مطالعۀ تطبیقی ضوابط قانونی کنترل ارتباطات الکترونیک در کشف جرائم
(برخی کشورهای اروپایی، امریکا و ایران)

مجتبی ستوده گندشمین[۱]
ناصر عتباتی[۲]

تاریخ دریافت: ۹۹/۲/۱۷
تاریخ پذیرش: ۹۹/۵/۱۸

چکیده

زمینه و هدف: پیشرفت فناوری‌های نوین استفاده از کنترل ارتباطات الکترونیک در کشف جرائم ملی و فراملی ناقض امنیت داخلی و خارجی کشـــورها از جمله قاچاق انســـان، موادمخدر، تروریسم، پولشـــویی، ترور، دزدی دریایی و قتل‌های زنجیره‌ای را اجتناب‌ناپذیر ســـاخته است. این پژوهش با هـــدف مطالعـــۀ تطبیقی ضوابط قانونی حاکم بر کنترل ارتباطات الکترونیک در اروپا و امریکا با ایران نگارش شده است.

روش: روش تحقیق در این پژوهش از نوع تحلیلی- توصیفی و روش گردآوری داده‌ها، کتابخانه‌ای- اسنادی است.

یافته‌ها و نتیجه‌گیری: نظام حقوقی کشـــورهای موردمطالعه، شرایط خاصی را تصویب کرده‌اند که ضمن احترام کامل به حریم خصوصی افراد، کنترل هرگونه ارتباطات الکترونیکی را مجاز و امکان اســـتفاده از محتوای ارتباطات الکترونیک را پیش‌بینی کرده اســـت. اصل و مبنای کنترل ارتباطات الکترونیک چه در حقوق ایران و چه در نظام حقوقی امریکا و کشورهای اروپایی، عدم کنترل ارتباطات الکترونیک در حوزۀ حریم خصوصی است

کلید واژه‌ها: ارتباطـــات الکترونیک، کنترل ارتباطات الکترونیـــک، حریم خصوصی، ارتباطات مخابراتی، جرائم سازمان‌یافته.

---

۱. عضو هیئت علمی گروه کشف جرائم دانشگاه علوم انتظامی امین، نویسندۀ مسئول:
snow.man.1983@chmail.ir
۲. دکتری حقوق جزا و جرم‌شناسی پژوهشگاه قوه قضائیه..

مقدمه

بـــا توجه به پیچیدگـــی جرائم و اینکه بزهکاران برای پیشـــبرد اهـــداف مجرمانهٔ خود از فناوری‌های اطلاعاتی و ارتباطی پیشـــرفته‌ای استفاده می‌کنند، اگر پلیس کشورها از همان شـــیوه‌های متعارف و معمول کشـــف جرم برای تعقیب و کشف جرائم استفاده کنند، بدیهی است که موفقیت ناچیزی کسب می‌کنند (ستوده و عالیزاده، ۱۳۹۴: ۶۵). در تعقیب و کشف انواع جرائم، روش‌ها و شیوه‌های متفاوتی وجود دارد و هرکدام از کشورها در راه دستیابی به این هدف، شیوه و روش خاصی را بکار می‌برند و در تلاش هستند تا به موازات پیشرفت‌های فنـــاوری و پیچیدگـــی روابط اجتماعـــی از طریق تخصص گرایی، خود را مجهز و مســـلح به آموزه‌های نو و شیوه‌های جدید در جرم‌یابی و کشف عملیات پنهان مجرمان حرفه‌ای بکنند و در راه مقابله با مجرمان که طرح و تدبیر فناوری را باهم در اختیار گرفته‌اند موفق عمل کرده و با کمترین هزینه مادی و انسانی تولید امنیت را به جامعه اهدا کنند (طالبیان، ۱۳۹۱: ۱۲۷). از شیوه‌های مؤثر و اثربخش در کشف جرائم، استفاده از کنترل ارتباطات الکترونیکی است.

ارتباطات الکترونیک از مهم‌ترین جلوه‌های حریم خصوصی در جهان به شـــمار می‌رود که حرمت تجسس در آن براساس مستندات حقوقی بین‌الملل و حتی قوانین داخلی کشورها مورد تأکید قانون‌گذاران ادوار مختلف بوده اســـت. منظور از ارتباطات الکترونیکی، کلیهٔ ارتباطاتی اســـت که برای انتقال هرگونه پیام خصوصی، با استفاده از ابزارهای مخابراتی و ارتباطی مثل مکالمات تلفن، پیامک، ایمیل بین دو نفر ردوبدل می‌شود. حال اگر این نوع ارتباطات کنترل شـــود، در حقیقت نوعی کنترل ارتباطات الکترونیکی انجام شده است. مهم‌ترین نوع کنترل ارتباطات الکترونیکی که در رویه‌های موجود قضایی برای کشف جرم استفاده می‌شود، شنود مکالمـــات تلفنی، اســـتخراج متن پیامک خطوط ارتباطی همـــراه و گاهی نیز بازخوانی متن پست‌های الکترونیکی که از آن‌ها به ایمیل یاد می‌شود، است (ستوده و عتباتی، ۱۳۹۸: ۱۰۳). پیشـــرفت فناوری‌های علمی کشف جرائم، استفاده از کنترل ارتباطات الکترونیک در کشف جرائم ملی و فراملی سازمان‌یافتهٔ ناقض امنیت داخلی و خارجی کشورها ازجمله قاچاق انسان، موادمخدر، تروریســـم، پولشـــویی، ترور، دزدی دریایی و قتل‌های زنجیره‌ای را اجتناب‌ناپذیر ساخته است. اما، از آنجایی که یکی از حوزه‌های مهم حریم خصوصی، ارتباطات است که به

معنای مصون بودن و حفظ حرمت تمامی انواع ارتباطات شهروندان اعم از مراسلات، مکاتبات و مخابرات از هرگونه دستیابی غیرمجاز مانند رهگیری، تفتیش، تخریب و شنود است و ارتباطات خصوصی ممکن است در شکل‌های مختلف نظیر ارسال نامهٔ پستی، تلفن، فاکس، وسایل ارتباطی رادیویی، وسایل ارتباطاتی نوین نظیر اینترنت، ایمیل و غیره .برقرار شود که برای برقراری همهٔ انواع ارتباطات خصوصی از واسطه‌های انسانی یا فنی استفاده می‌شود. از این‌رو، همواره مضمون پیام‌ها توسط واسطه‌ها در معرض خطر افشا است. همچنین، امکان انواع کنترل، پایش و شنود ارتباطات حتی در پیشرفته‌ترین اشکال و فناوری‌های آن وجود دارد و این امر می‌تواند زندگی خصوصی شهروندان را به مخاطره افکند.

برای حمایت کافی و مؤثر از حریم خصوصی داده‌های شخصی در ارتباطات الکترونیکی از جمله ارتباطات مخابراتی و اینترنتی، وجود قواعد حقوقی متناسب با چنین حمایتی اجتناب‌ناپذیر است (زرکلام، ۱۳۸۶: ۱۷۵) تا ضمن ممنوعیت دسترسی ارائه‌دهندگان خدمات به کاربران که با داده‌های شخصی افراد سروکار دارند و الزام آن‌ها به رعایت مسائل ایمنی و حفاظتی در برابر نفوذکنندگان، راهکارهایی قانونی برای دسترسی مقامات مسئول پلیسی و قضایی را به هنگام نیاز به محتوای ارتباطات الکترونیک را فراهم سازد.

این قواعد قانونی از مدت‌ها پیش در قالب مقررات قانونی در حقوق برخی از کشورهای اروپایی وارد شده است. اولین قانون ملی حمایت از داده‌ها در سال ۱۹۷۳ در سوئد تصویب شد (قاجار، ۱۳۸۹: ۷۵). همچنین، می‌توان به قانون حمایت از دادهٔ سال ۱۹۸۴ انگلستان که از سال ۱۹۹۸ با قانونی به همین نام جایگزین شد (باین بریدج[1]، ۲۰۱۰: ۳۵) نیز قانون شمارهٔ ۷۸-۱۷ مورخهٔ ۶ ژانویه ۱۹۸۷ فرانسه راجع به «انفورماتیک، پَروَنجاها و آزادی‌ها» که به‌ویژه با قانون مورخ ۱۸ ژوئن ۲۰۰۱ تحت عنوان «حمایت از اشخاص حقیقی در مقابل پردازش داده‌های خصوصی» مورد اصلاح واقع شده است، اشاره داشت (زرکلام، ۱۳۸۶: ۱۷۴). اما در قوانین موضوعهٔ ایران، متأسفانه حریم خصوصی و حق بر حریم خصوصی و در رأس آن‌ها ارتباطات الکترونیک اعم از ارتباطات مخابراتی یا شبکه‌های اجتماعی به‌صورت مشخص، دقیق و مدون، مورد حمایت واقع نشده و موضع حقوق موضوعه ایران، همانند

1. Bainbridge

موضع نظام اسلامی، در مواجهه با حریم خصوصی، یک موضع تحویل‌گرایانه است و حقوق و آزادی‌هایی که تحت عنوان حریم خصوصی حمایت می‌شوند، به‌طور ضمنی و در بطن سایر قواعد حقوقی ایران و در قالب احاله به حقوق و آزادی‌های دیگر مورد حمایت قرار گرفته‌اند (فروغی و همکاران، ۱۳۹۳: ۱۴۰). در این پژوهش، شرایط و ضوابط قانونی و قضایی کنترل ارتباطات الکترونیک در برخی کشـــورهای اروپایی و امریکا بحث، ســـپس قوانین موجود در ایران نیز مورد کنکاش گذاشته خواهد شد.

حریم خصوصی و ارتباطات الکترونیک

بـــا توجه به تغییراتـــی که در نوع نگاه و نگرش جوامع مختلـــف در خصوص مفهوم حریم خصوصی و دامنهٔ شـــمول آن وجود دارد، هنوز یک تعریفی کامل و مدون از اصطلاح «حریم خصوصی» انجام نشده و هریک از صاحب‌نظران نیز تعاریف مختلفی از حریم خصوصی ارائه کرده‌اند. برای مثال، ادوارد بلوستین[1] نقض حریم خصوصی را به‌عنوان یک اقدام توهین‌آمیز نســـبت به شرافت بشری قلمداد می‌کند. اما شـــاید توصیف حریم خصوصی به‌عنوان توهین به شـــرافت بشـــری کافی نباشد؛ زیرا گرچه نقض حریم خصوصی، نقض شرافت بشری است، شرافت فردی ممکن است بدون تجاوز به حریم خصوصی نیز مورد لطمه قرار گیرد (انصاری، ۱۳۹۳: ۸). حریم خصوصی را چنین نیز تعریف کرده‌اند: «تمایل هریک از ما به داشتن فضای فیزیکی که می‌توانیم در آن از مداخله، مزاحمت، اضطراب، آشفتگی و پاسخگویی رها باشیم و تلاش برای کنترل زمان و شـــیوهٔ افشای اطلاعات شـــخصی دربارهٔ خودمان» (نمکدوست تهرانی، ۱۳۹۵: ۸). در خصوص این تعریف باید گفت که حریم خصوصی صرفاً فضای فیزیکی را شـــامل نمی‌شود، بلکه فضای مجازی نیز ممکن است حریم خصوصی محسوب شود. برای مثال، شنود تلفن، نقض یک فضای مجازی است که نقض حریم خصوصی محسوب می‌شود. پس تعریف حریم خصوصی به فضای فیزیکی کامل به نظر نمی‌رسد. در همین زمینه، از سال ۱۹۲۸ دیوان عالی کشـــور ایالات متحده آمریکا در پرونده‌ای، شنود تلفن افراد توسط پلیس را ناقض حریم خصوصی ایشان دانست. بنابراین، شنود تلفن نقض بارز حریم خصوصی افراد

1- Edward j.Bloustein

محسوب می‌شود (اکر و برودی[1]، ۲۰۱۴: ۴۹). حقوقدانان ایرانی هم هریک به نوعی تعریفی از حریم خصوصی ارائه کرده‌اند. برخی حریم خصوصی را بخشی از حوزهٔ خصوصی دانسته و می‌گویند: «حوزهٔ خصوصی شامل دو قلمرو است؛ نخست قلمرو روابط شخصی و خانوادگی که بیشتر با عنوان حریم خصوصی شناخته می‌شود و دوم قلمرو خصوصی مبادلهٔ کالا و خدمات اجتماعی که در علم اقتصاد با عنوان اقتصاد بخش خصوصی شناخته می‌شود» (نوبهار، ۱۳۹۷: ۴۹). در تعریف دیگری آمده است: «حریم خصوصی عبارت است از هر آنچه در قلمرو یک شخص قرار دارد یا مختص به وی است و ورود و تعرض به آن ممنوع، مگر با اجازهٔ شخص یا در موارد استثنایی یا تجویز قانون» (احمدی، ۱۳۹۷: ۶).

مهم‌ترین جلوهٔ حریم خصوص نیز ارتباط الکترونیک است که متداول‌ترین وسیلهٔ ارتباطی اشخاص در جامعه است که روزانه از طریق تلفن‌های ثابت و همراه در بستر اینترنت و فیبر نوری انجام می‌گیرد. به همین جهت، بیشترین حساسیت و نگرانی نسبت به مکالمات تلفنی وجود دارد. بدین ترتیب، کنترل مکالمات تلفنی و سیگنال‌های رادیویی، پردازش محتوای در حال انتقال شبکه‌های اجتماعی پیام‌رسان، پسته‌ای الکترونیکی و پیامک‌ها از رایج‌ترین موارد نقض حریم خصوصی ارتباطی است. پیشرفت‌های فناوری ازجمله مهم‌ترین عواملی است که شنود و رهگیری تلفن‌های معمولی و همراه، کانال‌های رادیویی اعم از زمینی و یا ماهواره‌ای را ممکن و تسهیل می‌کند. در چنین شرایطی باید در مورد تهدیدهای فراوانی که حریم ارتباطات شخصی را در معرض خطر جدی قرار می‌دهد، تضمین‌های حقوقی و قانونی مناسب در نظر گرفته شود.

اهمیت این نوع حریم خصوصی از آن جهت است که ارتباطات در فضای الکترونیکی دو نوع داده تولید می‌کند؛ یکی داده‌های مرتبط با محتوای ارتباط اعم از صوت، تصویر، اسناد یا مدارک در حال مبادله و غیره و دیگری داده‌هایی که براساس زمان و مکان برقراری ارتباط، طول مدت ارتباط، شبکه‌ها و مسیرهایی که ارتباط توسط آن‌ها برقرار می‌شود و غیره که دستهٔ دوم داده‌ها بسیار اهمیت دارند. داده به هر نمادی از واقعهٔ اطلاعات یا مفاهیم قابل‌پردازش در سیستم رایانه‌ای یا مخابراتی اطلاق شده است که این تعریف گسترده هم شامل محتوا و هم دادهٔ ترافیک می‌شود.

1- Acker and Brody

ارتباطات الکترونیکی به شـــکل‌ها و روش‌های گوناگونی انجام می‌شود؛ ازجمله ارتباطات از طریق شـــبکه‌های رایانه‌ای، موبایل‌های هوشـــمند و شـــبکه‌های مجازی. نقش ارتباطات الکترونیـــک در ادارات و نهادهـــای دولتی و خصوصی پررنگ‌تر از گذشـــته بوده و هر جامعه برای ســـامان بخشیدن به این ارتباطات، قوانین و مقررات مربوط به خودش را اعمال می‌کند و ایجـــاد حفاظـــت از داده‌ها و اقدامات امنیتی برای بخش ارتباطات الکترونیکی تحت قوانین ملی و بین‌المللی تأسیس شده است (آیتی و محمدزاده، ۱۳۹۴: ۳۴). آنچه از مفهوم ارتباطات الکترونیک در این پژوهش به دنبال آن هستیم، ارتباطاتی است که به‌واسطهٔ استفاده از یکی از ابزارهای الکترونیکی مثل تلفن، ایمیل، فضای مجازی و شـــبکه‌های اجتماعی اســـت که مجرمان برای رفتار مجرمانهٔ خود از آن‌ها بهره می‌برند.

چنانچـــه حوزهٔ فناوری اطلاعات و ارتباطات را شـــامل دو حـــوزهٔ فناوری‌های ارتباطاتی و فناوری‌های اطلاعاتی در نظر بگیرم، این پژوهش به حوزهٔ فناوری‌های ارتباطاتی می‌پردازد. البتـــه بـــا توجه به وقوع همگرایی خدمات، فناوری و ظهـــور مفهوم فاوا، تفکیک این دو لزوماً همواره معتبر نیســـت. لذا حوزهٔ مشـــترک نظیر ارتباطات مبتنی بر آی‌پی (IP) نیز در این پژوهش مورد بررسی قرار می‌گیرد. هرچند حوزهٔ ارتباطات غیرالکترونیک مانند پست سنتی را شـــامل نمی‌شود. حوزهٔ ارتباطات الکترونیک که در این پژوهش مورد بررسی قرار می‌گیرد شامل موارد زیر است:

- ارتباطات سیمی (تلگراف، تلفن و کابل‌های زیردریایی)؛
- ارتباطات رادیویی؛
- ارتباطات ماهواره‌ای؛
- ارتباطات کابلی؛
- ارتباطات شبکه‌ای شامل شبکهٔ اینترنت و سایر ارتباطات مبتنی بر آی‌پی؛
- ارتباطات موبایل و بی‌سیم؛

کنترل ارتباطات الکترونیک و شیوه‌های آن

امروزه و همســـو با نظام‌های حقوقی مختلف و حتی اســـناد بین‌المللی، یکی از مهم‌ترین

شیوه و شگردهای تحصیل ادلهٔ جرم خصوصاً جرائم سازمان‌یافته، خشن و تأثیرگذار در جامعه مانند قتل، آدم‌ربایی، تجاوز به عنف، کنترل ارتباطات الکترونیک است. این نظارت و کنترل به نظر نوعی تعرض به حریم خصوصی افراد محسوب می‌شود و در حالت معمول، جرم محسوب می‌شود. برای اینکه اقدامات مجریان قانون مشمول استثنای وارد بر این جرم باشد، نظام حقوقی کشورهای مختلف، شرایط خاصی را برای این فرآیند بار کرده‌اند که ضمن احترام کامل به حریم خصوصی افراد، کنترل هرگونه ارتباطات الکترونیکی را ممنوع اعلام داشته و در صورت عدم تعیین مسیر تحقیقات در پرونده‌های قضایی برای جرائم، امکان استفاده از محتوای ارتباطات الکترونیک را برای کشف جرم پیش‌بینی کرده است (ستوده و عتباتی، ۱۳۹۸: ۱۰۶). کنترل ارتباطات الکترونیک در حال حاضر معادل کلمه Interception در پدیده‌های الکترونیکی است و در عرصهٔ سایبر مورد استفاده قرار می‌گیرد و با مفهوم قبلی آن، حتی در عرصهٔ شنودهای مخابراتی متفاوت است. بنابراین، در مفهوم عام، کنترل لزوماً به معنای استراق سمع نیست، بلکه منظور از آن، اطلاع یافتن عمدی از محتوای در حال انتقال در سامانه‌های مختلف رایانه‌ای، مخابراتی، الکترومغناطیسی و نوری و در یک کلام، الکترونیکی است و حتی این مفهوم شامل محتوای ذخیره‌شده نیز می‌شود (محسنی، ۱۳۹۱: ۶۷).

کنترل ارتباطات الکترونیکی شامل گردآوردی اطلاعات از طریق ابزارهای الکترونیکی است؛ شگردهایی مانند استراق سمع، نظارت بر ارتباطات الکترونیکی و تفتیش و توقیف داده‌ها و دسترسی به متن پیامک و محتوای پست‌های الکترونیکی. در بسیاری از کشورها به دلیل رعایت تضمین‌های حقوق بشری، در مراحل اولیهٔ شناسایی کاربرد محدودی دارند؛ مگر آنکه ادلهٔ متقن و قانع‌کننده‌ای وجود داشته باشد که جرمی ارتکاب یافته یا در حال وقوع است. کنترل ارتباطات الکترونیکی غالباً در جایی مورد استفاده قرار می‌گیرد که نمی‌توان به‌وسیلهٔ اشخاص به یک گروه مجرمانهٔ منسجم نفوذ کرد یا مراقبت فیزیکی خطر نارواییی را برای تحقیقات یا ایمنی تحقیق‌کنندگان به دنبال داشته باشد. نظارت الکترونیکی به‌طور معمول تحت تضمینات قانونی و نظارت قضایی ویژه‌ای قرار می‌گیرد تا مورد سوءاستفاده قرار نگیرد (ستوده و نظری، ۱۳۹۳: ۱۰۱).

ارتباطات الکترونیک در فضای الکترونیکی، دو نوع داده تولید می‌کند. یکی داده‌های مرتبط

با محتوای ارتباط اعم از صوت، تصویر، اسناد یا مدارک در حال مبادله و دیگری داده‌هایی که براســـاس زمان و مکان برقراری ارتباط، طول مدت ارتباط، شـــبکه‌ها و مسیرهایی که ارتباط توســـط آن‌ها برقرار می‌شود؛ این داده‌ها که بســـیار اهمیت دارند، حسب مورد دادهٔ ترافیک و دادهٔ موقعیت گفته می‌شـــود. دســـته‌ای دیگر اطلاعات مربوط به کاربر یا کاربران ارتباطات الکترونیک اســـت. اطلاعاتی چون مشخصات اســـمی هویتی کاربران و نوع و مشخصات فنی دستگاه که به داده‌های شخصی معروف است. بنابراین، بایستی هرگونه دسترسی به داده‌های شـــخصی، داده‌های ترافیکی و داده‌های مرتبط با محتوای ارتباط اعم از صوت، تصویر، اسناد یا مدارک در حال مبادله، همچنین تحریف و تخریب آن‌ها و نیز بهره‌برداری از آن‌ها و انتشار ایـــن اطلاعـــات برای اهداف مجاز و غیرمجاز و بالاخره ردیابی اطلاعات مرتبط با هویت فرد و محتوای پیام‌های ارسالی را کنترل ارتباطات الکترونیک تعریف کرد. بنابراین، سه نوع کنترل ارتباطات الکترونیک داریم:

الف) دسترســـی مجاز یا غیرمجاز به داده‌های شخصی کاربران ارتباطات الکترونیک اعم از مشخصات اسمی و هویتی، مشخصات و نوع دستگاه برقرارکنندهٔ ارتباطات الکترونیک و سایر اطلاعات شخصی نظیر اطلاعات جسمانی، تصویر، صدا، عقاید فلسفی، مذهبی، سیاســـی، ریشـــه‌های نژادی و قومی و حتی نوع علائق و سلیقه‌ها که به‌عنوان فایل در دستگاه ذخیره شده است؛

ب) دسترســـی مجاز یا غیرمجاز به داده‌های ترافیکی مانند زمان و مکان برقراری ارتباط، طول مدت ارتباط، شبکه‌ها و مسیرهایی که ارتباط توسط آن‌ها برقرار می‌شود؛

پ) دسترسی مجاز یا غیرمجاز به داده‌های مرتبط با محتوای در حال انتقال یا ذخیره‌شدهٔ ارتباطـــات عمومـــی یا غیرعمومی اعم از پیام، صوت، تصویر، اســـناد یا مدارک در حال مبادله و غیره؛

کنترل ارتباطات الکترونیک در سیاســـت تقنینی اتحادیهٔ اروپا و برخی کشورهای اروپایی

در محدودهٔ اتحادیهٔ اروپا، سه دستورالعمل در سال‌های ۱۹۹۵ و ۲۰۰۲ و ۲۰۰۶ در زمینهٔ

حمایت از حریم خصوصی داده‌های شخصی به تصویب شورا و پارلمان آن رسیده که هر سه دستورالعمل در واقع مکمل هم هستند و در برخی از مواد این دستورالعمل فرآیند دسترسی قانونی به داده‌های شـــخصی، ترافیکی و محتوای در حال انتقال کنترل ارتباطات الکترونیک مورد بحث بوده است.

۱- دستورالعمل اروپایی مورخ ۲۴ اکتبر ۱۹۹۵[1]: این دستورالعمل که با عنوان «حمایت از اشخاص حقیقی در مقابل پردازش داده‌های شخصی و گردش آزاد داده‌ها» در شش بخش کلی تدوین شـــده اســـت که بخش ششـــم آن با نام «مقامات کنترل‌کننده و گروه حمایت از اشخاص در مقابل پردازش داده‌های شخصی» مربوط به موضوع بحث است.

برابر بند (۱) مادهٔ ۱۳ دســـتورالعمل مذکور، کشـــورهای عضو می‌توانند مقرراتی مبنی بر محدود کردن تکالیف و حقوق پیش‌بینی‌شـــده در مادهٔ (۱-۶)، مادهٔ (۱۰) و (۱-۱۱) و مواد ۱۲ و ۲۱ وضع کنند؛ به‌شرط اینکه این محدودیت‌ها برای ملاحظات زیر ضرورت داشته باشد: امنیت کشور، دفاع ملی، امنیت عمومی، پیشگیری، جستجو، کشف و تعقیب اعمال مجرمانه یـــا تخلفـــات انتظامی دربارهٔ حرفه‌های تابع مقررات خـــاص (زرکلام، ۱۳۸۶: ۱۸۳). مبرهن اســـت که بر این اساس، مقامات مسئول اعم از قضایی یا پلیسی و امنیتی می‌توانند در جهت پیشگیری، جستجو، کشف و تعقیب اعمال مجرمانه نسبت به دسترسی به داده‌های شخصی، ترافیکی و محتوای در حال انتقال ارتباطات الکترونیکی عمومی و غیرعمومی اقدام کنند.

۲- دســـتورالعمل اروپایی مورخ ۱۲ ژوئیه ۲۰۰۲[2]: دســـتورالعمل مذکور با عنوان «زندگی خصوصی و ارتباطات الکترونیکی» مکمل دستورالعمل ۱۹۹۵ شد که در مادهٔ (۵) آن، تضمین محرمانگی ارتباطات در خصوص داده‌های عبوری مورد تأکید قرار گرفته اســـت. همچنین، برابر بند (۱) مادهٔ (۴) دســـتورالعمل مارالذکر، امنیت خدمات ارتباطات الکترونیکی توســـط ارائه‌دهندگان خدمات اینترنتی به لحاظ فنی بایستی تضمین شود.

۳- دســـتورالعمل اروپایی ۱۵ مارس ۲۰۰۶: مطابق مادهٔ ۵ دســـتورالعمل، انواع داده‌هایی که کشـــورهای عضو مکلف به نگهداری آن‌ها هســـتند، عبارت‌انـــد از: داده‌هایی که یافتن و

1- Cf.Directive n.95/46/ce

2- Cf.Directive europeénne du 12 juillet 2002

شناسایی مبدأ ارتباط (شماره تلفن تماس‌گیرنده و نام و آدرس مشترک یا کاربر) را ممکن سازد، داده‌هایی که برای شناسایی مقصد ارتباط (شماره تلفن طرف مکالمه) ضروری هستند، داده‌هایی که امکان تعیین تاریخ و ساعت و مدت ارتباط را فراهم سازد و بالاخره، داده‌هایی که برای شناسایی نوع ارتباط و هویت ملی طرفین ارتباط ضروری هستند. مدت نگهداری از داده‌ها با توجه به مادۀ ۶ دستورالعمل، حداقل ۶ ماه و حداکثر ۲ سال است.

با دقت در سایر مواد دستورالعمل مشخص می‌شود که به‌طور مشخص هدف تدوین‌کنندگان این دستورالعمل، مبارزه با انواع جرائم خصوصاً جرائم سازمان‌یافته و تروریسم است. احتمالاً برای جلوگیری از سوءاستفاده و نقض حریم خصوصی افراد در بند ۲ مادۀ (۱) دستورالعمل پیش‌بینی شده است که تکلیف دولت‌های عضو به نگهداری از داده‌ها، ناظر به محتوای ارتباطات الکترونیکی نیست. اما در قوانین داخلی برخی کشورهای اروپایی نیز به فرآیند کنترل ارتباطات الکترونیک پرداخته شده است.

– **سوئد:** پیشنهاد قانونی شنود و کنترل مکالمات و مراسلات تلفنی و اینترنتی یا همین *FRA* که نخستین بار در ۱۸ ژوئن ۲۰۰۸ در پارلمان سوئد به آراء نمایندگان واگذار شد؛ بیش‌ترین بحث را در مورد یک پیشنهاد قانونی در سوئد پدید آورد. این قوانین متشکل از یک سلسله اجزاست که به دولت، دبیرخانۀ دولت و نیروی دفاع کشور، این امکان را می‌دهد تا با استفاده از امکانات سازمان تجسس رادیویی وابسته به وزارت دفاع[1]، ترددهای اینترنتی و تلفنی را مورد شنود قرار دهند. هدف آن از ابتدا، از جمله این بود که نهادهای ذی‌ربط از فعالیت‌های مظنون تروریستی و بزهکاری‌های کلان به‌هنگام مطلع شوند و چنین فعالیت‌هایی را مورد پیگرد قرار دهند. این قانون به «گوش» سوئد در برابر جهان پیرامون موسوم شده است.

سازمان تجسس رادیویی وزارت دفاع سوئد یکی از نهادهای مهم دفاعی کشور به شمار میرود. بعد از حوادث تروریستی ۱۱ سپتامبر، دولت سوسیال دمکرات وقت، پیشنهادی به پارلمان ارائه کرد که کار تجسس در زمینۀ تردد وسائل ارتباطی که از سوئد میگذرند را ممکن میساخت. این پیشنهاد با مخالفت اکثر احزاب روبرو شد که باعث شد وزیر دادگستری وقت

1- Försvaret Radio Anstalt

سرانجام در سال ۲۰۰۶ پیشنهاد خود را پس بگیرد. بحث تجسس ترافیک اینترنتی و تلفنی بعدها وقتی احزاب بورژوائی زمام دولت سوئد را به دست گرفتند، توسط دولت ائتلاف احزاب بورژوائی پی گرفته شـــد و این احزاب پیشـــنهاد قوانینی تازه در این زمینه را به پارلمان ارائه دادند. پیشـــنهاد اولیهٔ ائتلاف احزاب بورژوائی در این زمینه در ســـال ۲۰۰۸ به‌طور مشروط به تصویب پارلمان رســـید و از ابتدای آن ســـال به مرحلهٔ اجرا گذاشته شد. شرط این بود که احزاب دولتی به تنظیم پیشنهاد بندهای جدید قانونی که ضامن حفظ حریم خصوصی باشند، بپردازند. پیشـــنهاد جدید دولت این بود که نهادهایی که اجرای قوانین شـــنود را عهده‌دار می‌شوند، باید پیش از آغاز عملیات تجسسی از یک دادگاه ویژه، مجوز بگیرند. اکثریت اعضای راست گروه دفاع پارلمان سوئد به این پیشنهاد رأی مثبت دادند (عتباتی، ۱۳۹۷: ۱۵۶).

– **آلمان:** مطابق مادهٔ ۱ بخش ۱۵ و مادهٔ ۱ بخش ۱۶، قانون فدرال حمایت از دادهٔ آلمان، در دسترس قرار دادن داده‌های شخصی بایستی به‌منظور انجام دادن وظیفه و تکلیف در بخش عمومی یا اجرای قرارداد در بخش خصوصی ضرورت داشـــته باشـــد و فقط به اندازهٔ ضرورت صورت گیرد. استثنائاتی مانند دفاع از امنیت ملی یا عمومی یا پیشگیری از تجاوزی مهم به حقوق دیگران می‌تواند توجیه‌کنندهٔ این ضرورت باشد. همچنین، براساس بند ۴ مادهٔ ۲ بخش ۴۳ و مادهٔ ۱ بخش ۴۴ این قانون، انتقال غیرمجاز داده‌های شـــخصی تخلفی اداری محسوب می‌شود که اگر کسی آن را عمداً به‌منظور تغییر میزان پرداخت یا با قصد کسب منفعت مالی برای خود یا دیگری یا با هدف آسیب زدن به شخص دیگر انجام دهد، جرمی کیفری با مجازات حبس حداکثر تا دو سال یا جزای نقدی مرتکب شده است (ناطور و آقابابایی، ۱۳۹۵: ۹).

– **فرانسه:** مادهٔ ۹۲ قانون آیین دادرسی کیفری فرانسه در خصوص بازرسی‌های مرتبط با وسایل مخابراتی بیان می‌کند که بازپرس می‌تواند در هر محلی برای انجام بررسی‌های مفید اقدام به بازپرســـی حضور یابد. او موضوع را به دادســـتان شهرستان که اختیار همراهی وی را دارد، اطلاع می‌دهد. بازپرس همواره به‌وسیلهٔ مدیر دفتر مساعدت می‌شود. او صورتجلسه‌ای از اقدامات خود را تهیه می‌کند (تدین، ۱۳۹۱: ۱۰۸). مرجع شناسایی و تحصیل ادله، بازپرس اســـت که افسران پلیس قضایی زیردســـت وی انجام‌وظیفه می‌کنند. به بازپرس و به‌تبع آن افســـران پلیس قضایی در حقوق فرانســـه اجازه داده شده که در هر مکانی که می‌توان اشیا یا

داده‌های حاوی اطلاعات رایانه‌ای که کشف آن‌ها برای ظهور حقیقت لازم است را پیدا کرد، بازرسی‌ها برای شناسایی داده‌ها می‌تواند صورت گیرد (مادۀ ۹۴ ق.آ.د.ک). همچنین، مادۀ ۹۷ همین قانون بیان می‌دارد: «هنگامی‌که در جریان تحقیقات، جستجوی اسناد یا داده‌های حاوی اطلاعات رایانه‌ای با توجه به ضرورت‌های تحقیق ... بازپرس یا افسر پلیس قضایی مأمور از طرف وی، حق شناسایی و بررسی آن‌ها، پیش از اقدام به توقیف و ضبط آن‌ها را دارد».

دقت در مطالب این قسمت نشان می‌دهد که علاوه بر تأکید دستورالعمل‌های اتحادیۀ اروپا برای استفاده از کنترل و نظارت ارتباطات الکترونیکی برای جرم‌یابی جرائم، مقررات داخلی کشورهای مختلف در نظام حقوقی متفاوت نیز این مجوز را برای مقامات پلیسی و قضایی پیش‌بینی کرده است تا با بهره‌گیری از کنترل ارتباطات الکترونیکی خصوصاً شنود نسبت به جرم‌یابی اقدام کنند.

کنترل ارتباطات الکترونیک در سیاست تقنینی امریکا

در آمریکا براساس متمم چهارم قانون اساسی که در ۱۵ دسامبر ۱۷۹۱ میلادی به تصویب رسیده است، تجسس و دستگیری غیرمنطقی، ممنوع و الزاماتی برای حکم تجسس بر مبنای تشخیص قاضی بی‌طرف براساس علت احتمالی تعیین می‌شود. در آمریکا شنود مخابراتی همه‌جانبه بر ارتباطات مخابراتی هدف موردنظر تمرکز دارد (علیدوست، ۱۳۹۱: ۶۲). بنابراین، در قانون اساسی امریکا شنود و تجسس منع شده است و تجویز آن بسته به نظر قانون و حکم مقام قضایی دانسته شده است.

در امریکا، رهگیری ارتباطات الکترونیک تاریخچه‌ای طولانی‌تر از ایران دارد، به‌طوری که مؤسسه‌های مجری قانون از ابتدای اختراع تلگراف در ۱۸۴۴ و تلفن در اوایل دهۀ ۱۸۹۰ به کنترل آن‌ها می‌پرداختند، اما در آن سال‌ها کنترل این خطوط بدون هیچ‌گونه محدودیتی توسط دستگاه‌های پلیسی و امنیتی صورت می‌گرفت تا اینکه از سال ۱۸۶۲ قوانین فدرال به‌صورت محدود و محتاط شروع به ممنوع کردن اعمال کنترل نامعقول بر ارتباطات افراد کردند. (ساعد و همکاران، ۱۳۹۸: ۴۲). پس از ماجرای رسوایی واترگیت و متعاقب تحقیقات به عمل آمده توسط کمیتۀ کلیسا و استحصال سوءاستفاده‌های به عمل آمده در زمینۀ

جاسوسی داخلی توسط ناسا، اف.بی.ای و سی.آی.ای، قانون نظارت بر فعالیت‌های جاسوسی[1] مصوب ۱۹۷۸ با نام اختصاری «فیسا» به تصویب رسید. قانون مذکور، ناظر بر نحوهٔ شنود و رهگیری ارتباطات، توسط سازمان‌های ضدجاسوسی امریکا، به‌منظور جمع‌آوری اطلاعات و مبارزه با جاسوسی خارجی است. فیسا اصلاحیه‌ای به بخش سوم قانون جامع کنترل بزهکاری و خیابان‌های امن ۹۶۸[2] بود که در مواردی قانون شنود[3] خوانده می‌شد. کنترل ارتباطات مخابراتی و الکترونیکی فوق، بدون هیچ ضمانت اجرایی مجاز دانسته و حتی برای شنود مکالمات خصوصی شهروندان، بدون رضایت آن‌ها نیز مورد استفاده قرار گرفته و غالباً به‌عنوان شواهد و مدارک در دادگاه‌ها مورد استفاده واقع شده بود (محسنی، ۱۳۹۱: ۱۸۷). بنابراین، برای حمایت از تمامیت و امانت دادگاه و تضمین عدم نقض حریم خصوصی شهروندان، فیسا چارچوبی قانونی برای استفاده از کنترل ارتباطات مخابراتی و الکترونیکی و رهگیری ارتباطات پیش‌بینی کرد. براساس آن، برای انجام چنین اقداماتی حکم دادگاه، مبنی بر اجازهٔ این کار را لازم دانسته و مجازاتی از قبیل حبس و جزای نقدی برای انجام این اقدامات بدون مجوز دادگاه، معین کرده بود. همان‌گونه که مشاهده می‌شود قانون فیسا در رویکردی جانبدارانه از رعایت حریم خصوصی حتی در صورتی که کنترل بدون رضایت صاحبان صوت صورت گرفته باشد، علاوه بر بی‌اثر کردن امارهٔ تحصیل شده در این خصوص، ضمانت اجرای مناسبی برای نقض حریم خصوص بدون مجوز به‌وسیلهٔ کنترل ارتباطات در نظر می‌گیرد. البته بعد از تصویب قانون میهن‌پرستی، اصلاحات عدیده‌ای به قانون فیسا وارد آمد که قانون فوق را در برخورد با موارد نقض حریم خصوصی از طریق کنترل ارتباطات مخابراتی و الکترونیکی خلع سلاح کرد.

قانون حریم خصوصی[4] ۱۹۷۴ که از حریم خصوصی مقامات و نهادهای عمومی حمایت می‌کند، قانون حریم خصوصی ارتباطات الکترونیکی[5] ۱۹۸۶ که به جرم‌انگاری شنود تلفنی

1- Sunset Provision
2- Omnibus Crime Control and Safe Streets Act of 1968
3- Wiretap Statute
4- The 1974 Privacy Act
5- The 1986 Electronic Communication Privacy Act (ECPA)

غیرمجـــاز می‌پردازد، قانون حمایـــت از حریم خصوصی راننـــدگان [1]۱۹۹۴ که در خصوص خریدوفروش وســـایل نقلیهٔ موتوری مواردی چون شـــماره تلفن، آدرس و اطلاعات پزشکی و شـــخصی را جزء حریم خصوصی دانســـته و نقض آن را مستوجب مجازات می‌داند و قانون حمایـــت از حریم خصوصی اطفال در ارتباطـــات اینترنتی [2]۲۰۰۰ که رضایت والدین اطفال زیر ۱۳ ســـال را در خصوص دســـتیابی به اطلاعات ناظر بر ارتباطات اینترنتی این اشـــخاص لازم می‌داند، همه مقررات فدرال هســـتند که در مقام حمایت از حریم خصوصی به تصویب رســـیده‌اند. علاوه بر قوانین فدرال مذکور در بالا، مقرره‌های متعدد دیگری در ســـطح ایالات در خصوص حمایت از حریم خصوصی وجود دارد که از ایالتی به ایالت دیگر متفاوت و حتی برخی اوقات متعارض است (شوارتز و سولوو[3]، ۲۰۱۲: ۳). البته لازم به ذکر است، این مقررات به موجب «توافقنامهٔ بندر امن» بین اتحادیهٔ اروپا و ایالات متحده در ســـال ۱۹۹۸ و ســـپس حادثهٔ ۱۱ سپتامبر و تصویب قانون میهن‌پرستی در سال ۲۰۰۲ (داولینق، ۲۰۱۲: ۱۸-۱۱) تحدید شده است؛ از جمله اینکه نقض حریم خصوصی در مقتضیات و مسائل امنیتی کشوری و مداخلات مقامات اجرایی درم واردی جایز شمرده می‌شود. در بخش ۱۸ قانون میهن‌پرستی آمده که رئیس‌جمهور برای حفاظت از ایالات متحدهٔ آمریکا، اقدامات لازم را انجام داده و برای ارتکاب اعمالی چون مداخله در حریم خصوصی افراد و شنود مکالمات تلفنی نیازی به مجوز دادگاه ندارد (کونانی و دیگران، ۱۳۹۱: ۴۱). قانون‌گذار آمریکا در دههٔ پیش در شرایطی این رویکرد را اتخاذ کرده که فناوری روزبه‌روز در حال توسعه است و لوازم نقض حریم خصوصی هرچه می‌گذرد، تسهیل می‌شود (سوتو[4]، ۲۰۱۲: ۶).

کنترل ارتباطات الکترونیک در سیاست تقنینی ایران

در ایـــران، موضـــوع کنترل ارتباطات الکترونیک مجاز به‌طور پراکنده در برخی قوانین و در محدوده‌های خاص پیش‌بینی شده و بر لزوم کنترل قانونی نیز توجه‌هایی صورت گرفته است،

1- The 1994 Driver s Privacy Protection Act
2- The 2000 Children_ s Online Privacy Protection
3- Schwartz and Solove
4- Sotto

اما در بسیاری موارد نیز خلأ قانونی وجود دارد. از مهم‌ترین آن‌ها می‌توان به قانون تجارت الکترونیکی، قانون نحوهٔ مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیرمجاز می‌کنند و قانون جرائم رایانه‌ای اشاره کرد. در قانون جرائم رایانه‌ای که مهم‌ترین قانون داخلی در این زمینه است، آمده: «شنود محتوایی در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای مطابق مقررات راجع به شنود مکالمات تلفنی خواهد بود». تبصرهٔ این ماده هم عنوان می‌کند که دسترسی به محتوای غیرعمومی ذخیره‌شده نظیر پست الکترونیک و پیامک در حکم شنود و مستلزم رعایت مقررات مربوطه است. در مادهٔ ۳۴ قانون مذکور نیز در رابطه با حفظ داده‌های رایانه‌ای ذخیره شده که برای تحقیق یا دادرسی لازم باشد، تأکید شده است که مقام قضایی می‌تواند دستور حفاظت از آن‌ها را برای اشخاصی که به نحوی تحت کنترل قرار دارند، صادر کند. در شرایط فوری نظیر آسیب دیدن یا تغییر یا از بین رفتن داده‌ها، ضابطان قضایی می‌توانند رأساً دستور حفاظت را صادر کنند و ظرف مدت ۲۴ ساعت نیز مراتب را به مقام قضایی اطلاع دهند. در مادهٔ ۳۶ همین قانون، تفتیش در سامانهٔ رایانه‌ای و مخابراتی ممنوع شده است؛ مگر به‌موجب دستور قضایی و در صورتی که ظن قوی به کشف جرم یا شناسایی متهم یا ادلهٔ جرم وجود داشته باشد.

در قانون آیین دادرسی کیفری نیز به ابعاد قانونی کنترل ارتباطات الکترونیک خصوصاً کنترل تلفن اشاره شده است. براساس مادهٔ ۱۵۰، کنترل ارتباطات مخابراتی افراد ممنوع است؛ مگر در مواردی که به امنیت داخلی و خارجی کشور مربوط باشد یا برای کشف جرائم موضوع بندهای (الف)، (ب)، (پ) و (ت) مادهٔ ۳۰۲ ق.آ.د.ک لازم تشخیص داده شود. در این صورت، با موافقت رئیس کل دادگستری استان و با تعیین مدت و تعداد کنترل اقدام می‌شود. کنترل مکالمات تلفنی اشخاص و مقام‌ها، موضوع مادهٔ ۳۰۷ ق.آ.د.ک منوط به تأیید رئیس قوهٔ قضائیه است و این اختیار قابل تفویض به سایرین نیست. شرایط و کیفیات کنترل ارتباطات مخابراتی به‌موجب مصوبهٔ شورای عالی امنیت ملی تعیین شده و کنترل ارتباطات مخابراتی محکومان نیز به تشخیص دادگاه نخستین مجری رأی یا قاضی اجرای احکام آن طبق تبصرهٔ ۲ مادهٔ مزبور است.

ذکر عبارت «...؛ مگر در مواردی که به امنیت داخلی و خارجی کشور مربوط باشد...» نشان

می‌دهد که قانون‌گذار برای پی‌جوئی قضایی و پلیسی جرائم علیه امنیت داخلی و خارجی، استفاده از کنترل ارتباطات الکترونیک مثل شنود، استخراج متن پیامک و رایانامه را مجاز شمرده است. جرائم علیه امنیت داخلی و خارجی در فصل اول کتاب پنجم قانون مجازات اسلامی (تعزیرات و مجازات‌های بازدارنده) برابر مواد ۴۹۸ الی ۵۱۲ جرم‌انگاری شده است.

نتیجه‌گیری

با دقت در مباحث مطروحه در پژوهش موصوف نمایان می‌شود که اصل و مبنای کنترل ارتباطات الکترونیک چه در حقوق ایران و چه در نظام حقوقی امریکا و کشورهای اروپایی، عدم کنترل ارتباطات الکترونیک در حوزهٔ حریم خصوصی است. البته ارتباطات الکترونیک به‌طور رسمی در بسیاری از کشورها، در جهت حفظ حریم خصوصی افراد بشدت کنترل می‌شود. در این کنترل‌ها که باید مبتنی بر رهگیری قانونی یعنی با مجوز مقام قضایی صالح آن‌هم با وجود شواهد و قرائن مجرمانه و توسط نهادهای مجاز باشد، احصای موارد مجاز و غیرمجاز کنترل‌ها سهم بسزایی در حفظ حریم خصوصی افراد ایفا خواهد کرد.

در چارچوب اتحادیهٔ اروپا، تصویب دستورالعمل مارس ۲۰۰۶ راجع به «نگهداری داده‌های شخصی تولید یا پردازش‌شده در چارچوب تأمین خدمات ارتباطات الکترونیکی قابل‌دسترسی برای عموم یا شبکه‌های عمومی ارتباطی و اصلاح دستورالعمل ۲۰۰۲ اتحادیهٔ اروپا»، خبر از نسل جدید قواعد مرتبط با داده‌های شخصی می‌دهد. برخلاف قوانین قبلی که بر حمایت از حریم ارتباطات الکترونیک معطوف است، هدف از تدوین دستورالعمل‌های معنونه، تأمین امنیت ملی، آرامش و نظم عمومی کشورهای عضو و پیشگیری از اعمال مجرمانه است؛ به طوری که برابر بند (۱) مادهٔ ۱۳ دستورالعمل «حمایت از اشخاص حقیقی در مقابل پردازش داده‌های شخصی و گردش آزاد داده‌ها»، کشورهای عضو اتحادیهٔ اروپا می‌توانند مقرراتی مبنی بر محدود کردن تکالیف و حقوق پیش‌بینی شده در مادهٔ (۱-۶)، مادهٔ (۱۰) و (۱-۱۱) و مواد ۱۲ و ۲۱ که مبنای حمایت از حریم ارتباطات الکترونیک است، وضع کنند؛ به‌شرط اینکه این محدودیت‌ها برای ملاحظات زیر ضرورت داشته باشد: امنیت کشور، دفاع ملی، امنیت عمومی، پیشگیری، جستجو، کشف و تعقیب اعمال مجرمانه یا تخلفات انتظامی دربارهٔ حرفه‌های تابع مقررات خاص.

در خصوص قوانین و مقررات ملی کشورهای اروپایی نیز بایستی گفت که در کشور آلمان در جهت دفاع از امنیت ملی یا عمومی یا پیشگیری از تجاوز مهم به حقوق دیگران مجوز لازم برای پایش و کنترل ارتباطات الکترونیک به مسئولان امر ارائه شده است. در کشور فرانسه به بازپرس و به تبع آن افسران پلیس قضایی در حقوق فرانسه اجازه داده شده که در هر مکانی که می‌توان اشیا یا داده‌های حاوی اطلاعات رایانه‌ای که کشف آن‌ها برای ظهور حقیقت لازم است را پیدا کرد، بازرسی‌ها برای شناسایی داده‌ها می‌تواند صورت گیرد. در سوئد، نهادهایی که اجرای قوانین شنود را به‌منظور اطلاع به‌هنگام از فعالیت‌های مظنون تروریستی و بزهکاری‌های کلان و پیگرد آن‌ها عهدهدار هستند، باید پیش از آغاز عملیات تجسسی از یک دادگاه ویژه، مجوز بگیرند.

در آمریکا براساس متمم چهارم قانون اساسی که در ۱۵ دسامبر ۱۷۹۱ میلادی به تصویب رسیده است، تجسس و دستگیری غیرمنطقی، ممنوع و الزاماتی برای حکم تجسس بر مبنای تشخیص قاضی بی‌طرف براساس علت احتمالی تعیین می‌شود. در آمریکا شنود مخابراتی همه‌جانبه بر ارتباطات مخابراتی هدف موردنظر تمرکز دارد.

مروری بر قوانین موجود در خصوص ارتباطات الکترونیک در ایران به‌صراحت آشکار می‌سازد که شنود مکالمات تلفنی، پیامک‌ها و پست الکترونیک نیازمند دستور قضایی است و در شرایط فوری نیز ضابطان قضایی ملزم به رعایت قانون شده‌اند. علاوه بر این، تفتیش در پیامک‌ها و پست الکترونیک در شرایط عادی ممنوع اعلام شده است. در ق.آ.د.ک ۱۳۹۲ نیز به ابعاد قانونی کنترل ارتباطات الکترونیک خصوصاً کنترل تلفن اشاره شده است.

منابع

منابع فارسی

- احمدی، احمد (۱۳۹۷). نقض حریم خصوصی؛ چالشی پیشروی پیشگیری وضعی از وقوع جرم. *فصلنامهٔ مطالعات پیشگیری از جرم*. دورهٔ ۱۳۹۷، شمارهٔ ۴۶، صص ۱۱۰-۷۷.

- انصاری، باقر (۱۳۹۳). حریم خصوصی و حمایت از آن در حقوق اسلام، تطبیقی و ایران. *مطالعات حقوق خصوصی*. دورهٔ ۵، شمارهٔ ۶۶، صص ۵۴-۱.

- آیتی، محسن و محمدزاده، علیرضا (۱۳۹۴). امنیت انسانی و کاربرد فناوری‌های نوین اطلاعاتی و ارتباطاتی. *مجموعه مقالات همایش بین‌المللی امنیت انسانی در غرب آسیا*.

- تدین، عباس (۱۳۹۱). *قانون آیین دادرسی کیفری فرانسه*. معاونت حقوقی قوهٔ قضاییه. تهران: انتشارات خرسندی. چاپ اول.

- زرکلام، ستار (۱۳۸۶). حریم خصوصی ارتباطات اینترنتی. *پژوهشنامهٔ حقوق اسلامی*. دورهٔ ۸، شمارهٔ ۲۵، صص ۱۹۶-۱۷۳.

- ساعد، محمدجعفر؛ عبدلی مرویلی و مهدی قاسمی، ناصر (۱۳۹۸). سیاست تقنینی ایران و امریکا در پایش سمعی و تأثیر تفکر امنیت‌گرایی بر آن. *فصلنامهٔ آفاق امنیت*. شمارهٔ ۴۴، صص ۶۵-۳۵.

- ستوده گندشمین، مجتبی و عالیزاده، موسی (۱۳۹۴). *مقدمه‌ای بر اطلاعات جنایی*. تهران: نشر کارآگاه. چاپ اول.

- ستوده گندشمین، مجتبی و عتباتی، ناصر (۱۳۹۸). شرایط و ضوابط کنترل ارتباطات الکترونیک در کشف جرائم در نظام قضایی ایران. *کارآگاه*. دورهٔ ۱۲، شمارهٔ ۴۸، صص ۱۲۲-۱۰۲.

- ستوده گندشمین، مجتبی و نظری، غلامحسین (۱۳۹۳). تعقیب و کشف جرائم سازمان‌یافتهٔ فراملی با رویکرد اطلاعات جنایی در کنوانسیون‌های بین‌المللی. *کارآگاه*. شمارهٔ ۲۹، دورهٔ دوم.

- طالبیان، حسین (۱۳۹۱). تبیین فرآیند تشکیل ابراطلاعاتی پلیس در کشف جرم. *کارآگاه*. دورهٔ ۲، شمارهٔ ۱۹، صص ۱۵۷-۱۲۶.

- عتباتی، ناصر (۱۳۹۷). *شرایط و ابعاد حاکم بر کنترل ارتباطات الکترونیکی با تأکید بر*

رویهٔ قضایی. رسالهٔ دکتر. پژوهشگاه قوهٔ قضاییه.

- علیدوست، یدالله (۱۳۹۱). قوهٔ قضاییه در امریکا. *نشریهٔ قضاوت*. شمارهٔ ۱۲، صص ۶۳-۶۱.

- فروغی، فضل‌الله؛ برجی، محمدناصر و مصلحی، جواد (۱۳۹۳). مبانی ممنوعیت نقض حریم خصوصی در حقوق ایران و امریکا. *مجلهٔ مطالعات حقوقی*. دورهٔ ۶، شمارهٔ ۳، صص ۱۷۲-۱۳۷.

- قاجار، سیامک (۱۳۸۹). ابعاد حقوقی کاربرد کامپیوتر (حریم خصوصی، حمایت از داده). *خبرنامهٔ انفورماتیک*. سال ۱۵، شمارهٔ ۱۶۷، صص ۱۸۱-۱۷۴.

-کونانی، سلمان؛ می‌رکمالی، علی‌رضا و امیرحشمتی، دیبا (۱۳۹۱). برهم‌کنش موازین حقوق بشر و سیاست جنایی امنیت‌گرا در افق قواعد حقوق بین‌الملل؛ با تأملی بر قانون میهن‌پرستی آمریکا. *فصلنامهٔ مطالعات بین‌المللی پلیس*. شمارهٔ ۱۱، صص ۶۳-۴۱.

- محسنی، فرید (۱۳۹۱). تحولات کیفری در قانون میهن‌پرستی امریکا. *دیدگاه‌های حقوق قضایی*. دورهٔ ۱۷، شمارهٔ ۶۰، صص ۲۱۲-۱۷۹.

- ناطوراحمدی، زهرا و آقابابایی، حسین (۱۳۹۵). جرائم علیه حریم خصوصی داده‌ها در فضای سایبری ایران و آلمان. رسانه و فرهنگ. سال ۶، شمارهٔ اول، صص ۲۳-۱.

- نمکدوست تهرانی، حسن (۱۳۹۵). اخلاق حرفه‌ای، حریم خصوصی و حق دسترسی به اطلاعات. مجلهٔ رسانه. شمارهٔ ۶۶، صص ۲۳۲-۱۹۷.

- نوبهار، رحیم (۱۳۹۷). *حمایت کیفری از حوزه‌های عمومی و خصوصی*. تهران: انتشارات جنگل. چاپ سوم.

منابع انگلیسی

- Acker, James and Brody, David (2014). Criminal procedure. Jones and Bartlett publishers.2nd edition.

- Bainbridge David (2010). Introduction to computer law.Longman.Fourth Edition

- Schwartz, Paul M.and Solove, Daniel J. (2012). Reworking Information Privacy Law, The American Law Institute.

- Sotto, Lisa (2012). Privacy Trends 2012, The Case For Growin Accountability, Ernst & Young.