان از هرگونه تعرض و تعدی در زمره حقوق اساسی و اولیه اعطاء شده به نوع بشر است. لیکن ظهور فناوری‌های پیشرفته در زمینه اطلاعات و ارتباطات، به نحو قابل ملاحظه ای، تحول و چالش‌های جدیدی را پیش روی مباحث مربوط به حریم خصوصی گذارده است. همگانی شدن امکانات فناوری اطلاعات نظیر تلفن همراه، اینترنت و مانند آن موجب شده است که غالب افراد جامعه به نوعی در معرض ارتکاب جرم قرار گیرند و یا قربانی آن شوند. برای مثال، امروزه تعقیب دیگران همراه با فیلمبرداری و یا عکسبرداری توسط دوربین تلفن‌های همراه و قرار دادن آن در شبکه اینترنت می‌تواند زندگی فرد را با اختلال جدی مواجه سازد. مشابه همین افعال، ضبط صدای دیگران در میهمانی‌ها و جلسات دوستانه و ایراد لطمه حیثیتی به قربانی آن، با استفاده از تجهیزات مدرن، دامنه‌ای بس متفاوت خواهد داشت.

بر این اساس، اعمال قوانینی سنتی و یا حتی جدید، بدون توجه به دامنه تاثیرگذاری جرم، نمی تواند پاسخگوی نیازهای روز باشد و مسلما تقنینی در این گونه موارد با نگاهی به اهمیت و جایگاه حریم خصوصی در زمینه اطلاعاتی ضروری است. در تقسیم بندی جهان حاضر به دو فضای حقیقی و مجازی، طبیعی است که استناد به مبانی سنتی، نیازهای امروز را برآورده نمی سازد. افزون بر آن صرف تصویب قوانین جدید نیز پاسخگوی تحولات و نیازهای جدید نیست. امروزه دنیای واقعی آن قدر متحول شده است که نیازمند به روز شدن قواعد و

تجدید نظر در مبانی آزادی اطلاعات در حوزه‌های مربوطه و نیز قلمرو حریم خصوصی است. بنابراین جرم انگاری صحیح و تعیین ضمانت اجرایی موثر در راستای اهداف اصلی و تدابیر کیفری یعنی «حتمیت، قطعیت و تناسب» می‌تواند راهگشای نیل به دو دستاورد ویژه حقوق کیفری یعنی ارعاب انگیزی و عبرت انگیزی باشد. بدین معنی که علاوه بر پیشگیری کیفری از وقوع جرم، سدی در برابر تکرار آن نیز باشد و سنجش میان منفعت حاصل از ارتکاب جرم و مشقت حتمی ناشی از مجازات، در قالب عامل بازدارنده ارتکاب یا تکرار جرم تجلی یابد. میزان حمایت هر جامعه از حریم خصوصی را ضوابط پیش بینی شده در قوانین آن کشور معین می‌سازند. ناتوانی سیستم قانونگذاری در ایجاد تعادل بین حقوق افراد و مصلحت عمومی باعث شده تا این حق به عنوان یکی از حقوق اساسی افراد در پهنه حمایت کیفری کمتر مورد توجه قرار گیرد. تنها راه حمایت از حریم خصوصی ضمن پذیرش لزوم محدود کردن آن در مواردی خاص، ضابطه مند کردن تعدیات احتمالی به انواع مختلف آن است.

به طور کلی در تمامی اشکال حریم خصوصی، نقض احتمالی آن باید حسب مورد، با احراز ضرورت بر اساس دلایل قابل قبول، به موجب تصمیم قضایی مقام صالح در رسیدگی‌های قضایی با رعایت تناسب میان اتهام و نوع مجوز صادره به صورت موردی انجام گیرد.

قوانین ایران در ارتباط با حمایت از حریم خصوصی همگام با تحولات پدید آمده در این زمینه نیست. از توجه به مطالب مذکور در این مقاله چنین بر می‌آید که در سیاست کیفری ایران، چه در قانون اساسی و چه در قوانین عادی، به صورت صریح به مفهوم حریم خصوصی اشاره نشده است و چنین استنباط می‌شود برخی از مصادیق آنچه که در اصطلاح به حریم خصوصی معروف است در برخی مواد مورد توجه قرار نگرفته است. مجموع احکام پیش بینی شده در این مواد نشان می‌دهد که اولا قانونگذار تمامی مصادیق حریم خصوصی را مد نظر قرار نداده است. ثانیا، حتی در آن قسمت که مد نظر قرار داده است، حمایت‌های لازم، چه کیفری و چه مدنی از آن به عمل نیاورده است. لذا این میزان از حمایت به هیچ وجه پاسخگوی نیازهای جامعه امروز و چالش‌های فرا روی جامعه در عصر

اطلاعات نیست و بازبینی کلی قوانین و گردآوری آن‌ها در مجموعه‌های قانونی جامع و یکپارچه ضروری است. بنابراین به عنوان پیشنهاد به نظر می‌رسد که باید هنگام مواجهه با جرایم متکی بر فناوری‌های مدرن، فارغ از تعاریف سنتی و کلاسیک، ماهیت آن‌ها بررسی و یا بازخوانی شود و سپس بر اساس معیارهای علمی از جمله میزان لطمه‌ای که به قربانی جرم وارد گردیده و نیز ارزش‌های مورد حمایت و همچنین ملاک‌های واقعی مانند گستره اثرگذاری و دامنه جرم و با در نظر گرفتن رابطه علیت و تناسبات مورد توجه در حقوق جزایی، به تعریف فعل مجرمانه و سپس تعیین مجازات آن پرداخته شود.

منابع

۱) آقایی نیا، حسین، حقوق کیفری اختصاصی (جرایم علیه اشخاص)، تهران، نشر میزان، ۱۳۸۶.

۲) انصاری، باقر، حقوق حریم خصوصی، تهران، انتشارات سمت، ۱۳۸۶.

۳) جلالی فراهانی، امیر حسین، پیشگیری از جرایم رایانه ای، مجله حقوقی دادگستری، شماره ۴۷، ۱۳۸۳.

۴) حسنی، جعفر، حمایت کیفری از حریم خصوصی در فضای سایبر، پایان نامه کارشناسی ارشد، دانشکده حقوق دانشگاه شهید بهشتی، ۱۳۸۵.

۵) رحمدل، منصور، حق انسان بر حریم خصوصی، مجله دانشکده حقوق و علوم سیاسی، شماره ۷۰، ۱۳۸۴.

۶) عالی پور، حسن، جرایم ضد امنیت ملی، تهران، میزان، ۱۳۸۴.

۷) گروه مطالعات حقوق عمومی، اظهار نظر کارشناسی درباره لایحه حمایت از حریم خصوصی(شور اول)، دوره هفتم- سال دوم، ۱۳۸۴.

۸) گروه ارتباطات و فناوری‌های نوین مرکز پژوهش‌های مجلس، گزارش توجیهی لایحه جرایم رایانه ای، نشریه اطلاع رسانی و کتابداری، شماره ۹۶، ۱۳۸۴.

۹) محسنی، فرید، حریم خصوصی اطلاعات، تهران، دانشگاه امام صادق(ع)، ۱۳۸۹.

۱۰) محسنی، فرید و قاسم زاده، فریدون، چالش‌های قانونی تجارت الکترونیکی در ایران، کنفرانس بین المللی مدیریت، تهران، ۱۳۸۲.

۱۱) محسنی، فرید و قاسم زاده، فریدون، حریم شخصی در فضای مجازی با تکیه بر حقوق ایران، فصلنامه علمی و پژوهشی شریف، شماره ۳۴، ۱۳۸۵.

منابع انگلیسی

۱۲) Oncidi, Anthony J., Mckenna, Kathleen. Privacy in the workplace, Proskauer Rose LLp, ۲۰۰۶.