دوره ۳، شماره ۲، پاییز و زمستان ۱۳۹۵(پیاپی ۷)
صفحات ۱۹۵ تا ۲۱۷

مبانی جرم‌انگاری ارسال پیام‌های الکترونیکی ناخواسته

بتول پاکزاد[۱]*، محمد حسین آزادی خواه[۲]

۱. استادیار دانشگاه آزاد اسلامی واحد تهران شمال

۲. کارشناس ارشد حقوق جزا و جرم شناسی، دانشگاه آزاد اسلامی تهران مرکز

(تاریخ دریافت: ۱۳۹۵/۳/۱۷ - تاریخ تصویب: ۱۳۹۵/۹/۲)

چکیده

پیام‌های الکترونیکی ناخواسته، آن دسته پیام‌هایی هستند که بدون رضایت شخص دریافت کننده برای وی ارسال می‌شود و حقوق وی را در دریافت پیام نادیده می‌گیرد. همچنین، می‌تواند بستر فعالیت‌های ناسالم و مجرمانه را در فضای سایبر فراهم نماید. مشکلات ایجاد شده به واسطه ارسال پیام‌های الکترونیکی ناخواسته از یک سو، و مؤثر نبودن روش‌های فنی و سیاست‌های خود تنظیمی توسط تأمین‌کنندگان فضای سایبر از سوی دیگر، قانونگذار کشورها را مجبور به اتخاذ تدابیر و اقدامات کنشی و واکنشی در رویارویی با این پیام‌ها کرده است. در این رابطه، بسیاری از کشورها با وضع قوانین خاص ضمن جرم‌انگاری ارسال پیام های ناخواسته، الزاماتی را برای تبادل پیام در فضای سایبر در نظر گرفته‌اند. در جرم‌انگاری این پدیده با توجه به تبعات ناشی از ارسال این پیام‌ها، به نظر می‌رسد مواردی همچون ضرر، حریم خصوصی و حقوق مصرف کننده به عنوان مبانی جرم‌انگاری این پدیده مطرح هستند. این تحقیق درصدد است تا ضمن مطالعه تطبیقی و با تأکید بر تدابیر کنشی، مبانی جرم‌انگاری ارسال پیام‌های ناخواسته را ارزیابی کند.

کلید واژگان

پیام‌های ناخواسته (اِسپَم)، فضای مجازی، جرم‌انگاری، ضرر، حریم خصوصی، حقوق مصرف کننده.

* d.b.pakzad@gmail.com

مقدمه

رشد و توسعه فناوری منجر به گسترش ارتباط سریع میان افراد از طریق ارسال پیام شده است. پیام‌هایی که ممکن است با انگیزه‌های مختلف تجاری و غیرتجاری از طریق نامه‌های الکترونیکی، تلفن همراه و دیگر وسایل ارتباطی میان افراد رد و بدل گردد. بی شک حقوق افراد اقتضاء می کند که در دریافت این پیام ها مختار باشند و تمایل خویش را نسبت به دریافت آنها اعلام نمایند. با این وجود، نبود قواعد مناسب در زمینه ارسال و دریافت پیام باعث بروز مشکلاتی برای افراد شده است، از آن جمله، می‌توان به وجود پیام‌های ناخواسته اشاره کرد که از یک سو تلف کردن زمان افراد برای مرور آنها، مصرف بالای انرژی، شلوغی خطوط ارتباطی و نامه های آلوده را به همراه دارد و از سوی دیگر زمینه بروز بسیاری از جرایم از قبیل کلاهبرداری، سرقت، سوء استفاده‌های جنسی و غیراخلاقی و ... را فراهم می‌سازد. علاوه بر این، حقوق افراد را در دریافت پیام و پذیرش آن نادیده می‌گیرد. از این رو، مدیریت پیام و جلوگیری از ارسال پیام‌های ناخواسته می‌تواند در کاهش جرایم مرتبط با آن مؤثر باشد. به همین منظور در بسیاری از کشورها رویارویی با این پیام‌ها و جرم‌انگاری آن مورد توجه قرارگرفته است؛ اگرچه باید گفت اختلاف نظرهایی دراین رابطه وجود دارد.

در حال حاضر، با وجود استفاده از ابزارهای فنی، بکارگیری روش‌های غیر حقوقی و اعمال تدابیر خود تنظیمی، آثار ناشی از پیام های ناخواسته همچنان ادامه دارد. بنابراین، لزوم وضع قوانین، به‌ویژه تدابیر کیفری، در مقابله با این پدیده احساس می‌شود، اما رویارویی در عرصه کیفری نیازمند مجموعه‌ای از مبانی حقوقی است تا بتوان براساس آن به ضرورت جرم‌انگاری آن پدیده پی‌برد. تبیین مبانی متناسب با هر کشوری متفاوت است. به عبارت دیگر، آثار یک پدیده در کشورهای مختلف یکسان نیست و هر گز نمی توان مبانی مورد نظر یک کشور را به کشوری دیگر تسری داد. به تناسب فرهنگ، اقتصاد، سیاست و ساختارهای حقوقی و اجتماعی، مبانی نیز متفاوت است و به تبعیت از آن، نوع جرم انگاری و تعیین مجازات هم از کشوری به کشور دیگر فرق دارد. بی‌شک اقدام به جرم‌انگاری و تعیین مجازات بدون توجه به ساختارهای حقوقی و اجتماعی و وجدان عمومی هر جامعه و با تأسی صرف از مبانی دیگر کشورها، نوعی عدم تمایل جامعه در اجرای آن قانون و مسکوت ماندن و در نتیجه بی‌کیفری را در پی خواهد داشت.

به لحاظ پیشینه تحقیق با توجه به عدم وجود قوانین و مقررات جامع در رابطه با ارسال پیام، پژوهش در این زمینه در داخل کشور بسیار اندک است و صرفاً محدود به دو مقاله «مقابله کیفری با پیام‌های ناخواستهٔ الکترونیکی (رویکرد جهانی، بایسته سنجی ملی)» (فضلی و باطنی، ۱۳۸۲) و «حمایت کیفری از حقوق مصرف کننده در قانون تجارت الکترونیکی» (زندی، ۱۳۹۱) و صفحاتی از دو کتاب «حقوق کیفری فناوری اطلاعات» (عالی‌پور، ۱۳۸۹) و «جرایم تجارت الکترونیکی» (جاویدنیا، ۱۳۹۲) می‌شود. در تمامی تحقیقات انجام شده بدون آنکه اشاره ای به ضرورت و مبانی جرم‌انگاری شده باشد، صرفاً موضوعاتی همچون رویکردهای جرم‌انگاری پیام های ناخواسته، الزامات موجود در حوزه تبلیغات

تجاری و ارتباط این پیام‌ها با جرایم سایبری مورد بررسی قرار گرفته است. به عبارت دیگر، آن چه این تحقیق را از سایر تحقیقات انجام شده در این زمینه متمایز می‌نماید آن است که با توجه به تدابیر کنشی و واکنشی اتخاذ شده توسط کشورها به بررسی مبانی جرم‌انگاری این پدیده پرداخته و ضمن ارزیابی آن در سیاست جنایی تقنینی ایران به دنبال پاسخگویی به این سؤالات است که آیا مبانی جرم‌انگاری در زمینه تبلیغات تجاری و مدیریت ارسال پیام در کشور وجود دارد؟ آیا صرف اقدامات کنشی و مدنی از سوی مقنن می تواند در مقابله با چنین پدیده‌ای مؤثر باشد؟ در این نوشتار با نگاه تطبیقی ابتدا به صورت اجمالی به ارائه تعریف از پیام‌های ناخواسته و بیان شیوه‌های رویارویی با ارسال این پیام‌ها پرداخته خواهد شد و سپس با توجه به محدودیت‌هایی که برای مقابله با این پدیده در روش‌های فنی و الزامات کنشی وجود دارد، ضمن تأکید بر جرم‌انگاری ارسال پیام‌های ناخواسته، مبانی رویارویی کیفری آن بیان می‌شود.

۱. تعریف پیام‌های الکترونیکی ناخواسته

پیام در مفهوم پیام‌های ناخواسته، بسته‌ای شامل هرگونه محتوای متنی، تصویری و صوتی می‌شود. بنابراین، هر پیامی که بتواند در بستر فضای سایبر تبادل شود می تواند با لحاظ سایر شرایط در مفهوم پیام های الکترونیکی ناخواسته گنجانده شود. بند یک از بخش اول «قانون ضد پیام‌های ناخواسته» کانادا هرگونه محتوای ارسال شده متنی، صوتی و تصویری را پیام می‌داند. (Canada'sAnti-Spam Law,2010) درحقوق ایران اگرچه خود پیام به عنوان بسته‌ای از داده (لایحه پیام دیجیتال) تعریف نشده است، ولی محتوا و اطلاعات پیامی تحت عنوان داده پیام (Data Message) مورد تعریف قانونگذار قرار گرفته است. در این رابطه در «قانون تجارت الکترونیکی» داده پیام هر نمادی از واقعه، اطلاعات یا مفهوم تعریف شده است (ماده ۲ قانون تجارت الکترونیکی مصوب ۱۳۸۲). از نگاه قانونی، رویارویی مقنن در مورد پیام‌های الکترونیکی ناخواسته از یک کشور به کشور دیگر متفاوت است. بیشتر کشورها با توجه به جنبه های تجاری پیام، تبلیغات تجاری پیام های ناخواسته را در قوانین خود مد نظر قرارداده‌اند؛ اما این بدین معنا نیست که تعریف قانونی این پدیده باید حول محور تبلیغات تجاری باشد، بلکه می تواند جنبه های غیرتجاری را در برگیرد. بسیاری از دریافت کنندگان، پیام هایی با ماهیت سیاسی، مذهبی و یا تبلیغات نژادپرستانه مشاهده می‌کنند. این پیام‌ها اگرچه تجاری نیستند، ولی ناخواسته می‌باشند. همچنین وجود پیام‌های بداندیشانه مثل فریب، کلاهبرداری و مسائل غیراخلاقی از یک سو، و تفاوت‌های کیفی میان ارسال کنندگان پیام‌های بداندیشانه و بازاریابان قانونی از سوی دیگر، این مطلب را آشکار می سازد که محدود کردن پیام‌های ناخواسته تنها به بازاریابان، ناعادلانه و نادرست است (Scott, 2004, p10). از این رو، پیام‌های الکترونیکی ناخواسته یا اسپم (Spam:Unsolicited Emails) را باید آن دسته پیام‌هایی

دانست که در سطح گسترده، به صورت ناخواسته و به طریق غیرقانونی برای دریافت کننده پیام، از طریق سیستم‌های پیام‌رسان الکترونیکی ارسال می‌گردد.

۲. شیوه‌های رویارویی با پیام‌های الکترونیکی ناخواسته

ارسال پیام‌های ناخواسته اگرچه از یک سو مزیت‌های فراوانی از قبیل کسب درآمد و بالارفتن سود از طریق تبلیغات تجاری و کسب میلیون‌ها مشتری بالقوه را برای ارسال‌کنندگان خود به همراه داشته است؛ اما از سوی دیگر عاملی بالقوه برای هرگونه سوء استفاده در روند تبادل پیام محسوب می‌شود. قابلیت دوگانه در این ابزار ارتباطی سبب می‌شود تا فضا برای سوء استفاده از آن فراهم گردد و از یک ابزار تبلیغی ساده و بی‌ضرر به ابزاری مخرب برای کاربران تبدیل شود. استفادهٔ ناروا از ابزار پیامی نه تنها پیامدها و مشکلات مختلفی را برای کاربران به دنبال دارد، بلکه سبب پایین آمدن کارایی مثبت ارسال پیام می‌شود، (Hallace Kikuchi, 2004, pp 16-17) به‌گونه‌ای که دریافت کنندگان را مجبور به واکنش‌های متفاوت نسبت به آن می‌کند.

۱.۲. روش فنی

با توجه به آنکه پیام ناخواسته مولود فناوری‌های نوین است، مقابله با آن نیز از طریق بکارگیری فناوری انجام می‌شود. در این روش، اتکاء اصلی بر فناوری‌های علمی و استفاده نرم‌افزاری است. به عبارت دیگر، با استفاده از اقدامات غیرحقوقی آثار منفی ناشی از پیام های ناخواسته در عرصه ارتباطی کاهش می‌یابد و به حداقل می‌رسد. رویارویی با پدیده پیام ناخواسته در این روش به صورت فناوری در مقابل فناوری است. نگاه حقوقی در این روش وجود ندارد و متخصصان عرصه ارتباطات و فناوری با بکارگیری ابزارهای علمی تلاش می کنند تا در مقابل این پدیده راهکارهای علمی و تخصصی ارائه دهند. در مقابل، ارسال کنندگان پیام ناخواسته نیز به مرور زمان از شیوه های جدیدتری برای ارسال پیام‌های ناخواسته استفاده می‌کنند و سعی می‌نمایند تا اقدامات پیشگیرانه متخصصان علمی برای عدم ارسال این پیام‌ها را خنثی نمایند و یا آن را کم اثر کنند. اگرچه باید گفت تا زمانی که ارسال‌کنندگان پیام ناخواسته از ارسال آن نفعی هر چند ناچیز می‌برند، مناقشه میان ارسال‌کنندگان و متخصصان ضد پیام‌های ناخواسته همچنان ادامه دارد.

۲.۲. تدابیر خود تنظیمی

روش دوم مقابله با پیام های ناخواسته، با وضع مجموعه مقررات غیر رسمی و ارائه کدهای رفتاری در فضای سایبر اعمال می‌شود. مقررات خود تنظیمی (Self – Regulation) را باید آن دسته سیاست‌ها و خط مشی‌هایی دانست که توسط بخش خصوصی به شکل سازمانی و در قالب موضوعی خاص جهت تنظیم روابط بکار می رود، اعم از اینکه این خود تنظیمی به بخش خصوصی محول

شده باشد و یا اینکه بخش خصوصی به صورت مستقل اقدام به وضع آن نماید (Ong, 2010, P 240). در این رابطه، تأمین‌کنندگان خدمات با وضع تدابیر خود تنظیمی و اجرای سیاست‌های لازم سعی در کاهش ارسال پیام به صورت ناخواسته دارند. از نگاه تأمین‌کنندگان، ارسال پیام‌های الکترونیکی ناخواسته عاملی زیان‌بار برای ارائه خدمات به مشتریان می باشد و هزینه های ناشی از افزایش ترافیک را به آنها تحمیل می‌نماید.

از نظر نوع تدابیر و اقدامات بکار رفته در رویکرد خود تنظیمی، می‌توان آن را به دو دسته آداب شبکه و خط مشی‌های قابل پذیرش (Acceptable Use Policies) تقسیم نمود. قواعد مربوط به آداب شبکه به اوایل ۱۹۷۰ برمی گردد؛ یعنی زمانی که کاربران فضای سایبر برای استفاده از چنین فضایی قواعدی را به عنوان قرارداد پایه‌ریزی کردند. این قواعد در میان عموم، امروزه آداب شبکه نامیده می شود. آداب شبکه عبارت است از مجموعه رفتارها و روش‌هایی که افراد برای استفاده مناسب از فضای سایبر به عنوان ابزاری ارتباطی رعایت می کنند (Tedre, 2006). در مورد تبادل پیام در فضای سایبر، رعایت حقوق مصرف کننده همچون اخذ رضایت از وی، ممنوعیت انتقال اطلاعات نادرست و گمراه کننده و ارائه مشخصات کامل ارسال کننده به همراه پست الکترونیک معتبر از جمله موارد مربوط به آداب ارسال پیام می‌باشد. آداب شبکه که از آن تحت عنوان کدهای رفتاری نانوشته نیز یاد می شود بر رفتار افراد در فضای سایبر تأثیرگذار است. با این وجود، تأثیرگذاری آن منوط به پذیرش از سوی افراد است؛ زیرا در مورد عدم رعایت این آداب ضمانت اجرای حقوقی وجود ندارد (Lydia Pallas Loren, 1999).

عدم رعایت آداب شبکه در تبادل پیام و فقدان ضمانت‌اجرای لازم در این مورد سبب شد تا بسیاری از تأمین‌کنندگان خدمات برای تنظیم مقررات و جلوگیری از ارسال مکرر پیام‌های ناخواسته، اقدام به وضع سیاست ها و خط مشی هایی برای مشترکان خویش بنمایند. از این رو، ارائه خدمات به مشتریان را منوط به رعایت این خط مشی‌ها از سوی مشترکان نمودند. از جمله این سیاست‌ها می‌توان به ممنوعیت ارسال پیام‌های ناخواسته از دستگاه رایانه‌ای پشتیبانی شده توسط تأمین کننده، ممنوعیت جمع آوری اطلاعات دیگران مثل آدرس رایانامه و دستکاری در اطلاعات سرپیام و استفاده از آدرس اشخاص ثالث برای پنهان ماندن منشاء پیام اشاره کرد. تأمین‌کنندگان خدمات در مقابل تخلف از هریک از سیاست های خویش می توانند بدون اخطار قبلی رابطه خویش را با مشترک قطع کنند (Lottersberger,2003 Pp 30-31).

۳.۲. تدابیر قانونی

در مقابل روش‌های فنی و خود تنظیمی، دیدگاه دیگری وجود دارد که معتقد است ارسال پیام در فضای سایبر باید در چهارچوب قوانین و مقررات خاصی باشد؛ زیرا در غیر این صورت، آثار مخرب این پیام‌ها به افراد و تأمین‌کنندگان خدمات تحمیل می‌شود. این دیدگاه با تکیه بر محدودیت‌های موجود

در روش‌های فنی همچون هزینه‌های پیاده‌سازی نرم‌افزارها، بکارگیری روش‌های جدید در ارسال پیام های ناخواسته جهت دور زدن روش‌های فنی، از بین رفتن ارتباطات مشروع افراد به دلیل درصد خطای ابزار فنی (Sorkin, 2001, p 356) و همچنین مؤثر بودن سیاست‌های خودتنظیمی تأمین‌کنندگان، (Lottersberger,2003, p34) این روش‌ها را برای مقابله با پیام‌های الکترونیکی ناخواسته کافی نمی‌داند و معتقد به نظام‌مند کردن ارسال پیام از طریق قوانین و مقررات قانونی می‌باشد. بر اساس این رویکرد بسیاری از کشورها با توسل به سیاست‌های تقنینی شروع به مقابله با این پیام‌ها نموده‌اند.

با توجه به معضل پیام‌های الکترونیکی ناخواسته در کشورهای مورد مطالعه، گونه‌های مختلفی از قوانین توسط این کشورها جهت مقابله با این پدیده وضع شده است. بررسی قوانین موجود در این کشورها نشان می‌دهد طیف گسترده‌ای از اقدام‌ها و تدابیر کیفری و غیر کیفری، به منظور کنترل این پدیده مجرمانه توسط قانونگذار اتخاذ شده است که در مجموع بیانگر سیاست جنایی تقنینی در خصوص پیام‌های الکترونیکی ناخواسته می‌باشد. مقابله با پیام‌های ناخواسته در کشورهای مورد مطالعه، در قالب یک قانون خاص متمرکز نمی‌باشد و مقابله با آن در طیف گسترده‌ای از قوانین وجود دارد. در امریکا علاوه بر قانون خاص در پیام‌های ناخواسته پست الکترونیک و مقررات کمیسیون تجارت فدرال، قانون دیگری نیز تحت عنوان حمایت از مشترکان تلفن (Telephone Consumer Protection Act Tcpa) وجود دارد که ارتباطات ناخواسته بی‌سیم همچون تلفن همراه را پوشش می‌دهد. همچنین تا قبل از قانون ضد پیام‌های ناخواسته فدرال در مجموعه قوانین کیفری امریکا نیز در باب ۱۸ از فصل ۴۷ تقلب و فعالیت‌های مرتبط با پست الکترونیک مورد جرم‌انگاری قرار گرفته بود. (بخش ۱۰۳۷ از کد کیفری امریکا با تصویب قانون ضد پیام‌های ناخواسته فدرال امریکا به بخش ۷۷۰۳ الحاق شد.)

در کشور کانادا قوانین متعددی همچون مجموعه قوانین کیفری، قانون رقابت، قانون حمایت از مصرف کننده در رایانامه تجاری، کدهای رفتاری و راهنمایی‌های صنعتی و قانون خاص فدرال برای مقابله با پیام های ناخواسته وجود دارد. در ژاپن نیز با توجه به قوانین در دسترس می‌توان به دو قانون ارسال رایانامه معین و قانون انتقال تجاری خاص اشاره کرد، همچنین بخشی از مقابله با این پیام‌ها نیز به صورت شیوه‌های رفتاری و راهنمایی‌های صنعتی می‌باشد (Moustakas, Evangelos, Ranganathan, C, Duquenoy, Penny, 2005).

در ایران در خصوص پیام‌های الکترونیکی ناخواسته هنوز قانون خاصی وجود ندارد و قوانین موجود نیز نشان‌دهنده عدم توجه قانونگذار به این مسأله می‌باشد. همچنین تلاش‌ها برای تدوین یک قانون خاص در این خصوص بی نتیجه بوده و تنها منتج به تهیه چند لایحه از جمله لایحه پیام‌های ناخواسته و لایحه پیام دیجیتال شده است. در این خصوص با توجه به وجود ایرادات بسیار در هر دو لایحه و عدم هماهنگی در تدوین یک قانون جامع، براساس نظر کارگروه فرعی بررسی لایحه پیام دیجیتال، مقرر شده است تا مقابله با این پدیده به صورت چند ماده در قالب لایحه

اصلاحی قانون تجارت الکترونیک به این قانون الحاق گردد. با این وجود، با توجه به قوانین موجود می‌توان به برخی مصادیق مقابله با این پیام‌ها در قوانین ایران اشاره کرد. در خصوص ارسال محتوای مجرمانه می توان به مواد۶۹۷ تا ۷۰۰ قانون تعزیرات سال ۱۳۷۵ و مواد ۱۴ تا ۱۸ قانون جرایم رایانه‌ای اشاره کرد که البته در این رابطه به نظر می‌رسد هدف مقنن، محتوای مجرمانه بوده است و نه ارسال محتوای ناخواسته. ایجاد مزاحمت از طریق ارسال پیام ناخواسته موضوع ماده ۶۴۱ قانون تعزیرات سال ۷۵ نیز می‌تواند به عنوان یکی از مصادیق مقابله با پیام‌های ناخواسته باشد. با وجود مصادیق بیان شده مهم‌ترین مصداق قانونی در مقابله با این پیام‌ها قانون تجارت الکترونیکی مصوب ۱۳۸۲ است. برخلاف دو قانون قبلی، این قانون را باید مهم‌ترین سیاست جنایی تقنینی ایران در مورد پیام‌های الکترونیکی ناخواسته دانست؛ زیرا هر چند ناقص، به بیان کلی قواعد تبلیغ در ارسال پیام تجاری پرداخته است و برای متخلف از مقررات، ضمانت اجرای کیفری در نظر گرفته است. علاوه بر قوانین اشاره شده، در ایران نیز همچون سایر کشورهای مورد بررسی، قواعد و مقررات رفتاری در ارسال پیام وجود دارد. در این خصوص ضوابط و مقررات سازمان تنظیم مقررات برای اپراتورهای تلفن همراه(مصوبات شماره ۱۴۷ و ۱۶۸ کمیسیون تنظیم مقررات ارتباطات در خصوص ارسال پیام از طریق تلفن همراه)، نمونه خوبی از مقررات خود تنظیمی می‌باشد.

۳. جرم‌انگاری ارسال پیام‌های الکترونیکی ناخواسته

امنیت فضای سایبر منوط به جلوگیری از وقوع تهدیدها و جرایم سایبری است و پیام های ناخواسته نیز عاملی مؤثر در ایجاد تهدید و وقوع جرم در چنین فضایی می باشد. بنابراین، می توان نتیجه گرفت که مقابله با پدیده پیام ناخواسته در کنترل جرم و بهبود امنیت در فضای سایبر مؤثر است. به عبارت دیگر، جرم‌انگاری و وضع تدابیر کیفری در پیام ناخواسته می‌تواند از وقوع جرایم دیگر جلوگیری کند. در این رابطه می توان به تأسیس جرم مانع در نظام حقوقی ما اشاره کرد. در مورد جرم‌انگاری پیام‌های ناخواسته نیز می‌توان چنین دیدگاهی را متصور بود، به این معنا که امنیت فضای سایبر ایجاد نمی‌شود مگر اینکه این پیام‌ها به عنوان عاملی سازنده در وقوع و تسهیل جرم مدیریت و کنترل شود. وقوع جرایم سنتی نظیر جعل و کلاهبرداری در فضای سایبر از یک سو، و جرایم جدید همچون جرایم علیه محرمانگی یا صحت و تمامیت داده‌ها و سیستم‌های رایانه‌ای و مخابراتی از سوی دیگر، حقوق کیفری را به سمت مداخله و جرم‌انگاری های جدید در چنین فضایی سوق داده است. تبادل پیام و ارتباطات الکترونیکی نیز از این امر مستثنی نیست. امروزه، رویکرد بین‌المللی در قانونگذاری به سمت اختصاص مواد و مباحث مستقل به مسائل ویژه ارتباطات الکترونیکی است. (حسنی،۱۳۸۵، ص۹۸) و این قبیل مسائل در حوزه حقوق ارتباطات الکترونیکی مورد مطالعه قرار می‌گیرد.

در سال ۲۰۰۲ دستورالعملی در راستای حفظ حریم خصوصی ارتباطات الکترونیکی در اتحادیه اروپا به تصویب رسید که براساس آن مباحثی همچون شنود، داده ترافیک و داده موقعیت و ارتباطات و تماس‌های ناخواسته مورد توجه قرارگرفت. پدیده پیام‌های ناخواسته یکی از مصادیق مورد بحث در حوزه ارتباطات ناخواسته است. چالش‌های بوجود آمده توسط این پدیده نوظهور در زمینه حقوق مصرف کننده، وسایل ارتباطی، تجارت عادلانه، اموال، عفت عمومی، امنیت مجازی و حفاظت از اطلاعات شخصی (xingan, 2006) سبب شد تا بسیاری از کشورهای جهان اقدام به وضع قوانین و ضمانت اجرای‌های حقوقی نمایند که از این میان برخی کشورها مثل امریکا به طور خاص و برخی دیگر نظیر کانادا و ژاپن در قالب قوانین دیگر به لزوم ضمانت‌اجراهای کیفری تأکید داشته‌اند.

۴. مبانی جرم‌انگاری ارسال پیام‌های الکترونیکی ناخواسته

در مورد مبانی جرم انگاری باید دو نکته مهم را مورد توجه قرار داد. نکته اول اهمیت مبانی جرم‌انگاری یک پدیده است، اینکه تا چه میزان مبانی مورد نظر می‌تواند در اقناع مقنن برای جرم‌انگاری آن و تطبیق با وجدان عمومی برای پذیرش آن مؤثر باشد. نکته دوم اینکه مقنن با جرم‌انگاری چه هدفی را دنبال می‌کند؟ آیا عواملی چون حبس‌زدایی، مجازات‌های جایگزین، تورم کیفری و حداقل‌گرایی درضمانت اجراهای حقوق کیفری می‌تواند در این هدف تاثیرگذار باشد و برآن غلبه کند؟

اهمیت مبانی جرم‌انگاری در مورد پیام‌های الکترونیکی ناخواسته متناسب با ساختارهای اجتماعی و حقوقی یک جامعه متفاوت است. جامعه ای که در آن تجارت الکترونیکی رونق بیشتری دارد و بازاریابی در فضای مجازی به صورت گسترده‌ای توسعه یافته است با چالش‌های بیشتری در زمینه بروز تخلفات و جرایم روبرو است. در چنین جامعه ای، مسأله ضرر، هزینه‌های تحمیلی و حقوق مصرف‌کننده بیشتر مدنظر قرار می‌گیرد. در مقابل، جامعه‌ای که در عرصه فضای سایبری فعالیت کمتری دارد با چالش‌های کمتری همچون ضرر، هزینه‌های تحمیلی و نقض حقوق مصرف‌کننده هم روبرو است. برای نمونه، بخش دوم از قانون ضد پیام‌های ناخواسته امریکا در تبیین یافته‌های کنگره، خسارت و هزینه‌های عمده به تأمین‌کنندگان خدمات دسترسی به اینترنت، هزینه‌های تحمیلی به دریافت کنندگان، کاهش کارایی نامه‌های الکترونیکی، محتوای مبتذل و جنسی و اطلاعات فریبنده و گمراه کننده را به عنوان مبانی تعیین‌کننده در جرم‌انگاری چنین پدیده‌ای دانسته است. (15 U.S.C § 7701(a)) یافته‌های کنگره از یک طرف، نشان‌دهنده اهمیت بالای این مبانی در کشوری مثل امریکا می باشد، کشوری که تبلیغات از طریق پست الکترونیکی و بازاریابی اینترنتی مشکلات فراوانی را برای تأمین‌کنندگان خدمات و دریافت کنندگان ایجاد کرده بود و قانونگذار را به این نتیجه رساند که به راه‌حل‌های کیفری توجه ویژه داشته باشد. از طرف دیگر، مشکلات بوجود آمده برای مردم این کشور، وجدان عمومی جامعه را برای پذیرش چنین

مقرراتی آماده کرده است. مسأله قابل طرح این است که آیا تمام این مبانی قابل تسری در سیاست جنایی تقنینی ایران است؟ آیا بروز مشکل و ایجاد خسارت برای تأمین‌کنندگان و دریافت کنندگان به همان شدت کشور امریکا است؟ برای نمونه در زمینه پست الکترونیکی، استفاده کاربران ایرانی با وجود برخی رایانامه‌های ایرانی از حساب‌های غیربومی است و تحمیل هزینه به تأمین‌کنندگان خارجی بی‌معنی است؛ زیرا تأمین کننده، ایرانی نیست. در مقابل، دریافت کنندگان ایرانی از همین حساب‌ها، بسیاری از پیام‌های ناخواسته را دریافت می‌کنند و متحمل خسارات مادی و معنوی می‌شوند. این مسأله نشان دهنده آن است که پیام‌های الکترونیکی ناخواسته یک مشکل بین‌المللی است تا جایی که بسیاری از کشورها در مقابله با این پدیده اقدام به همکاری‌های بین‌المللی کرده‌اند. برای نمونه می‌توان به دو کشور امریکا و کانادا اشاره کرد که در دو سطح طرح دعوا برای گرفتن خسارت و ارائه دعاوی حقوقی با یکدیگر همکاری دارند (Geist,2005).

در رابطه با سیاست جنایی تقنینی، قانونگذار ایرانی ابتدا باید مبانی مصداقی در کشور را مورد بررسی قرارداده و میزان اهمیت آن را برای رویارویی کیفری تحلیل نماید. درحال حاضر پیامک‌های ناخواسته تبلیغاتی تلفن همراه در کشور ما یکی از مصادیق این پدیده است که سبب بروز مشکل برای دریافت کنندگان آن شده است و سیاست‌های غیرکیفری و مقررات خود تنظیمی هم نتوانسته است در حل این معضل مؤثر باشد.

مورد دیگری که مقنن در جرم‌انگاری هر عمل یا رفتاری باید به آن توجه کند هدف جرم‌انگاری است، در مورد پیام‌های الکترونیکی ناخواسته هدف مدیریت ارسال پیام و جلوگیری از وقوع جرایم در چنین بستری است. به عبارت دیگر، نوعی حمایت عمومی و جلوگیری از تضییع حقوق مصرف کننده است.

۱.۴. ضرر

موضوع ضرر را باید مهم‌ترین مبنای مقابله با پدیده پیام‌های ناخواسته دانست. اهمیت این موضوع تا جایی است که به عنوان دلایل توجیهی در قوانین کشورها مورد توجه قرار گرفته است. همچنین مقابله با این پدیده در قالب پیام‌های تجاری ناخواسته در بسیاری کشورها سبب شده است تا تمرکز بر خسارات وارده از ناحیه پیام ناخواسته به عنوان یکی از مبانی اصلی از جایگاه ویژه‌ای برخوردار باشد. در این رابطه بخش سه از قانون ضد پیام‌های ناخواسته کانادا در بیان اهداف این قانون آن را عاملی برای جلوگیری از تحمیل هزینه‌های اضافه بر کسب و کار و مصرف کنندگان می‌داند؛ و یا بخش (۷۷۰۱) از مجموعه قوانین امریکا، رشد نامه‌های تجاری الکترونیکی ناخواسته را عامل تحمیل هزینه‌های عمده پولی به تأمین‌کنندگان خدمات دسترسی اینترنت و تجارت کسب و کار می‌داند. در قانون تنظیم انتقال پست الکترونیکی معین مصوب ۲۰۰۲ ژاپن به طور صریح این مسأله عنوان نشده است. در مقررات ایران با توجه به باب قواعد تبلیغ، در قانون تجارت الکترونیکی

موضوع مخاطب تبلیغ و جلوگیری از دریافت تبلیغات غیرقانونی، فریب و مشتبه شدن آن ملاک است و بحث خسارات ناشی از ارسال پیام مورد توجه قانونگذار نبوده است. دو مؤلفه اصلی در باب ضرر که در ادامه مورد بررسی قرار خواهد گرفت؛ یکی توجه به نوع ضرر وارده و دیگری توجه به افراد زیان‌دیده از پیام‌های ناخواسته است.

۱.۱.۴. نوع ضرر

در خصوص پیام‌های الکترونیکی ناخواسته گونه‌های ضرر وارده را می‌توان به دو دسته زیان‌های ناشی از جرم و خسارت مدنی مربوط به ارسال پیام‌های ناخواسته تقسیم نمود. در حالت اول، مبنای جرم‌انگاری پیام‌های ناخواسته، ضرر و زیان ناشی از جرایم مرتبط با ارسال پیام‌های ناخواسته است و به واسطه جرم ارتکابی از طریق ارسال این پیام‌ها هریک از اشخاص دریافت کننده ممکن است متحمل ضرر شوند. در این رابطه پیام‌های ناخواسته قابلیتی بالقوه برای انواع تهدیدها می‌باشد و این تهدیدها سبب کاهش قابلیت اطمینان و امنیت فضای سایبر می‌شود. منظور از تهدیدها آن دسته اقدامات خرابکارانه و مجرمانه‌ای است که علاوه بر آسیب به امنیت شبکه، سامانه‌ها و رایانه‌های شخصی افراد در یک ارتباط آنلاین، سبب می‌شود تا زمینه برای بزه‌دیده شدن افراد در فضای سایبر فراهم شود. به عبارت دیگر، ارسال کنندگان پیام‌های ناخواسته مجرمانی هستند که از این پیام‌ها برای ارتکاب انواع جرایم از قبیل کلاهبرداری، پول‌شویی، اخاذی، اذیت و آزار، سرقت هویت و انتشار انواع مختلی از بدافزارها، برنامه‌های مخرب و ویروس‌ها استفاده می‌کنند و این طریق نه تنها امنیت شبکه و فضای سایبر را برای ارتباطات افراد ناامن می‌نمایند، بلکه ممکن است خسارات فراوانی را به هریک از دریافت کنندگان بزه دیده تحمیل نمایند. در حالت دوم، ارسال کنندگان پیام ناخواسته بدون آنکه مرتکب جرمی شوند و یا قصدی برای ارتکاب جرم داشته باشند به صرف ارسال پیام‌ناخواسته برای اشخاص ممکن است آنها را در معرض زیان قرار دهند. در این رابطه خسارت ناشی از ارسال پیام ناخواسته را می‌توان در دو بعد خسارت مادی و معنوی مورد بررسی قرار داد. منظور از خسارت مادی آن دسته از هزینه‌های مادی و پولی است که به اشخاص خسارت دیده به واسطه گسترش حجم بالای پیام ناخواسته در تبادل پیام وارد می‌شود. این هزینه‌ها نسبت به هر دو نوع شخص حقوقی و حقیقی تحمیل می‌شود. در موضوع شخص حقوقی، هزینه‌های تحمیلی در دو بعد سخت‌افزاری و نرم‌افزاری نمود پیدا می‌کند. در بعد شخص حقیقی تحمیل هزینه بصورت بالا رفتن نرخ خدمات بویژه در رابطه با خدمات ارتباطی پولی است. در مقابل، خسارت معنوی آن دسته از هزینه‌های غیرمادی را شامل می‌شود که اعتبار شخص حقوقی و آسایش و امنیت روانی و اجتماعی شخص حقیقی را هدف قرار می‌دهد. در مورد اخیر، خسارت ارتباط نزدیکی با سایر مبانی جرم‌انگاری پیام ناخواسته نظیر حریم خصوصی و حقوق مصرف کننده دارد؛ زیرا نقص هر دوی این موارد به منزله سلب آرامش روحی و روانی افراد است.

۲.۱.۴. اشخاص زیان دیده

موضوع دیگر در باب ضرر، اشخاص زیان‌دیده از پیام‌های ناخواسته است که باید مشخص گردد. در این رابطه، طیف گوناگونی از اشخاص ممکن است به صورت مستقیم و غیرمستقیم قربانی شوند. به صورت مستقیم دریافت کنندگان پیام در معرض انواع مختلفی از جرایم مالی و محتوایی قرار دارند. همچنین تأمین‌کنندگان خدمات که به واسطه ارسال حجم گسترده‌ای از پیام‌ها با فشار وارده به تجهیزات و خسارت به آنها مواجه می‌شوند و در نتیجه به سبب عدم کیفیت در ارائه خدمات، مشتریان خود را از دست می‌دهند (Lottersberger, 2003, Pp 12-13). بازاریابان و کسب و کار قانونی نیز از ارسال پیام‌های ناخواسته متحمل ضرر می‌شوند در این خصوص ارسال پیام‌های تبلیغاتی فریبنده و بدون رضایت دریافت کننده، سبب می‌شود تا پیام‌های تبلیغاتی قانونی، توسط دریافت کننده نادیده گرفته شده و پاک گردد (Lottersberger, 2003, p 14)؛ زیرا ذهنیت بدی نسبت به پیام‌های تبلیغاتی دارد. اما در مقابل اشخاص دیگری نیز هستند که به طور غیرمستقیم از ارسال پیام ضرر می‌بینند. برای نمونه، اشخاص ثالثی که ارسال کنندگان به صورت غیرمجاز و جعلی از نام دامنه، آدرس پست الکترونیکی و خدمات رایانامه آنها جهت ارسال پیام ناخواسته استفاده می‌کنند و ممکن است به اشتباه در معرض فشار و شکایت‌های دریافت کنندگان قربانی، قرار بگیرند (Lottersberger, 2003, p 14) و یا اشخاصی که به اشتباه آدرس پست الکترونیکی آنها ممکن است توسط سیستم‌های ضد پیام‌های ناخواسته تأمین‌کنندگان در لیست سیاه قرار بگیرد و بی دلیل از ارسال پیام برای افراد دیگر محروم شوند (Goodman, 2004, p7). با توجه به تقسیم گونه‌های ضرر، در ادامه به ذکر برخی مصادیق ورود ضرر به اشخاص زیان‌دیده پرداخته می‌شود.

اگرچه ارسال پیام ناخواسته از سوی ارسال کنندگان در سطح انبوه برای مقاصد مختلف با توجه به هزینه‌های آن ارزان است، اما دریافت پیام ناخواسته برای دریافت کننده ارزان نیست. در بسیاری از کشورها هزینه‌های ارتباطی پولی است و فرد در مقابل پرداخت هزینه، خدمات دریافت می‌کند. برای نمونه ۱۵ درصد مشتریانِ تأمین‌کنندگان بزرگ در امریکا، به طور جاری برای زمان اتصال پول پرداخت می‌کنند (Bahr, 1998, p 12)، که در چنین اوضاع و احوالی مشتریان بطور مستقیم متحمل هزینه از تأمین کننده می‌شوند. بنابراین، زمان سپری شده در صندوق‌های پستی آنها برای حذف یا دانلود پیام‌های ناخواسته در افزایش هزینه آنها مؤثر است. همچنین این حجم پیام و بررسی آنها در رایانامه سبب می‌شود ترافیک اختصاص یافته برای یک دوره مشترک به اتمام برسد. جدا از بحث هزینه اشتراک، وجود برخی نرم‌افزارهای مخرب در این پیام‌ها، نه تنها باعث پاک شدن اطلاعات افراد می‌شود، بلکه به لحاظ نرم‌افزاری ممکن است به رایانه‌های شخصی خسارت وارد کند. پیام ناخواسته علاوه بر تحمیل خسارت مادی به لحاظ معنوی نیز بر رفتار و افکار دریافت کنندگان مؤثر است و می‌تواند منجر به سلب آرامش روحی و روانی افراد شود. بسیاری از پیام‌های ناخواسته آزاردهنده است و باعث عصبانیت افراد دریافت کننده می‌شود و اتلاف وقت آنها را به منظور

بازکردن و پاک کردن این پیام‌ها به همراه دارد. تصور کنید زمانی که فردی در انتظار دریافت یک پیامک شخصی است، در همین حین پیامکی ناخواسته دریافت می‌کند یا زمانی که فرد در شخصی‌ترین حالات و ساعات خویش در حال برقراری یک ارتباط میان فردی است و در یک لحظه با ورود تبلیغاتی ناخواسته و آزار دهنده مواجه می‌شود؛ در تمام این موارد نمی‌توان مرزی میان ارتباط فردی و جمعی و بالتبع حریم خصوصی افراد قائل بود (طاهره خیرخواه، به نقل از برکت، ۱۳۸۶، ص ۸). همچنین، هدف قرارگرفتن محتوایی رایانامه کاربران خاص، مثل نوجوانان برای آزار و اذیت جنسی و نگرانی والدین آنها برای دریافت پیام‌های غیراخلاقی توسط فرزندانشان، از دیگر مصادیق خسارت معنوی است (Metchis, 2003, p 7).

تأمین‌کنندگان خدمات ارتباطی نیز از گسترش حجم بالایی از پیام‌های ناخواسته ناراضی هستند. این تأمین‌کنندگان اگرچه همچون دریافت کنندگان به صورت مستقیم هدف قرار نمی‌گیرند، ولی آثار ناشی از این حملات سبب شده است تا آنها نیز متحمل برخی خسارات مادی و معنوی شوند. فشار ناشی از پیام ناخواسته به سرورها و افزایش ترافیک شبکه به دلیل حجم بالایی از تبادل پیام، تأمین‌کنندگان را وادار می‌کند تا نسبت به بکارگیری تجهیزات و افزایش پهنای باند جهت رضایت مشترکان خود اقدام کنند و این موضوع هزینه‌بر است. نمونه‌ای دیگر از تحمیل هزینه به تأمین‌کنندگان مسأله پالایش است؛ آنها مجبور هستند برای رضایت مشترکان و جلب اعتماد آنها از ارسال پیام ناخواسته به رایانامه‌شان جلوگیری بعمل آورند و برای این کار نیازمند بکارگیری و استفاده از نرم‌افزارهای قوی و البته گران‌قیمت هستند. عدم ارائه خدمات به مشترکان به واسطه پیام ناخواسته، در برخی مواقع منجر به تعقیب تأمین کننده از ناحیه مشترک شده است که این موضوع جدا از بحث تاوان خسارت، بی‌اعتباری تأمین کننده را در قالب خسارت معنوی به همراه دارد (Metchis, 2003, p 7).

بازاریابان و کسب و کار قانونی از دیگر اشخاص زیان دیده از پدیده پیام ناخواسته می‌باشند. از نظر خسارت مادی وجود حملات متعدد پیام ناخواسته و هجوم ویروس‌های پیامی، هزینه‌های پشتیبانی فنی بالایی را جهت حفظ کارایی و بهره‌وری برای بازاریابان و کسب و کار تجاری ایجاد کرده است. همچنین وجود پیام ناخواسته به عنوان یک عامل تهدید در بازاریابی و تبلیغات پیامی تلقی می‌شود؛ زیرا استفاده از روش‌های غیرحرفه‌ای در ارسال پیام بویژه پیام‌های تجاری، کاهش مشتریان را برای کسب و کار به همراه دارد. به لحاظ خسارت معنوی نیز بازاریابان و کسب و کار، متأثر از ارسال پیام ناخواسته هستند، در این خصوص می‌توان به استفاده از آگهی‌های متقلبانه، فریبنده و تبلیغات نادرست اشاره کرد. در این فرآیند، ارسال کنندگان پیام ناخواسته و بازاریابان غیرقانونی از هر روشی برای رسیدن به مقاصد خویش استفاده می‌کنند، برای نمونه آنها برای جلب مشتریان اقدام به استفاده از نام‌های تجاری معروف در ارسال پیام می‌کنند. این موضوع نه تنها منجر به فریب مشتری می‌شود، بلکه بی‌اعتباری کسب و کار اصلی را هم در پی دارد. و نتیجه‌ای که

از این فرآیند عاید کسب و کار تجاری می‌شود چیزی جز کاهش اعتماد مصرف کنندگان نیست (Xingan, 2006). نمونه دیگر از خسارت معنوی به بازاریابان و کسب و کار، موضوع تعقیب قضایی آنها توسط مشتریان است. در بسیاری از کشورهای دارای قوانین ضد پیام ناخواسته مثل امریکا، امکان گزارش پیام ناخواسته به نهادهای قانونی فراهم شده است، برای مثال در امریکا کمیسیون تجارت فدرال یکی از این نهادها است. اما برخی مواقع به دلیل حجم بالای پیام ناخواسته و کلافه شدن مشتریان از آن، پیام‌های قانونی بازاریابان به اشتباه به جای پیام ناخواسته گزارش می‌شود؛ که این موضوع مشکلاتی را برای بازاریابان ایجاد می‌کند.

۲.۴. حریم خصوصی

از جمله حقوق شناخته شده برای انسان‌ها حق حریم خصوصی آنها می‌باشد. امروزه، دیگر صرف حمایت از حریم خصوصی افراد در محیط فیزیکی مطرح نیست، بلکه بکارگیری نامناسب فناورهای نوین و سوء استفاده از وسایل ارتباطی در نقض حریم خصوصی افراد در فضای سایبر، قانونگذار بسیاری از کشورها را به سمت حمایت از چنین فضایی رهنمون کرده است. حمایت ازحریم خصوصی در فضای سایبر را باید در دو حوزه حریم خصوصی اطلاعاتی و حریم خصوصی ارتباطاتی مورد بررسی قرار داد. این دو حوزه از حریم خصوصی می‌تواند به صورت یکجا و ذیل حمایت از اطلاعات نیز بحث شود. زیرا ارتباطات الکترونیکی با تبادل حجم بالایی از داده‌ها در فضای سایبر صورت می‌گیرد و همین امر سبب می‌شود قواعد حاکم بر هر دو حوزه مشابهت‌های زیادی باهم داشته باشند (حسنی، صص ۱۶۸-۱۶۷). به عبارت دیگر، چون حریم خصوصی ارتباطاتی در فضای سایبر مبتنی بر ایجاد، پردازش و انتقال داده‌ها صورت می‌گیرد اصول و قواعد یکسانی با حریم خصوصی اطلاعاتی دارد (رجبی، ۱۳۹۱، ص۳۸). بدین سان حریم خصوصی در فضای سایبر همچون فضای فیزیکی مورد احترام می‌باشد؛ و تعرض به حریم الکترونیکی افراد نیز باید مورد حمایت قانونگذار قرار بگیرد. چه بسا توجه به این فضا باید مورد حمایت بیشتر باشد؛ زیرا «نمی توان انکار کرد که زمینه‌های تعرض به حریم الکترونیکی افراد همانند بسیاری از سوء استفاده‌های مجرمانه و ناهنجار، از سهولت بیشتری در این فضا برخوردار است» (جلالی فراهانی، ۱۳۸۵، ص۱۵). مفهوم حریم خصوصی در فضای سایبر گاهی با توجه به وجود شباهت‌ها و اهمیت داده‌ها در تبادل ارتباطات بر مبنای اطلاعات و حمایت از داده مورد تعریف قرار می‌گیرد و گاهی هم هر دو حوزه اطلاعات و ارتباطات به صورت مجزا تعریف می‌شود. حریم خصوصی در مفهوم اطلاعاتی عبارت است از حق اولیه افراد در محرمانه ماندن اطلاعات شخصی و ممانعت از تحصیل، پردازش و انتشار غیرقانونی داده‌های شخصی مربوط به ایشان مگر در موارد مصرح قانونی. و حریم خصوصی در مفهوم ارتباطاتی عبارت است از حق اشخاص در امنیت کلیه اشکال و صور مراسلات و مخابرات متعلق به ایشان و محرمانه باقی ماندن محتوای آنها و اطلاعات مربوطه (اصلانی، ۱۳۸۹، ص۲۸). پیشینه حمایت از حریم خصوصی ارتباطاتی به

ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی برمی‌گردد که بـه حـق بهـره‌بـرداری از مصـونیت مکاتبات و مراسلات اشاره دارد. همچنین چنین حقی در بند ب مـاده ۱۸ اعلامیـه اسـلامی حقـوق بشر به رسمیت شناخته شده است (مهرپور، ۱۳۷۴، ص۴۵۲). ولی، در حوزه ارتباطات الکترونیکـی سـابقه آن بـه دسـتورالعمل «پـردازش داده‌هـای شخصـی و حمایـت از حـریم خصوصـی ارتباطـات الکترونیکی 2002/58/EC» اتحادیه اروپا برمی‌گردد. در ماده یک این دسـتورالعمل بـه طـور خـاص حریم خصوصی افراد در جریان اطلاعـات شخصـی در بخـش ارتباطـات الکترونیکـی و انتقـال آزاد خدمات و تجهیزات ارتباطات الکترونیکی مورد حمایت قرار گرفته است. براساس دستورالعمل حـریم خصوصی اتحادیه اروپا در سال ۲۰۰۲ از جمله مواردی که می‌تواند جهت حمایـت از حـریم‌خصوصـی ارتباطاتی در قلمرو حقوق کیفری مورد بررسی قرار گیرد موضوعاتی چون شنود، مسائل راجـع‌بـه داده ترافیک و داده موقعیت و ارتباطات و تماس‌های الکترونیکی ناخواسته است (حسنی، ۱۳۸۵، ص۱۷۷). آنچـه در حال حاضر در این تحقیق بدان پرداخته می‌شود موضوع پیام ناخواسته به عنوان یکی از مصادیق ارتباطات الکترونیکی ناخواسته است. در موضوع پیام‌های ناخواسته، به‌ویـژه از نـوع تجـاری یکـی از جنبه‌هایی که از سوی مشتریان و دریافت کنندگان مورد اعتراض قرار مـی‌گیـرد تجـاوز بـه حـریم خصوصی‌شان است. از دید بیشتر مردم صندوق‌های پست‌الکترونیکی یـک فضـای شخصـی اسـت و ورود به آن مستلزم کسب اجازه است (Sipior, 1998, p 2). بدین جهت، حریم خصوصی به عنوان یکـی از مبانی حقوقی مورد توجه کشورها قرار گرفته است. برای نمونه، می‌توان به قانون ضـد پیـام‌هـای ناخواسته کانادا اشاره کرد که در آن ارسال پیام‌های ناخواسته به عنوان یکی از رفتارهـای نامناسـب تجاری به منزله اخلال در حفظ حـریم خصوصـی و امنیـت اطلاعـات محرمانـه تلقـی شـده اسـت (Canada's anti Spam Law, § 3(3)).

در رابطه با مصادیق نقض حریم خصوصی توسط پیام ناخواسته با توجه به تعریفی کـه از حـریم خصوصی ارتباطاتی بیان شد می‌توان بـه ورود بـه خلـوت افـراد، امنیـت تبـادل پیـام و محرمـانگی اطلاعات تماسی و ارتباطی افراد اشاره کرد. حق خلوت، عبارت است از حق تنها مانـدن شـخص در حریم شخصی خویش و عدم مزاحمت از سوی سایرین نسبت به وی. مشخص نبودن مرزهای حریم خصوصی در کشور باعث می‌شود خلوت افراد به کرات مورد تعرض قرار بگیرد. ارسال حجم بالایی از پیام‌های ناخواسته از طریق وسایل ارتباطی در هر ساعت از شبانه روز، مختل کننده چنین حقی در فضای سایبر است. این پیام‌ها از طریق شخصی‌ترین ابزارها، حریم خصوصی افراد را نشانه می‌گیـرد و به آنها راه پیدا کرده و افراد بدون آنکه حضور این پیام‌ها را درک کنند ناآگاهانه آنها را می‌پذیرنـد و با آنها ارتباط برقرار می‌کنند. این مساله باعث شده است تا پیام‌های ناخواسته به تـدریج جزئـی از زندگی افراد شوند (برکت، ۱۳۸۶، ص۸). در ایران پیامک‌های تبلیغاتی تلفن همـراه در مقایسـه بـا سـایر پیام‌های ناخواسته شیوع بیشتری دارد. ارسال انبوه پیامک‌های تبلیغاتی بی‌فایده و در برخـی مـوارد فریبنده برای افراد، دیگر از یک دلخوری ساده فراتر رفته است و تبدیل بـه یـک تهدیـد نسـبت بـه حریم خصوصی افراد شده است. اخذ رضایت برای ورود به خلوت افراد حق اولیه هـر فـردی اسـت،

ولی متاسفانه چنین حقی با ارسال پیام‌های ناخواسته غیرمنتظره نادیده گرفته می‌شود. همچنین ارسال پیام‌های ناخواسته علاوه بر اینکه ورود به حق خلوت افراد می‌باشد به صورت ناخواسته فرد را به سوی یک ارتباط جمعی سوق می‌دهد و بدین ترتیب مرز ارتباط میان فردی از بین می‌رود (طاهره خیرخواه، به نقل از برکت، ۱۳۸۶، ص ۸).

ارسال پیام‌های متعدد و با حجم بالا از سوی ارسال کنندگان پیام ناخواسته (Spammer) با اهداف تجاری و غیرتجاری اگرچه منجر به مختل شدن کامل ارتباطات خواسته شده افراد نمی‌شود، اما کارایی سیستم‌های ارتباطی را کاهش می‌دهد. حملات کاهنده کارایی(Buffer Overflow Attacks)، نسبت به تخریب‌کننده‌های سیستم‌های رایانه‌ای قدرت تخریبی و بازدارندگی کمتری دارند، ولی امروزه به عنوان یک عمل ممنوع و ناقض حریم خصوصی به رسمیت شناخته می‌شوند. در عرصه مخابراتی به اینگونه حملات، تماس ناخواسته و در عرصه ارتباطات اینترنتی، پیام ناخواسته گفته می‌شود (اصلانی، ۱۳۸۹، ص ۲۹۷). جرم‌انگاری ارسال پیام‌های ناخواسته در کنوانسیون جرایم سایبر مصوب سال ۲۰۰۱ مورد توجه قرار گرفت؛ اگرچه به عنوان یکی از جرایم سایبری توافقی در مورد آن صورت نگرفت، با این وجود در گزارش توجیهی کنوانسیون در مبحث جرم‌انگاری اخلال در سیستم‌ها، موضوع ماده پنج، به ارسال پیام ناخواسته با حجم گسترده توجه شده است و آن را عاملی مختل‌کننده برای سیستم‌های رایانه‌ای و ارتباطی می‌داند. براساس این گزارش ارسال حجم زیادی پیام ناخواسته آن هم به کرات ممکن است برای گیرنده آن ایجاد مزاحمت نماید. همچنین زمانی باید نسبت به چنین عملی جرم‌انگاری صورت گیرد که موجب قطع ارتباطات به طور جدی و از روی عمد شده باشد (عالی پور، ۱۳۹۰، ص ۳۴۷).

نقض محرمانگیِ اطلاعات تماسی و ارتباطی افراد و سوء استفاده از آنها نمونه‌ای دیگر از مصادیق نقض حریم خصوصی توسط پیام ناخواسته است. ارسال نامه‌های ناخواسته می‌تواند از دو جنبه برای ارسال‌کنندگان آن مفید باشد. اول آنکه در صورت پاسخ از سوی دریافت کننده، صحت اعتبار پست الکترونیکی وی برای ارسال کننده روشن می‌شود و از این پس ارسال به صورت هدفمند و نه تصادفی انجام می‌شود. دوم آنکه اطلاعات تماسی و آدرس الکترونیکی دریافت کننده مورد انواع سوء استفاده‌ها توسط ارسال کننده قرار می‌گیرد و در واقع می‌تواند مقدمه‌ای برای وقوع جرایم باشد. از جمله مصادیق نقض حریم خصوصی کاربران می‌توان به جمع‌آوری آدرس‌های الکترونیکی و ذخیره سازی و بهینه سازی آن برای ارسال پیام‌های الکترونیکی ناخواسته اشاره کرد (جلالی فراهانی، ۱۳۸۵، ص۲۹). ارسال کنندگان پیام ناخواسته با استفاده از دستگاه‌های خودکار اقدام به جمع‌آوری آدرس‌های الکترونیکی افراد به منظور ارسال پیام‌های ناخواسته به آنها می‌کنند. این موضوع حتی به صورت سازمان یافته توسط گروه‌ها و شرکت‌ها انجام می‌شود. سازمان‌هایی وجود دارد که کار آنها به طور اختصاصی جمع‌آوری پست الکترونیکی کاربران، خرید و فروش آنها و ارسال پیام ناخواسته است. این سازمان‌ها با استفاده از ابزارهای لازم نظیر رایانه‌های کارگزار، نیروی

انسانی متخصص اقدام به جمع‌آوری آدرس‌های الکترونیکی افراد از تارنماها می‌کنند و سپس آدرس‌های بدست آمده را در اختیار شرکت‌ها و مؤسساتی قرار می‌دهند که اقدام به ارسال پیام‌های تبلیغاتی تجاری می‌نمایند. این در حالی است که هویت افراد ارسال کننده و رایانه‌های آنها با اقدامات متقلبانه مخفی می‌ماند (حسنی، ۱۳۸۵، ص۱۷۴).

سوء استفاده ارسال کنندگان پیام ناخواسته از اطلاعات تماسی و آدرس‌های الکترونیکی افراد به شیوه‌های دیگری نیز انجام می‌شود. برای مثال، استفاده از آدرس‌های واقعی افراد علیه اشخاص ثالث و یا استفاده از آدرس‌های واقعی ثبت شده در پست الکترونیکی افراد و ارسال انواع پیام‌های ناخواسته به عنوان دوستانی که فرد با آنها ارتباط الکترونیکی در فضای سایبر دارد. برای مثال ارسال پیام‌های ناخواسته با آدرس استاد برای دانشجویانش. در این رابطه می‌توان به کلاهبرداری هکرها از تجار ایرانی اشاره کرد که براساس آن هکرها با نفوذ در رایانامه شخص و سوء استفاده از اطلاعات تماسی افرادی که قبلاً این شخص با آنها ارتباط کاری داشته اقدام به برقراری ارتباط می‌کنند. در این پرونده فرد هکر با ارسال رایانامه‌ای مشابه فرد طرف معامله با زیان‌دیده، اقدام به دادن شماره حساب با پیش فاکتور جدید می‌نماید و زیان دیده را به نوعی با ارسال رایانامه مشابه فریب داده و اقدام به بردن مال وی می‌نماید. (http://www.cyberpolice.ir/news/29641) در رابطه با جلوگیری از نقض محرمانگی اطلاعات تماسی و آدرس‌های الکترونیکی افراد می‌توان به ماده (۱) ۱۳ دستورالعمل2002/58/EC اتحادیه اروپا اشاره کرد که در آن استفاده از سیستم‌های تماسی خودکار یا استفاده از پیام‌های الکترونیکی به قصد بازاریابی مستقیم، تنها با رضایت قبلی افراد مجاز شناخته شده است. همچنین، در حقوق برخی کشورها نظیر امریکا در رابطه با جمع‌آوری اطلاعات تماسی افراد الزاماتی در نظر گرفته شده است. قانون ضد پیام‌های ناخواسته فدرال امریکا مصوب ۲۰۰۳ در بخش (۷۷۰۴) هرگونه جمع‌آوری آدرس پست الکترونیکی، ایجاد حساب‌های پست الکترونیکی متعدد و تکرار ارسال پیام از طریق دسترسی غیرمجاز را از مصادیق نقض‌های شدید در مورد پست الکترونیکی تجاری می‌داند.

۳.۴. حقوق مصرف کننده

ارسال پیام برای اشخاص باید دارای قواعدی خاص باشد و در این میان فرقی میان پیام‌های تجاری و غیرتجاری نیست. وجود شرایط و ویژگی‌های خاص در تبادل پیام تضمین‌کننده حقوق طرفین پیام است. نبود مدیریت در ارسال پیام و قواعد قانونی لازم در این رابطه باعث شده است تا نه تنها نوعی بی‌اعتمادی و عدم رغبت در دریافت پیام برای دریافت کنندگان آن ایجاد شود، بلکه در بسیاری از موارد نظیر بازاریابی مستقیم نتیجه‌ای معکوس برای ارسال‌کنندگان آن به بار آورد. برای نمونه، «موفقیت‌های ناشی از تجارت الکترونیکی به منافع ناشی از آن برای مصرف‌کنندگان و جلب اعتماد آنان وابسته است و فقدان اعتماد کافی در مصرف‌کنندگان نسبت به حمایت از برخی حقوق

آنان در مواردی مانند تبلیغات گمراه‌کننده و اطلاع رسانی نادرست در فضای مجازی مانعی برای گسترش تجارت الکترونیکی خواهد بود.» (گروه مطالعات و پژوهش‌های حقوق اقتصادی و بازرگانی، ۱۳۸۸، ص۲۷). هر شخصی حق دارد تا نوع، میزان و طرف ارتباط را خود انتخاب نماید و نسبت به اطلاعات تماسی ارسال کننده اطلاع لازم را داشته باشد. امروزه، ارسال کنندگان پیام ناخواسته بدون توجه به تمایلات، وضعیت فردی و اجتماعی فرد مبادرت به ارسال پیام برای وی می‌کنند، بدون آنکه از قبل بابت ارسال پیام اجازه‌ای اخذ نمایند و یا نظر دریافت کننده را در مورد این ارتباط و موضوع آن جویا شوند. در صورتی هم که فرد خواسته یا ناخواسته به ارسال پیام، پاسخ مثبت بدهد در بسیاری از موارد ساز و کارهایی برای اعلام انصراف و قطع این رابطه وجود ندارد و به ناچار باید دریافت این پیام‌ها را تحمل نماید. فارغ از اهداف پیام‌های ناخواسته، ورود به حریم خصوصی افراد نیازمند رعایت الزاماتی است. این الزامات، حقوقی از قبیل حق انتخاب، اعلام انصراف، اطلاع از موضوع و اطلاعات تماسی ارسال کننده را برای دریافت کننده پیام (مصرف کننده) تضمین می‌کند.

۱.۳.۴. حق انتخاب

اعلام رضایت از سوی دریافت کننده به منزله ایجاد حق انتخاب برای دریافت پیام است. البته باید گفت این حق در رضایت اولیه نمود بیشتری دارد؛ زیرا در رضایت ثانویه افراد بعد از دریافت پیام می‌توانند نسبت به این حق خویش اظهارنظر نمایند که آیا مایل به ادامه دریافت هستند یا خیر و در صورت عدم تمایل می‌توانند نسبت به آن اعلام انصراف کنند. در حالی که در رضایت اولیه انتخاب و اراده آزاد شخص ملاک است؛ به عبارت دیگر، در رضایت اولیه، انتخاب، اعلام رضایت است، اما در رضایت ثانویه اعلام انصراف است. در دستورالعمل سال ۲۰۰۲ اتحادیه اروپا بر لزوم مقرراتی مبنی بر شرط رضایت قبلی افراد و تضمین رضایت آنها در ارتباطات الکترونیکی بویژه در زمینه بازاریابی و تجارت الکترونیکی در مقرارت کشورهای عضو تاکید شده است (مواد (۳) (۴) ۱۳ دستورالعمل 2002/58/EC اتحادیه اروپا). دیدگاه کشورهای مورد مطالعه در موضوع حق انتخاب متناسب با نوع سیستم اعلام رضایت متفاوت است. در قانون ضد پیام‌های ناخواسته فدرال امریکا ارسال کننده ملزم به تطبیق براساس رضایت ثانویه می‌شود و انتقال پیام ۱۰ روز بعد از دریافت عدم رضایت ممنوع است (Hallace, 2004, p 73). در مقابل، در قانون ضد پیام‌های ناخواسته کانادا و ژاپن اعمال حق انتخاب متناسب با رضایت اولیه است، در قانون کانادا شخصی که پیام را دریافت می‌کند باید رضایت به دریافت آن داده باشد (Canada's Anti Spam Law, § 6(1)). همچنین مطابق با قانون ضد پیام‌های ناخواسته ژاپن ارسال کننده پیام باید پیش از انتقال پیام رضایت دریافت کننده را کسب نماید و در صورت رد دریافت توسط دریافت کننده از ارسال پیام خودداری نماید (Japanese new anti-spam law Article 3,).

در حقوق ایران در قانون تجارت الکترونیکی مصوب ۱۳۸۲ ماده ۵۵ به طور خاص نسبت به نحوه دریافت پیام تجاری از طریق بازاریابی مستقیم اشعار می‌دارد: «تأمین‌کنندگان باید تمهیداتی را برای

مصرف کنندگان در نظر بگیرند تا آنان راجع به دریافت تبلیغات به نشانی پستی و یا پست الکترونیکی خود تصمیم بگیرند.» همانطور که از متن ماده برداشت می‌شود در خصوص حق انتخاب برای دریافت پیام، تأمین کننده ملزم به رعایت تمهیدات است، ولی ساز و کارهای این تمهیدات مشخص نیست؛ همچنین منظور از تمهیدات بیان نشده است. شاید منظور آن رعایت الزامات شکلی نظیر ذکر مشخصات ارسال کننده پیام و ذکر آدرس تماس برگشت به گیرنده پیام است تا در صورت عدم تمایل به دریافت مجدد پیام، آن را به اطلاع فرستنده برساند (فضلی، باطنی، ۱۳۸۸، ص ۲۰۹). صرف نظر از عدم تبیین تمهیدات برای دریافت پیام، این ماده به نوبه خود نشان دهنده احترام به خواسته‌های مصرف کننده است. «مطابق ماده ۲۷ رویه حرفه‌ای بین‌المللی اتاق بازرگانی درباره بازاریابی مستقیم، اگر سیستمی برای بیان خواسته‌های مصرف کننده مبنی بر عدم دریافت مرسوله پستی فاقد نشانی ارسال کننده، در میان باشد باید به این خواسته احترام گذارده شود.» در این خصوص می‌توان به قانون سال ۲۰۰۳ امریکا با عنوان "در لیست تماس نگیرید" اشاره کرد که به موجب آن افرادی که تمایل به دریافت تماس‌های ناخواسته تبلیغاتی ندارند می‌توانند مشخصات خویش را در این لیست وارد کنند و بازاریابان نیز براساس اسامی وارده در این لیست از تماس با آنها خودداری می‌کنند (خندانی، ۱۳۸۵، صص۷۹-۷۸).

اجرای این سیستم در مورد پیام‌های ناخواسته نیز مورد بررسی قرارگرفته است (National Do Not Email Registry). در این سیستم، در مرحله اول افرادی که تمایلی به دریافت پیام‌های تبلیغاتی ندارند اقدام به ثبت رایانامه می‌کنند و در مرحله دوم فهرست این رایانامه‌ها در اختیار بازاریابان قرار می‌گیرد تا براساس آن اقدام به حذف نام این افراد از میان لیست مخاطبان خود نمایند. براساس قانون ضد پیام‌های ناخواسته فدرال امریکا کمیسیون تجارت فدرال موظف به دادن گزارشی در رابطه با قابلیت چنین سیستمی شده بود. در گزارش سال ۲۰۰۴ کمیسیون بیان شده است که اجرای چنین سیستم ملی در کشور بدون یک سیستم در محل برای تأیید هویت منشاء پیام ناخواسته با شکست روبرو خواهد شد. بنابراین، پیشنهاد می‌کند در گام اول برای جلوگیری از رایانامه‌های جعلی، پست الکترونیکی تقویت شود (Federal Trade Commission, 2004, p I). در این گزارش آمده است با وجود ثبت رایانامه‌های افرادی که تمایلی به دریافت پیام‌های تبلیغاتی ندارند، اما ارسال کنندگان با توسل به رایانامه‌های جعلی دوباره اقدام به ارسال پیام ناخواسته می‌نمایند. بنابراین، فقدان سیستمی برای تصدیق هویت منبع پیام‌ها باعث می‌شود تا نه تنها میزان پیام‌های ناخواسته کاهش پیدا نکند، بلکه حتی به دلیل دسترسی بازاریابان به رایانامه‌های معتبر میزان آن افزایش یابد (Federal Trade Commission, 2004, p 33). علاوه بر این، دسترسی بازاریابان به اطلاعات تماسی افراد به نوعی حریم خصوصی آنها را نیز تهدید می‌نماید. کمیسیون فدرال «این سیستم را در بهترین حالت بی‌اثر و در بدترین حالت فلج کننده برای سیستم رایانامه و تسهیل‌کننده در ارسال بیشتر پیام ناخواسته می‌داند.» در نهایت، کمیسیون در گزارش خویش به کنگره با وجود مدل‌های

پیشنهادی برای ثبت رایانامه، مؤثرترین روش برای مبارزه با پیام ناخواسته را ایجاد استانداردهایی بـرای احراز هویت رایانامه تبلیغ‌کننده می‌داند (Federal Trade Commission, 2004, pp 34-37).

۲.۳.۴. اعلام انصراف

همانطور که مصرف کننده مخییر به دریافت پیام است باید نسـبت بـه قطـع رابطـه و پایـان دادن بـه تبادل پیام نیز دارای اختیار باشد. چنین حقی برای مصرف کننده به صورت اعلام انصـراف جلـوه پیـدا خواهد کرد. نمی‌توان افراد را به واسطه رضایت اعم از (اولیه، ثانویه) بـه ارتبـاط پیـامی دائمـی مجبـور کرد، بلکه باید شخص هـر زمـان کـه اراده کـرد بتوانـد بـه ایـن ارتبـاط پایـان دهـد. مـاده (۳) ۱۳ از دستورالعمل اروپایی بر لزوم حق انصراف و اعلام عدم رضایت بـرای مشـترکین ارتباطـات الکترونیکـی تأکید دارد. چنین حقی برای افراد به طور معمول با مکانیزم لغو اشتراک فراهم می‌شود. ایـن مکـانیزم تابع مجموعه شرایطی است که با فراهم شدن آنها امکان حق انصراف برای فرد دریافت کننده پیـام بـه وجود می‌آید و یا در برخی موارد تسهیل می‌شود. اولین شرط در این مکـانیزم اعـلام آدرس برگشـتی توسط ارسال کننده پیام است. دومین شرط امکان اعلام انصراف با هر وسیله الکترونیکی، اعم از همـان وسیله‌ای که با آن پیام ارسال شده است و یا هر وسیله‌ای غیرآن. و در نهایت، وجود یک نهـاد نظـارتی برای پیگیری اعلام انصراف دریافت کننده به عنوان شرط سوم. در قانون ضد پیام‌های ناخواسته امریکا ارسال پیام بدون وجود مکانیزم آدرس برگشتی غیرقانونی است و ارسال پیام بـه همـراه آدرس پسـتی معتبر می‌باشد. شخص دریافت کننـده نیـز مـی‌توانـد براسـاس رفتـاری خـاص مبتنـی بـر ارتباطـات الکترونیکی اعلام انصراف از دریافت پیام‌های بیشتر را از سوی ارسال کننده نماید. این رفتار مـی‌توانـد به صورت یک پاسخ منفی و یا دیگر اشکال ارتباطی باشد.((15 U.S.C § 7704(a) (3),(4)) اجـرا و نظـارت بـر این قانون به وسیله کمیسیون تجارت فدرال امریکـا انجـام مـی‌شـود. همچنـین تجـاوز از قـانون ضـد پیام‌های ناخواسته براساس بخش ۱۸ قانون کمیسیون تجارت فدرال، عملی فریبنده و ناعادلانـه تلقـی می‌گردد (15 U.S.C § 7706). بخش ۱۱ از قانون ضد پیام‌های ناخواسته کانادا نیز، تحت عنوان «مکـانیزم لغو اشتراک»، شخص ارسال کننده پیام را ملزم می‌کند تا بـرای دریافـت کننـده، توانـایی نشـان دادن عدم دریافت پیام از وی یا از طرف وی را فراهم نماید. این امکان یا توسـط همـان وسـیله الکترونیکـی ارسال پیام انجام می‌شود و یا در صورت عدم امکان با هر وسیله دیگر. همچنین یک آدرس الکترونیکـی در صفحه تارنما برای دسترس بودن باید توسط ارسال کننده تعیین گـردد. همچنـین اجـرای اولیـه ایـن قانون برعهده کمیسیون رادیو و تلویزیون و ارتباطات کانادا است(Beardwood And M. A, 2011).

۳.۳.۴. حق اطلاع

براساس این حق ارسال کننده باید جزئیات اطلاعات تماسی را جهت شروع تبـادل پیـام در اختیـار دریافت کننده قرار دهد؛ زیرا بدون اطلاع از مشخصات ارسال کننـده و موضـوع پیـام، اعتمـاد لازم

برای شروع یک تبادل پیامی وجود ندارد و عدم رضایت دریافت کننده و ناخواسته بودن پیام را به همراه دارد. عدم ذکر اطلاعات تماسی در پیام ناخواسته یکی از تفاوت‌های موجود با پیام‌های خواسته شده است. به عبارت دیگر، گمنامی جزئی از فضای پیام‌های ناخواسته می‌باشد که در آن ارسال کنندگان قادر به انجام هرگونه فعالیت غیرقانونی و مجرمانه خواهند بود و هیچ حقی برای دریافت کننده پیام از باب درخواست عدم ارسال قائل نخواهند بود. در رابطه با حق اطلاع از اطلاعات تماسی دستورالعمل اروپایی علاوه بر به رسمیت شناختن آن به معتبر بودن این اطلاعات نیز تأکید ویژه‌ای دارد. بر این اساس دستورالعمل اروپایی تاکید می‌کند که ارسال پیام در راستای بازاریابی مستقیم باید همراه با اطلاعات تماسی معتبر باشد تا گیرنده پیام بتواند در صورت عدم تمایل درخواست خویش را ارسال نماید. دستورالعمل تأکید می‌کند که عدول از این حقوق باید در قانونگذاری ملی کشورها ممنوع شود (ماده (۴) ۱۳ دستورالعمل 2002/58/EC اتحادیه اروپا). در مقررات ضد پیام‌های ناخواسته اکثر کشورها این موضوع به طور معمول در ذیل عنوان «الزامات و ممنوعیت‌ها در انتقال پیام» مطرح می‌شود. در قانون فدرال امریکا ارسال کننده ملزم به ارائه اطلاعات تماسی معتبر است و مطابق بخش (۷۷۰۴) از قانون ضد پیام‌های ناخواسته فدرال از هرگونه اطلاعات نادرست و گمراه‌کننده منع شده است. قانون ضد پیام‌های ناخواسته کانادا نیز در بخش شش شخص ارسال کننده و یا از طرف او را ملزم به دادن اطلاعات لازم جهت شناسایی هویت و اطلاع پیدا کردن گیرنده پیام برای ارتباط با او یا شخصی از طرف وی می‌کند. همچنین مطابق با قانون ضد پیام‌های ناخواسته ژاپن ارسال کننده باید مشخصات کامل فردی و تماسی و سایر موضوعات تعیین شده توسط وزارت ارتباطات را در انتقال پیام لحاظ کند و از ارسال اطلاعات جعلی برای گیرنده خودداری نماید (Japanese New Anti-Spam Law, Articles 3 & 4).

در حقوق ایران در «قانون تجارت الکترونیکی» باب قواعد تبلیغ در بستر مبادلات الکترونیکی در ماده ۵۳ تبلیغ کننده اعم از شخص یا بنگاه ملزم شده است تا به صورت روشن و صریح هویت خویش را ذکر نماید. همچنین در ماده ۵۲ این قانون ذکر اطلاعات دقیق و صریح در مورد موضوع بازاریابی باید توسط تبلیغ کننده مشخص گردد. همانطور که از مفاد مواد بالا برداشت می‌گردد حق اطلاع از موضوع و اطلاعات تماسی توسط قانونگذار ما به صورت محدود و در قالب قواعد تبلیغ بیان شده است، در حالی که پیام ناخواسته محدود در تبلیغات نیست و از طرفی، این مقرره قانونی نمی‌تواند فقدان مدیریت ارسال پیام و جلوگیری از وقوع جرایم از طریق پیام ناخواسته را جبران کند.

نتیجه گیری

هدف از جرم‌انگاری ارسال پیام‌های الکترونیکی ناخواسته، مدیریت ارسال پیام و جلوگیری از وقوع جرایم در چنین بستری است. مقابله کیفری با این پدیده، چیزی فراتر از مجازات حبس و جزای نقدی است و آن جنبه عمومی دادن به آن از باب حمایت سریع و قاطع از حقوق مصرف کننده

است که تنها با جبران خسارت مدنی صرف برطرف نمی‌گردد؛ زیرا سهولت استفاده از این پدیده در انجام جرم صرفاً با اقدام مدنی، دارای بازدارندگی لازم نیست و نیازمند یک حمایت عمومی برای مقابله با این پدیده است.

میان جرم و ارسال پیام‌های الکترونیکی ناخواسته رابطه وجود دارد و این پیام‌ها علاوه بر جرم مستقل می توانند به عنوان یک وسیله مجرمانه یا جزء تشکیل‌دهنده در یک جرم مدنظر قرار گیرند. در این رابطه با توجه به ناکارآمد بودن سایر روش‌های مقابله با ارسال پیام ناخواسته و فقدان ضمانت اجرای لازم در صورت عدم رعایت آنها و همچنین وجود انگیزه‌های مجرمانه در ارسال این پیام‌ها، جرم‌انگاری ارسال پیام‌های الکترونیکی ناخواسته ضروری است؛ زیرا می‌تواند به عنوان یک جرم مانع از وقوع جرایم دیگر پیشگیری نماید.

ارسال پیام‌های ناخواسته منجر به ورود خسارت به اشخاص می‌شود. این خسارت می‌تواند ناشی از جرم یا نقض مقررات مدنی باشد. همچنین این پیام‌ها می‌تواند تهدید کننده حریم خصوصی افراد باشد و یا حقوق آنان را در تبادل پیام نادیده بگیرد. بنابراین، مصادیقی همچون ورود ضرر، نقض حریم خصوصی و نادیده گرفتن حقوق مصرف کننده می‌تواند به عنوان مبانی جرم‌انگاری ارسال پیام‌های ناخواسته مدنظر قانونگذار قرار بگیرد.

سیاست جنایی تقنینی ایران در رابطه با پیام‌های ناخواسته ناقص و محدود به ماده ۵۵ قانون تجارت الکترونیکی مصوب ۱۳۸۲ است و صرف ارسال پیام بدون محتوای مجرمانه در حال حاضر نمی‌تواند جرم باشد؛ زیرا هدف قانونگذار در این ماده صرف ارسال پیام نمی‌باشد، بلکه تنها عدم رعایت تمهیدات توسط تأمین کننده است. همچنین، این ماده نیز محدود به تبلیغات تجاری است و شامل سایر پیام‌ها نمی‌شود.

با توجه به ارسال پیام‌های الکترونیکی ناخواسته در ایران به‌ویژه در خصوص تلفن همراه و سوء استفاده مجرمان از این وسایل ارتباطی در ارتکاب جرایم، قوانین و مقررات در این رابطه کافی نیست و مستلزم وضع مقررات جدید می‌باشد. در حال حاضر، ارسال پیام صرفاً یک وسیله برای ارتکاب جرم است که تأثیری در وقوع جرم ندارد. بنابراین، به نظر می‌رسد نظر قانونگذار نسبت به ارسال این پیام‌ها باید از سطح وسیله فراتر رفته و خود نیز جرم‌انگاری گردد؛ زیرا جرم‌انگاری این موضوع مانعی برای ارتکاب جرایم دیگر همچون کلاهبرداری، سرقت هویت و اطلاعات و... است.

در وضع تدابیر کیفری توسط قانونگذار مصادیقی همچون ارسال پیام‌های ناخواسته انبوه دارای محتویات هرزه، فریبنده و جعلی، ارتکاب اعمال متقلبانه در ارسال پیام از قبیل جعل هویت، جعل اطلاعات سرپیام و موضوع پیام، تقلب در آدرس‌های الکترونیکی و نام دامنه و منشاء پیام‌ها، جمع آوری غیرقانونی آدرس‌ها و استفاده از نرم‌افزارهای خودکار آدرس‌های ساختگی می‌تواند به عنوان جرم مورد توجه قرار بگیرد.

منابع

الف) فارسی

۱. اصلانی، حمیدرضا، (۱۳۸۹)، حقوق فناوری اطلاعات، چاپ دوم، تهران: نشرمیزان.

۲. برکت، محیا، (۱۳۸۶)، نگاهی به وضعیت ارسال اس ام اس های تبلیغاتی: خط قرمز های فراموش شده، (گزارش اجتماعی)، روزنامه اعتماد، شماره ۱۴۹۴ به تاریخ ۸۶/۶/۲۷ ، ص ۸ .

۳. جلالی فراهانی، امیرحسین، (۱۳۸۵)، گزارش حریم خصوصی در فضای سایبر«حریم داده‌های الکترونیکی»، مرکز پژوهش‌های مجلس- معاونت پژوهشی- گروه ارتباطات و فناوری‌های نوین.

۴. جاویدنیا، جواد، (۱۳۹۲)، جرایم تجارت الکترونیکی، چاپ سوم، تهران: انتشارات خرسندی.

۵. حسنی، جعفر، (۱۳۸۵)، حمایت کیفری از حریم خصوصی در فضای سایبر، دانشکده حقوق، دانشگاه شهید بهشتی.

۶. خندانی، سید پدرام، (۱۳۸۵)، حمایت از حقوق مصرف‌کننده در قانون تجارت الکترونیکی مصوب ۸۲/۱۰/۱۷ با توجه به حقوق روز اتحادیه اروپا، دانشکده حقوق، دانشگاه شهید بهشتی.

۷. رجبی، اکرم، (۱۳۹۱)، نقض حریم خصوصی در فضای سایبر، چاپ اول، تهران: نشر آرمان.

۸. زندی، محمدرضا، (۱۳۸۹)، تحقیقات مقدماتی در جرایم سایبری، چاپ اول، تهران: انتشارات جنگل.

۹. عالی پور، حسن، (۱۳۹۰)، حقوق کیفری فناوری اطلاعات، چاپ اول، تهران: انتشارات خرسندی.

۱۰. فضلی، مهدی و باطنی، ابراهیم، (۱۳۸۸)، مقابلهٔ کیفری با پیام‌های ناخواستهٔ الکترونیکی (رویکرد جهانی، بایسته سنجی ملی)، *حقوق اسلامی*، سال ششم، شماره ۲۲، صص ۲۱۶-۱۸۳.

۱۱.گروه مطالعات و پژوهش‌های حقوق اقتصادی و بازرگانی، (۱۳۸۸)، اخلاق در تجارت الکترونیکی: رویکرد حمایت از حقوق مصرف‌کننده، چاپ اول، تهران: موسسه مطالعات و پژوهش‌های بازرگانی.

۱۲. مهرپور، حسین، (۱۳۷۴)، حقوق بشر در اسناد بین‌المللی و موضع جمهوری اسلامی ایران، چاپ اول، تهران: انتشارات اطلاعات.

ب) انگلیسی

1. Act on Regulation of the Transmission of Specified Electronic Mail, 2002.
2. Bahr, S (1998), No Stomach For Spam, America's Network, Vol. 102, Iss. 23,Usa.
3. Controlling the Assault of Non-Solicited Pornography and Marketing, Act (CAN-SPAM) 2003.
4. Canada'sAnti Spam Law,2010.
5. Geist, Michael (2005), *Untouchable? A Canadian Perspective On The Anti-Spam Battle*, University Of Ottawa Law And Technology Journal, Canada, Available At: (http://www.michaelgeist.ca/component/option,com_docman/task,doc_download/gid,5/).
6. Goodman, Danny (2004), Spam Wars: Our Last Best Chance To Defeat Spammers, Scammers, And Hackers, Selectbooks, New York.
7. Hallace Kikuchi, Erika (2004), Spam In A Box: Amending Can-Spam & Aiming Toward A Global Solution, *Journal Of Science & Technology Law*, Vol. 10.2, Boston University School Of Law, Summer, Pp 16-17.
8. John Beardwood And Gabriel M. A, Complying With Anti-Spam Legislation: A Cross-Jurisdictional View, Bulletin Technology & Intellectual Property, May 20, 2011. Available At: (Http://Www.Fasken.Com/En/Anti-Spam-Legislation-Comprehensive-Guide/).
9. Lottersberger, Andre (2003), Unsolicited Commercial Email-Overview On Possible Approaches Towards The Problem Of Spamming From An American And European Legal Perspective, University Of CAPE TOWN.
10. Lydia Pallas Loren, Regulating Cyberspace: A Case Study In Spam, Northwestern School Of Law Of Lewis And Clark College, In Learning Cyberlaw In Cyberspace, Aug. 1999. Available At: (http://www.cyberspacelaw.org/loren/index.html).
11. Metchis Hanah (2003), Singleton Solveig, Spam, That Ill O' The ISP:A Realitycheck For Legislators, Competitive Enterprise Institute, Washington.
12. Moustakas, Evangelos, Ranganathan, C,. Duquenoy, Penny, Combating Spam Through Legislation: A Comparative Analysis Of Us And European Approaches, Conference On Email And Anti-Spam - CEAS, 2005. Available

At:(Http://Pdf.Aminer.Org/000/085/114/Combating_Spam_Through_Legislation_A_Comparative Analysis_Of_Us_And.Pdf).
13. Ong, R.Y.C, Mobile Communication And The Protection Of Children, Leiden University Press, Netherlands, 2010.
14. Sorkin, David E, Technical And Legal Approaches To Unsolicited Electronic Mail, *University Of San Francisco Law Review*, Vol. 35, No 2, United States, 2001.
15. Scott, Jacob (2004), The Role Of Public Policy In The Fight Against Spam, Journal Of Engineering And Public Policy, *Washington Internships For Students Of Engineering*, Vol 8, August .
16. Sipior, J. C,. Ward, B. T,. Bonner, P. G (1998), The United States Responds To Spam, University Of Richmond School Of Law, 545, United States.
17. Tedre, Matti, Kamppuri, M, Kommers, P, An Approach To Global Netiquette Research Iadis International Web Based Communities, 2006. Available At:Http://Cs.Joensuu.Fi/~Ethno/Articles/Globalnetiquette_Iadis2006.Pdf. 2013/05/04.
18. Xingan, Li (2006), E-Marketing, Unsolicited Commercial E-Mail, And Legal Solutions, *Webology*, Volume 3, Iran, Number 1, March.