مقابلهٔ کیفری با پیام‌های ناخواستهٔ الکترونیکی

(رویکرد جهانی، بایسته‌سنجی ملی)

تاریخ دریافت: ۸۷/۷/۱۵ تاریخ تأیید: ۸۷/۸/۲۲

مهدی فضلی*
ابراهیم باطنی**

چکیده

پیام‌های ناخواسته (اسپم) که معمولاً با اهداف تجاری و به منظور تبلیغات از راه شبکه‌های رایانه‌ای یا مخابراتی به صندوق پُست الکترونیکی یا صندوق دریافت پیام افراد ارسال می‌شود، حجم زایدی از اطلاعات محسوب می‌شود که گاهی بیش از نود درصد پیام‌های الکترونیکی را شامل می‌شود. ارسال چنین پیام‌هایی برای مقاصد تبلیغاتی، از سویی هزینه‌های سنگینی را بر دوش نقش‌آفرینان فضای سایبر ـ به ویژه ارائه‌کنندگان خدمات ـ تحمیل می‌کند و از سوی دیگر، نقض حریم خصوصی و حق خلوت اشخاص محسوب می‌شود؛ در عین حال، ارسال پیام‌های ناخواسته برای تبلیغات، اکنون به یک تجارت سازمان‌یافته تبدیل شده است؛ به همین منظور استفاده از روش‌های متقلبانه و غیرقانونی برای جمع‌آوری آدرس پُست الکترونیکی افراد یا برای ارسال، دریافت و مشاهدهٔ چنین پیام‌هایی همچنان رو به رشد است. دو رویکرد عمده در میان دولت‌ها برای کنترل پیام‌های ناخواسته مشاهده می‌شود؛ یک رویکرد، ناظر بر عدم دخالت یا دخالت حداقلی دولت و کنترل از راه روش‌های فنی ـ آموزشی و رویکرد دوم، افزون بر روش‌های مزبور، ناظر بر کنترل از راه وضع و اِعمال قانون ـ اعم از کیفری و حقوقی ـ است. مقالهٔ حاضر در عین بررسی رویکرد جهانی در برخورد با پیام‌های ناخواسته، می‌کوشد بایستگی برخورد با آن از راه وضع قانون کیفری در کشورمان را بررسی کند.

واژگان کلیدی: *پیام‌های ناخواسته، اسپم، پُست الکترونیکی، حقوق کیفری.*

---

* پژوهشگر مرکز پژوهش‌های مجلس (mrmfazli@yahoo.com).
** دانشجوی دکتری حقوق جزا و جرم‌شناسی دانشگاه تهران (ebrahim.bateni@yahoo.com).

مقدمه

در مفهوم رایج، «اسپم» (Spam) واژه‌ای است که به پیام‌های الکترونیکی که بدون رضایت گیرندهٔ پیام و معمولاً به میزان زیاد ارسال می‌شود، اطلاق می‌گردد. از این‌گونه پیام‌ها به عنوان «پیام‌های الکترونیکی ناخواستهٔ توده‌وار»* نیز یاد می‌شود و از آنجا که بیشتر این پیام‌ها برای تبلیغ کالاها و خدمات به کار می‌رود، به آنها «پیام‌های الکترونیکی ناخواستهٔ تجاری»** نیز گفته می‌شود (Chissick et al., 2002, P. 4).***

اسپم به لحاظ تاریخی، ریشه در تبلیغات تجاری ناخواستهٔ خیابانی که به «fly posting» مشهور شده‌اند**** و نیز تبلیغات ناخواستهٔ کالاها که از راه تلفن یا فاکس (telemarketing) صورت می‌گیرد، دارد. با گسترش تبلیغات در فضای سایبر، پُست الکترونیکی افراد نیز از حجم گستردهٔ پیام‌های تبلیغی در امان نمانده است؛ با این حال، امروزه اسپم به خدمات پُست الکترونیکی محدود نیست و محتوای آن نیز فقط تبلیغات

---

* Unsolicited Bulk E-mail (UBE).

** Unsolicited Commercial E-mail (UCE).

*** واژهٔ Spam در واقع نام نوعی قوطی گوشت کنسروی است که ارتباطی با اسپم در معنای پیام‌های ناخواسته در معنای امروزی آن ندارد. گفته می‌شود که این واژه نخستین بار به‌وسیلهٔ گروه موسیقی و نمایشی «مانتی پیتون» بر سر زبان‌ها افتاد. این گروه در کافه‌ای به صورت همسرایی و به تکرار، این سرود را زمزمه می‌کردند: «اسپم، اسپم، اسپم». قوطی کنسرو اسپم شرکت Hormel Spiced Ham یکی از مهم‌ترین منابع غذایی سربازان انگلیسی در جنگ جهانی دوم به شمار می‌رفت و به نظر می‌رسد که گروه مانتی پیتون، سرمست از پیروزی متفقین در جنگ جهانی و تأثیر شگفت‌انگیز اسپم، سرود معروفشان را ساخته باشند. چهرهٔ اعتباری اسپم از «تکرار» این واژه در سرود گروه مانتی پیتون ناشی می‌شود؛ زیرا پیام‌های ناخواسته به صورت مکرر و در سطح گسترده ارسال می‌شوند (www.wikipedia.org/Spamming). فرهنگ تشریحی اصطلاحات کامپیوتری مایکروسافت در تعریف اسپم آورده است: «توزیع گستردهٔ موارد پُستی ناخواسته در اینترنت از طریق ارسال یک پیام به گیرندگان یا گروه‌های خبری بسیار زیاد...». البته شاخص تکرار و توزیع گستردهٔ اسپم همراه با شاخص کم‌هزینه‌بودن آن است؛ به همین دلیل فرهنگ مزبور در یک تعریف دیگر، اسپم را «استفادهٔ نادرست از اینترنت جهت توزیع یک پیام به شمار زیادی از اشخاص با کمترین هزینه» دانسته است (فرهنگ تشریحی اصطلاحات کامپیوتری مایکروسافت، ۱۳۸۱، ص ٦٩٤).

**** در ایالات متحده به این نوع تبلیغات غیرقانونی «Bandit Signs» یا «Street Spam» اطلاق می‌شود (http://en.wikipedia.org/wiki/Flyposting).

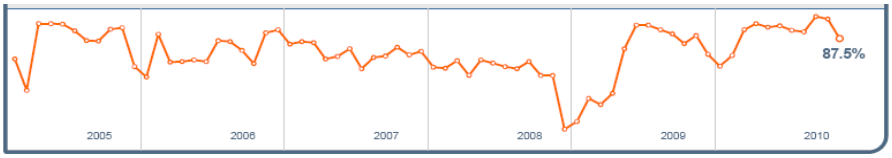
تجاری نیست. امروزه گروه‌های خبری مانند وبلاگ‌ها، محیط‌های گپ اینترنتی یا چَت، موتورهای جست‌وجو، پیام‌های تلفن‌های همراه و ابزار ارتباطی بی‌سیم دیگر نیز با پدیدهٔ اسپم مواجه‌اند. محتوای اسپم‌ها نیز علاوه بر تبلیغات تجاری، تبلیغات سیاسی، فرهنگی و هرگونه تبلیغات دیگر را شامل می‌شود (Encyclopedia of Privacy, 2007, P. 553). نخستین مورد جدی از ارسال اسپم در محیط‌های پُست الکترونیکی در ۱۲ آوریل ۱۹۹٤ گزارش شده است. «لورنس کانتر» (laurence canter)، وکیلی که دربارهٔ امور مهاجرت در ایالت آریزونای ایالات متحده فعالیت می‌کرد، برنامهٔ رایانه‌ای کوچکی تهیه کرد که به وسیلهٔ آن هزاران پیام را به تابلوهای پیام آنلاین می‌فرستاد و خدمات حقوقی مؤسسهٔ او را تبلیغ می‌کرد. جامعه نوپای اینترنت بلافاصله این اقدام او را مورد تقبیح قرار داد، ولی به‌رغم این انتقادها، کانتر ادعا کرد که تلاش‌های او برای بازاریابی در کارش موفق بوده، سود هنگفتی به همراه داشته است. ده سال پس از این واقعه، ارقام و آمار مربوط به اسپم تغییری جدی کرد (www.wikiedia.org/spamming).

ارسال‌کنندگان اسپم که بیشتر شرکت‌هایی‌اند که می‌خواهند با این ابزار ارتباطی کم‌هزینه، تبلیغی جهانی داشته باشند، اصراری ندارند که متن پیام‌های ارسالی آنها مورد مطالعه قرار گیرد. اینکه کاربری هر روز در صندوق پُستی خود فقط نام این شرکت‌ها را مشاهده کند، برای آنها که به دنبال شهرت و معروفیت در این بازار بزرگ مجازی‌اند، کافی است. اهمیت این موضوع آنقدر زیاد شده است که امروزه حرفهٔ اصلی برخی مؤسسات در سطح جهانی، جمع‌آوری آدرس‌های الکترونیکی و ارسال اسپم است؛ به گونه‌ای که به صورت سازمان‌یافته با دریافت مبالغی، میلیون‌ها اسپم را به صندوق پُست الکترونیکی کاربران در سراسر جهان ارسال می‌دارند. طبیعت آزاد و مبتنی بر آنارشیسم اینترنت و به‌خصوص وجود رایانه‌های کارگزار (سِرور) آزاد هم به راحتی اجازهٔ چنین فعالیت‌هایی را به آنان می‌دهد (Sullivan, 2003, P. 3).

با این حال، پرسش اینجاست که آیا به رغم همهٔ تأثیرات منفی اسپم در محیط‌های دیجیتال، ضرورتی به مداخلهٔ حقوق و به ویژه حقوق کیفری برای کنترل آن وجود دارد؟ آیا موضوع حمایت از محیط‌های دریافت پیام الکترونیکی آنقدر جدی است که قانون ـ آن هم قانون کیفری ـ خود را نیازمند به ورود در آن حیطه ببیند؟ یا این امر

باید از راه سازوکارهای دیگر غیرکیفری ـ و حتی غیرحقوقی ـ سامان یابد؟ مهم‌تر اینکه، آیا در کشور ما ضرورتی برای جرم‌انگاری ارسال پیام‌های ناخواسته وجود دارد؟ برای یافتن پاسخ این پرسش‌ها، در ذیل وضعیت آماری پیام‌های ناخواسته (۱)، رویکرد کلی کشورها در زمینهٔ مبارزه با پیام‌های ناخواستهٔ الکترونیکی (۲)، جرایم قابل ارتکاب از راه پیام‌های ارسالی(۳) و صِرف جرم‌انگاری ارسال پیام‌های ناخواسته (٤) را مورد بررسی قرار داده‌ایم و در نهایت بایستگی برخورد حقوقی و به ویژه کیفری با آن در کشورمان را مورد سنجش قرار داده‌ایم (۵).

۱. تأثیر پیام‌های ناخواسته بر جامعهٔ اطلاعاتی



این نمودار میزان فراز و نشیب اسپم را از اوایل سال ۲۰۰۵ تا پایان اکتبر ۲۰۱۰ به صورت سالانه در سطح جهانی به تصویر می‌کشد (messagelabs intelligence report, Nov 2010, P. 14). به جز اواخر سال ۲۰۰۸ و اوایل سال ۲۰۰۹ که ارسال پیام‌های ناخواسته به کمترین میزان خود در شش سال گذشته رسیده است، در بقیهٔ سال‌ها با یک نوسان مستمر در حال افزایش بوده است؛ به گونه‌ای که در آگوست سال ۲۰۱۰ به بالاترین سطح خود؛ یعنی ۹۲/۰۲ درصد از کل پیام‌های ارسالی در سراسر جهان رسیده است (messagelabs intelligence report, aug 2010, P. 9). در پایان اکتبر سال ۲۰۱۰، نرخ مزبور با کمی کاهش نسبت به ماه‌های قبل ۸۷/۵ درصد را نشان می‌دهد. گزارش ارائه‌شده در سال ۲۰۰۹ نیز میزان کلی اسپم را در این سال ۸۷/۷ درصد، با نرخ رشد ٦/۵ درصد نسبت به سال ۲۰۰۸ و به طور تخمینی روزانه ۱۰۷ میلیارد پیام ناخواسته ارسالی به آدرس پُست الکترونیکی اشخاص در سطح جهان نشان می‌دهد (messagelabs intelligence: annual security report, 2009, P. 7).

براساس گزارش شرکت سوفوس در سال ۲۰۱۰، از نظر جغرافیایی، ایالات متحده

همچنان در صدر ارسال‌کنندگان اسپم قرار دارد و پس از آن به ترتیب هند، برزیل و کرهٔ جنوبی قرار دارند (sophos security threat report, 2010, P. 21).

این حجم از ترافیک اطلاعات زاید ـ که گاهی بیش از نود درصد پیام‌های ارسالی را دربرمی‌گیرد ـ و افزایش هر سالهٔ تعداد کشورهایی که به عنوان مبادی عمدهٔ ارسال اسپم شناخته می‌شوند، بسیار تکان‌دهنده است. منابع جامعهٔ اطلاعاتی به هر میزان که باشند، باز هم محدودند و این حجم اطلاعات هرز و ناکارآمد، بر کارکرد آن تأثیر منفی زیادی دارد. مهم‌ترین تأثیر منفی اسپم بر اینترنت جهانی، مشغول‌شدن میزان عمده‌ای از پهنای باند کشوری و جهانی برای ترافیک اطلاعاتی زاید و نیز اختصاص‌یافتن حجم زیادی از فضای دیجیتال برای انتقال، پردازش و ذخیرهٔ این‌گونه پیام‌های هرز است (spam summit report, 2007, P. 2).

به لحاظ کاربر، طبق بررسی آماری در سال ۲۰۰۳، هر گیرندهٔ خدمات به طور متوسط از ۳ تا ۵ دلار اینترنتی از بابت اسپم متضرر شده است (Malik, 2003, P. 4). محتوای پیام‌ها نیز می‌تواند متضمن اطلاعاتی باشد که بر آنان ـ و مخصوصاً کاربران کودک ـ تأثیری منفی داشته باشد. پیامک‌های ارسالی به وسیلهٔ تلفن‌های همراه نیز تأثیری به مراتب بدتر از پیام‌های ارسالی در پُست الکترونیکی افراد دارند؛ زیرا معمولاً افراد به اتکای شرکت سرویس‌دهندهٔ مخابراتی خود که معمولاً شرکتی داخلی است، به پیام‌ها و تبلیغات ارسال‌شده راحت‌تر اعتماد می‌کنند؛ در حالی که محتوای برخی از آنها که فریبنده است، امروزه یکی از شگردهای نوین برای کلاهبرداری به شمار می‌آید.

اما عمده‌ترین هزینه‌های اسپم بر ارائه‌کنندگان خدمات ــ اعم از اینترنتی و مخابراتی ـ تحمیل می‌شود. علت عمدهٔ این هزینه‌ها، به خاطر تعهد ارائه‌کنندگان خدمات برای ارائهٔ خدماتی سالم به مشترکان خویش است. به‌کارگیری نرم‌افزارهای ضد اسپم و پالایش پیام‌های ناخواسته، هزینه‌های بسیاری را بر آنان تحمیل می‌کند. بر این امر باید هزینه‌هایی که ارائه‌کنندگان خدمات در برابر ترافیک اطلاعاتی زاید ناشی از ارسال اسپم ـ که گاهی به از کار افتادن رایانه‌های کارگزار و هزینهٔ مجدد برای راه‌اندازی آن منجر می‌شود ـ را نیز افزود. هزینه‌های سیستم، هزینه‌های پرداختی به پرسنل، هزینه‌های آموزشی و هزینه‌های پشتیبانی که ارائه‌کنندگان خدمات عرضه

می‌کنند، از جمله هزینه‌های ارسال اسپم است که بر آنان وارد می‌آیـد (Moustakas et al., 2003, P. 4).

اکنون اسپم به شکل سازمان‌یافته انجام می‌شود و سازمان‌هـایی بـدین‌منظـور شـکل گرفته‌اند که کار آنها فقط جمع‌آوری آدرس‌هـای پُسـت الکترونیـک کـاربران، خریـد و فروش آنها و ارسال اسپم است. این مؤسسه‌ها بسیاری از اسپم‌ها را بـا انجـام اقـدامات متقلبانه یا مخفی‌داشتن هویت رایانه‌هایی که از راه آن به ارسال اسـپم اقـدام مـی‌کننـد، انجام می‌دهند تا بدین وسـیله عملیـات شناسـایی آنهـا غیـرممکن شـود یـا بتواننـد بـا فریب‌دادن و گمراهکردن گیرندگان پیام‌ها به اهداف خود که مشاهدهٔ پیام است، دسـت یابند (Moustakas et al., 2005, P. 7).

به رغم همهٔ تأثیرهای منفی پیام‌های ناخواسته که پیش‌تر به آنها پرداختیم، هنوز این پدیده طرفدارانی دارد. موافقان ارسال اسپم، با توجه به اصل آزادی گـردش اطلاعـات، معتقدند ارسال اسپم یک حق و از لوازم آزادی بیان و آزادی نشـر اطلاعـات اسـت کـه باید محترم شمرده شود. این دسته معتقدند تبلیغـات از راه پیـام‌هـای الکترونیکـی باعـث رونق و شکوفایی تجارت و به ویژه تجارت الکترونیکی می‌شـود (Wayne, 2001, P. 9). مخالفان ارسال اسپم، عدم رضایتِ گیرندگان پیام‌ها و نقض حـریم خصوصـی افـراد را ملاک قرار می‌دهند و بیان می‌دارند بسـیاری از گیرنـدگان پیـام‌هـا بـه عنـوان کـاربران خدمات اینترنتی و مخابراتی رضایتی به دریافـت اسـپم ندارنـد و ایـن عـدم توجـه بـه رضایت آنها، بی‌احترامی به حق خلوت آنهاسـت کـه از منظـر اخـلاق سـایبر وحقـوق کاربران، مطرود است و باید مشمول منع قانونی قرار گیرد (Stacy, 2003, P. 463).

۲. رویکرد دولت‌ها در مبارزه با اسپم

برای مبارزه با اسپم در سطح جهانی، به طور مشخص، دو رویکرد به وسـیلهٔ دولـت‌هـا قابل تشخیص است:

۱ـ۲. عدم لزوم وضع مقررات مستقل

این دیدگاه از قضیهٔ ارسال اسپم به وسیلهٔ کانتر در سال ۱۹۹٤ به این سو شکل گرفت و

تا اوایل سال ۲۰۰۰ همچنان ادامه داشت و هنوز هم در کشورهایی که تـأثیر کمتـری از اسپم می‌گیرند، طرفداران فراوانی دارد. این دیدگاه نگرانی چندانی نسبت به تأثیر اسـپم بر محیط اینترنت و تجارت الکترونیک ندارد و معتقد است دست‌انـدرکاران اینترنـت و از جمله ارائه‌کنندگان خدمات خود، پاسخ مناسـبی بـرای ایـن مسـئله خواهنـد یافـت. براساس این رویکرد، اسپم فقط یک «مزاحمت» عادی در محیط اینترنت است؛ بنابراین نیازی به وضع مقررات در این حوزه وجود ندارد. از آنجا که تاکنون بسیاری از کشورها در سطح جهان مقرره‌ای مستقل برای کنترل اسپم وضع نکرده‌اند، این دیـدگاه همچنـان دیدگاه غالب محسوب می‌شود. تأکید این دیدگاه بر آن است که باید با تشویق و ایجـاد بازار رقابت میان ارائه‌کنندگان خـدمات اینترنتـی در ارائـهٔ راهکارهـای فنـی، از جملـه روش‌های پالایش (فیلترینگ) کوشید و در نهایت با استفاده از تضـمین‌هـای قـراردادی همچون بستن حساب پُست الکترونیکی ارسـال‌کننـدگان اسـپم و مسـدودکردن سـایت اینترنتی آنها در صورت تخلف، اِعمال مقررات موجـود مربـوط بـه حـریم خصوصـی، روش‌های جبران خسارت مدنی و نیـز اِعمـال قـوانین کیفـری موجـود دربـارهٔ جـرایم رایانه‌ای، تقلب و کلاهبرداری، جرایم مرتبط با محتوا، جرایم مربـوط بـه نقـض حـریم خصوصی افراد و مانند آن که به وسیلهٔ پیام‌های ناخواسته صورت می‌گیرد، با اسـپم بـه مبارزه پرداخت.* در این میان، تأکید بر روش‌های فنی ـ آموزشی به وسیلهٔ ارائه‌کنندگان خدمات اینترنتی و مخابراتی اسـت و سـازمان‌هـای دولتـی نیـز مـی‌تواننـد بـه عنـوان هماهنگ‌کننده بر اقدامات ارائه‌کنندگان خدمات، نظارت داشـته باشـند.** از نظـر ایـن دیدگاه، دولت باید کمترین نقش را برای حل مشکل اسـپم داشـته باشـد و ایـن بخـش

* تا زمان تصویب قانون Can-Spam Act در ایـالات متحـده، برخـی از دعـاوی کیفـری مطروحـه بـا موضوع ارسال اسپم جهت ارتکاب تقلب و سوء استفاده‌های مالی در ایـن کشـور، براسـاس قـوانینی چون «قانون تقلب و سوء استفاده از رایانـه» (Computer Fraud and Abuse Act) و قـوانین موجـود جرایم رایانه‌ای ایالات این کشور طرح شده، به نتیجه هم رسیده بود. در کانادا نیز براساس کد کیفری این کشور، برخی از دعاوی در رابطه با جرایم مرتبط بـا محتـوا مطـرح و منتهـی بـه صـدور حکـم محکومیت ارسال‌کنندهٔ اسپم شده است (Geist, 2005, P. 15).

** برای نمونه، کمیسیون تجارت فدرال FTC در ایالات متحده تا قبل از تصـویب قـانون Can-Spam در این کشور در سال ۲۰۰۳ چنین نقشی داشت و پس از تصـویب ایـن قـانون نیـز رسـماً عهـده‌دار بسیاری از امور مربوط به کنترل اسپم شده است.

خصوصی است که با «خودمقرره‌زایی» (self-regulation) به جـای «وضـع مقـرره از بـالا» (over-regulation) و به‌کارگیری کدهای رفتاری (codes of conduct)، باید راهکـاری برای حل این مشکل بیابد. روش‌های فنی مکمل در کنـار پـالایش چـون ارائـهٔ گزینـهٔ اذن پیشینی یا اولیه (opt-in) به کاربران، به این معنا که کـاربر بایـد قبـل از واردشـدن پیـام بـه صندوق پستی‌اش، اجازهٔ ورود پیام را بدهد و نیز روش اجازهٔ پسینی یا ثانویه (opt-out) که پیام تا زمان اعلام عدم رضایت صریح کاربر همچنان به وی ارسال خواهـد شـد نیـز از جمله روش‌های فنی است (Geist, 2005, P. 7-8).

ارائه راهکارهای آموزشی به کاربران خدمات پُست الکترونیکی نیز شامل مواردی مانند ترغیب به استفاده از نرم‌افزارهای آنتی‌اسپم، بالابردن آگاهی عمومی آنان نسبت به روش‌های ارتکاب جرایم و به‌خصـوص سوءاسـتفاده‌هـای مـالی، تقلـب و کلاهبـرداری و همچنـین پاسخ‌ندادن به پیام‌های ناخواسته و گزارش به مراجع قضایی اسـت کـه مـی‌توانـد در کنـار روش‌های فنی برای کنترل اسپم مفید باشد؛ به عنـوان مثـال، براسـاس قـانون Can-Spam ایالات متحده، کمیسیون تجارت فدرال (FTC) «federal trade commission» مسـئول دریافت شکایت‌های مربوط به اسپم و رسیدگی به آنها و طرح شکایت نـزد مقـام‌هـای قضایی است و از زمان این مسئولیت، روزانه هزاران پیام اسپم که کاربران آنها را بـرای پیگیری به این کمیسیون ارسال کرده‌اند، دریافت کـرده اسـت (spam summit report, 2007, P. 4).

۲ـ۲. وضع مقررات مستقل و همکاری‌های بین‌المللی

گروه‌های مبارزه‌کننده با اسپم، از سال ۱۹۹۵ تلاش خود را برای وضع مقرراتی خـاص آغاز کردند، ولی در بسیاری کشورها تا سال‌ها اقدامات آنان چنـدان مـورد توجـه قـرار نگرفت؛ برای نمونه، در ایالات متحده اقدامات کنگرهٔ این کشور برای وضع قانون ضـد اسپم در سال‌های ۱۹۹۸ و ۱۹۹۹ با ارائـه طـرح‌هـایی ماننـد «قـانون حـریم خصوصـی صندوق دریافت نامه‌ها» (inbox privacy bill)، با انتقادهای زیادی که بر آن وارد شـد، عملاً مسکوت ماند تا اینکه سرانجام در سال ۲۰۰۳ قانون Can-Spam در سطح فـدرال به تصویب رسید. البته پیش از تصویب قانون مزبور، در ۳۶ ایالت این کشـور مقرراتـی

خاص در این باره وضع شده بود (Blanke, 2004, P. 4).

تصویب مقرراتی خاص دربارهٔ اسپم، از سال ۲۰۰۰ تاکنون در کشورهای دیگر نیز روندی رو به رشد داشته است. رویّهٔ کشورها در مبارزه با اسپم از راه وضع مقررات خاص نیز متفاوت بوده است. از این میان، کشورهایی که قانونی مستقل در این باره دارند یا دست کم موادی قانونی را در درون قوانین دیگر خود پیش‌بینی کرده‌اند، برخی ضمانت اجراهای کیفری را برای نقض مقررات مصوب وضع کرده‌اند و برخی دیگر ضمانت اجراهای مدنی مانند خسارت‌های قانونی و طرح دعوا برای جبران خسارت‌ها را پیش‌بینی کرده‌اند. برخی کشورها نیز تلفیقی از هر دو ضمانت اجرا را برگزیده‌اند.

افزون بر این، با توجه به طبیعت جهانی اینترنت، برخی کشورها به وضع مقررات مستقل در این باره اکتفا نکرده، همکاری‌های بین‌المللی را نیز آغاز کرده‌اند. اکنون کشورهای ایالات متحده و کانادا در شمال قارهٔ امریکا، در دو بُعد طرح دعوا برای گرفتن خسارت‌ها و ارائهٔ دعاوی حقوقی، همکاری خویش را آغاز کرده‌اند. همین امر در روابط دو کشور استرالیا و کرهٔ جنوبی به صورت دوسویه آغاز شده است و این دو کشور یادداشت تفاهمی را برای توسعهٔ و بهبود مقررات در اکتبر سال ۲۰۰۳ امضا کرده‌اند. ایالات متحده و انگلستان همچنین بیانیهٔ مشترکی را در این باره در دسامبر سال ۲۰۰۳ صادر کرده‌اند، ولی دربارهٔ اجرای قانون کیفری یکسان، هنوز مشکلات مربوط به صلاحیت در محیط آنلاین و ناهماهنگی قوانین کیفری وجود دارد (Geist, 2005, P. 10).

اقدامات برخی سازمان‌های بین‌المللی نیز در این باره اهمیت دارد؛ از جملهٔ این اقدامات می‌توان به تشکیل اجلاسی بین‌المللی در فوریه ۲۰۰٤ به وسیلهٔ «سازمان همکاری و توسعهٔ اقتصادی» (OECD) و اجلاسی دیگر به وسیلهٔ «اتحادیهٔ بین‌المللی ارتباطات راه دور» (ITU)* در ماه مِی سال ۲۰۰٤ اشاره کرد. از موارد دیگر همکاری میان دولت‌ها، برگزاری کنفرانسی در ژانویه ۲۰۰٤ برای به‌کارگیری راهکارهایی برای کاهش اسپم با استفاده از «رایانه‌های کارگذار (سِرور) آزاد» (open relay servers)

* International Telecommunication Union.

است که ارسال بیش از شصت درصد اسپم‌ها به وسیلهٔ آنها صورت می‌گیرد. استفاده از روش‌های مؤثر برای مقابله با پولشویی توسط سازمان‌های دلال ارسال اسپم یا خرید و فروش آدرس‌های پُست الکترونیکی نیز راهکاری است که به وسیلهٔ دولت‌ها برای مسدودکردن منابع مالی ارسال‌کنندگان اسپم به صورت سازمان یافته مورد توجه قرار گرفته است (Geist, 2005, P. 10).

۳. جرم‌انگاری ارسال پیام‌های ناخواسته با محتوای مجرمانه

دولت‌ها در مبارزه با اسپم از راه اِعمال قانون کیفری نیز دو رویکرد گوناگون اِعمال کرده‌اند. تعدادی از آنان صِرف ارسال اسپم را جرم ندانسته‌اند و در صورتی که محتوای پیام ارسالی متضمن مطالب، محتویات یا نرم‌افزارهای غیرقانونی باشد، براساس قوانین موجود مربوط به جرایم عمومی یا جرایم رایانه‌ای با آن به مقابله برخاسته‌اند، ولی برخی کشورها مقررات موجود را کافی نمی‌دانند و مقررات کیفری ویژه‌ای برای صِرف ارسال اسپم (اسپمینگ) وضع کرده‌اند. بیشتر جرایمی که از راه محتوای پیام‌های ناخواسته الکترونیکی قابل ارتکاب‌اند را در ذیل با بررسی مختصر قوانین کیفری کشورمان مورد تحلیل قرار داده‌ایم.

۱ـ۳. جرایم مالی

از میان جرایم مالی، کلاهبرداری (تقلب مالی) اعم از رایانه‌ای و غیررایانه‌ای، گسترده‌ترین و شایع‌ترین جرم مالی (و گاهی اقتصادی) است که در بسیاری موارد از راه فضای سایبر و ارسال پیام‌های ناخواسته صورت می‌گیرد (spam summit report, 2007, P. 14). البته باید توجه داشت که هرگونه کلاهبرداری به وسیلهٔ ارسال پیام کلاهبرداری رایانه‌ای نیست، بلکه حسب مورد می‌تواند رایانه‌ای یا غیررایانه‌ای و مستقیم یا غیرمستقیم باشد.* با این حال، ارتکاب این‌گونه کلاهبرداری‌ها از راه فضای سایبر، لزوماً باعث

* مادهٔ ۱ قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری مصوب ۱۳٦۷ ارتکاب کلاهبرداری «با استفاده از تبلیغ عامه از طریق وسایل ارتباط جمعی از قبیل رادیو، تلویزیون، روزنامه و مجله یا نطق در مجامع و یا انتشار آگهی چاپی یا خطی» را مورد توجه قرار داده است و آن را از دلایل تشدید مجازات دانسته است.

نمی‌شود این نوع کلاهبرداری را رایانه‌ای بنامیم (عالی‌پور، ۱۳۸۳، ص ۱٦۸).

تقلبات مالی از راه اسپم در فضای سایبر، بیشتر از نوع اول یعنی غیررایانه‌ای است که می‌توان با عنوان تقلب از راه سوءاستفاده از اعتماد دیگران در فضای سایبر یا Confidence Fraud گرد آورد.* بیشتر کلاهبرداری‌ها نخست با کسب اطلاعات مالی افراد آغاز می‌شود. روش‌های موسوم به «مهندسی اجتماعی»** که بیشتر از راه محیط‌های گپ یا پُست الکترونیکی برای اغفال افراد با تلاش برای ارتباط‌گرفتن با آنان و تخلیهٔ اطلاعات خصوصی مالی آنها یا «سرقت هویت» (identity theft) صورت می‌گیرد ـ از جمله «شگرد یا ترفند نیجریه‌ای» (nigerian scam) ـ از راه اسپم، بسیار شایع است.*** «شگرد لاتاری» (Lottery Scam) گونهٔ دیگری از این روش‌هاست، به طوری که با ارسال پیامی به مخاطب، بیان می‌شود که وی مقادیر کلانی پول را در قرعه‌کشی اینترنتی شرکت‌های معتبری چون Microsoft یا Google برنده شده است و باید برای دریافت آن مبلغ، اطلاعات حساب بانکی خود را ارسال کند یا مقادیری پول برای انجام هزینه‌های ارسال مبلغی که برنده شده است، از وی درخواست می‌شود. هر روزه شگردهای مهندسی اجتماعی نوینی در فضای سایبر مورد استفاده بزهکاران قرار

* عنوان مزبور یکی از انواع تقلب‌های مالی است که توسط مرکز دادخواهی جرایم اینترنتی (Internet Crime Complaint Center) در ایالات متحده امریکا ارائه شده است (www.ic3.gov).

** مهندسی اجتماعی «Social Engineering» واژه‌ای به ظاهر فنی است که ابتدا در نوشته‌های فلسفی قرن بیستم و به ویژه در آثار کارل پوپر به کار برده شد و در دنیای رایانه و اینترنت در قالب معنایی به کار می‌رود که اساساً با معنای لغوی آن همخوانی ندارد. حملات مهندسی اجتماعی در واژگان رایانه‌ای عبارت است از روند نفوذ به سیستم‌های رایانه‌ای از طریق کاربرد حیله‌های گوناگون نسبت به افراد جهت افشای کلمات عبور و اطلاعات مربوط به موارد آسیب‌پذیر شبکه (فرهنگ تشریحی اصطلاحات کامپیوتری مایکروسافت، ۱۳۸۱، ص ٦۸۸).

*** در یکی از ترفندهای مرسوم نیجریه‌ای، ارسال‌کنندهٔ پیام اظهار می‌دارد که خود یا یکی از بستگانش دارای مقادیر فراوانی پول در حساب بانکی در یک کشور (معمولاً افریقایی)اند و چون به دلیل غضب دولت وقت نمی‌توانند آن را از حساب خویش خارج سازند و استفاده کنند، نیازمند کمک شخص دیگری در خارج از کشورند و از مخاطب می‌خواهند یک شمارهٔ حساب بانکی در اختیار آنان قرار دهد و با تطمیع بزهدیده به وی قول می‌دهند که نیمی از مبلغ مزبور در صورت خروج از کشور متعلق به وی خواهد بود. با این روش بزهدیده فریب می‌خورد و با دادن اطلاعات حساب بانکی، موجودی حساب بانکی‌اش به یغما می‌رود (The “Nigerian” Scam: Costly Compassion, 2003, P. 3).

می‌گیرد (Recognizing and Avoiding Email Scams, 2008). ارسال چنین پیام‌هایی از راه تلفن همراه کاربران، به واسطهٔ اعتبار بیشتری که پیام‌های تلفن همراه نسبت به پیام‌های پُست الکترونیکی دارد، می‌تواند بیشتر باعث اغفال آنان شود.* روشن است از نظر حقوق کیفری، ارسال چنین پیام‌هایی تا به نتیجه‌ای منجر نشده است، در مرحلهٔ اقدامات مقدماتی یا شروع به جرم کلاهبرداری قرار دارد.

تبصرهٔ ۲ مادّهٔ ۱ قانون تشدید مجازات مرتکبان ارتشاء، اختلاس و کلاهبرداری، شروع به کلاهبرداری غیررایانه‌ای را جرم‌انگاری کرده است؛ با این حال، این موضوع که آیا ارسال اسپم برای دریافت اطلاعات مالی افراد، قسمتی از عملیات مادی جرم (مانور متقلبانه) است و شروع به کلاهبرداری غیررایانه‌ای محسوب می‌شود یا فقط مقدمات جرم است و نه شروع به جرم، می‌تواند محل اختلاف باشد. با توجه به اینکه شروع به جرم کلاهبرداری رایانه‌ای در قانون جرایم رایانه‌ای جرم‌انگاری نشده است، تلاش برای گرفتن اطلاعات از راه اسپم که برای ارتکاب کلاهبرداری رایانه‌ای قابل استفاده است، نمی‌تواند شروع به جرم کلاهبرداری رایانه‌ای باشد، مگر اینکه بتوان به نوعی آن را با عنوان کیفری دیگری، همچون دریافت غیرمجاز اطلاعات خصوصی دیگران، تطبیق داد. دریافت اطلاعات خصوصی افراد، از جمله اطلاعات مربوط به حساب بانکی آنها همزمان می‌تواند جزء جرایم علیه حریم خصوصی افراد باشد. البته به دلیل عدم تصویب، لایحه حریم خصوصی تاکنون در کشور ما مستند قانونی نیافته است.

* مادّهٔ ۵۸ قانون تجارت الکترونیکی بیان می‌دارد: «ذخیره، پردازش و یا توزیع "داده‌پیام"های شخصی مبیّن ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و "داده‌پیام"های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آنها به هر عنوان غیرقانونی است» و مجازات تخلف از مقررات این مادّه را در مادّهٔ ۷۱ این قانون، یک تا سه سال حبس تعیین کرده است؛ با این حال، این قانون دربارهٔ دستیابی به داده‌های خصوصی و حساس افراد، تصریحی ندارد. مادّهٔ ۱ قانون جرایم رایانه‌ای نیز فقط به دسترسی غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی اختصاص دارد که به وسیلهٔ تدابیر امنیتی حفاظت شده‌اند و تا این شرایط فراهم نباشد، چنین مواردی را دربرنمی‌گیرد.

۲ـ۳. جرایم علیه تمامیت داده‌ها و سیستم‌های رایانه‌ای

ارسال اسپم می‌تواند یکی از روش‌هایی باشد که تمامیت و قابلیت دسترسی داده‌ها و سیستم‌های رایانه‌ای را به خطر بیاندازد. جرایم علیه اطلاعات و نیز جرایم علیه سیستم‌های رایانه‌ای را می‌توان در سه دسته کلی طبقه‌بندی کرد:

ـ از میان‌بردن، ایجاد اختلال، غیرقابل پردازش یا غیرقابل دسترس‌کردن داده‌ها؛

ـ ایجاد اختلال در کارکرد سیستم‌ها و شبکه‌های رایانه‌ای؛

ـ انتشار برنامه‌های مخرب و مختل‌کننده.

ایجاد اختلال در کارکرد سیستم‌های رایانه‌ای، در واقع ناظر به حالتی است که کارکرد سیستم‌های رایانه‌ای با اختلال مواجه شده‌اند یا سیستم‌ها به طور کلی از کار می‌افتند که از آن جمله می‌توان به حملات (DoS) «denial of service attacks» و حملات گسترده‌تر آن (DDoS) «distributed denial of service attacks» اشاره کرد (فضلی، ۱۳۸۳، ص ۱۷۹ـ۱۸۳). برخی از این حملات با ارسال اسپم در مقادیر بسیار زیاد به رایانهٔ گارگذار ارائه‌کنندهٔ خدمات صورت می‌گیرد که به از کارافتادن سیستم‌های رایانه‌ای وی منجر می‌شود. اسپم همچنین می‌تواند حاوی یکی از نرم‌افزارهای مخرب چون کرم، ویروس یا بمب‌های منطقی باشد که از راه پیام‌های الکترونیکی به سیستم‌های رایانه‌ای یا مخابراتی افراد ارسال می‌شود. از نمونهٔ این ویروس‌ها می‌توان به ویروس Good Times اشاره کرد (Brenton, et al., 2002, P. 263-264).

جرایم مربوط به از میان‌بردن، اخلال یا غیرقابل دسترس‌ساختن داده‌ها و سیستم‌های رایانه‌ای در مواد ۸ تا ۱۱ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ جرم‌انگاری شده‌اند. بند (الف) مادهٔ ۲۵ این قانون نیز «تولید، انتشار یا توزیع یا معامله» داده‌ها یا نرم‌افزارها یا هر نوع ابزار الکترونیکی که «فقط» به منظور ارتکاب جرایم رایانه‌ای به کار می‌روند را جرم‌انگاری کرده است. روشن است اگر پیام ناخواسته متضمن یکی از داده‌ها و نرم‌افزارهایی باشد که «فقط» به منظور ارتکاب جرایم رایانه‌ای به کار می‌روند و این پیام از راه پُست الکترونیکی «منتشر یا توزیع» شده باشد، مشمول آن بند خواهد شد. قانون مزبور ضابطه‌ای برای «انتشار یا توزیع» ارائه نمی‌دهد و بیان نمی‌کند که چند مورد ارسال یا پخش، مصداق توزیع و انتشار است. با این حال، قدر متیقن این است

که «در دسترس‌گذاشتن» داده‌ها یا نرم‌افزارهای مزبور به این معنا که فقط به یک نفر ارائه شده باشد، از شمول آن بند خارج خواهد بود.

۳ـ۳. جرایم علیه محرمانگی اطلاعات و سیستم‌های رایانه‌ای

پیام‌های ناخواسته، همان‌گونه که ناخواسته وارد پُست الکترونیکی کاربران می‌شوند، با بازکردن پُست الکترونیکی، به طور ناخواسته در سیستم آنها نیز نصب می‌شوند و اطلاعات مربوط به آنان را به مهاجم ارسال می‌کنند. نمونه‌های بسیاری از تروا‌ها و پایش‌افزارهای مشهور به وسیلهٔ پیام‌های ناخواسته به سیستم‌های رایانه‌ای افراد وارد و در آنجا نصب شده‌اند و اطلاعات خصوصی و محرمانهٔ را به مهاجمان ارسال کرده‌اند. حملات مهندسی اجتماعی که پیش‌تر در جرایم مالی به آنها اشاره شد، جرایمی است که علیه اطلاعات خصوصی مالی افراد ارتکاب می‌یابد و در بسیاری موارد پیام‌های ارسالی، روشی برای دستیابی به این اطلاعات است. البته روشن است، تا زمانی که این اقدامات به دریافت اطلاعاتی منجر نشده است، در مرحلهٔ شروع به جرم قرار دارد که با توجه به جرم‌نبودن دریافت اطلاعات خصوصی در کشورمان، شروع به جرم آن نیز جرم نخواهد بود.

در قانون جرایم رایانه‌ای مصوب ۱۳۸۸، جاسوسی در مادّهٔ ٤ و تولید، انتشار، توزیع، معامله داده‌ها یا نرم‌افزارها و یا هر نوع ابزار الکترونیکی که فقط به منظور ارتکاب جرایم رایانه‌ای به کار می‌روند و نیز فروش یا انتشار یا در دسترس قراردادن گذرواژه یا هر داده‌ای که امکان دسترسی غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی متعلق به دیگری را فراهم می‌کند، به ترتیب در بندهای (الف) و (ب) مادّهٔ ۲۵ مورد جرم‌انگاری قرار گرفته‌اند. با این حال، مواد موصوف، ارسال پیام ناخواسته برای دریافت اطلاعات سرّی و خصوصی برای دسترسی به سیستم‌های رایانه‌ای را دربرنمی‌گیرند؛ زیرا این امر خود در نهایت، شروع به جرم دریافت اطلاعات خصوصی یا محرمانه است که در قوانین ما جرم نیست، مگر اینکه این کار از راه «انتشار یا توزیع» نرم‌افزارهای تروا یا پایش‌افزارها به وسیلهٔ پیام‌های الکترونیکی صورت گیرد که در این صورت، ذیل بند (الف) مادّهٔ ۲۵ قانون مذکور قرار خواهد گرفت و آن نیز فقط ناظر بر

جاسوسی مذکور در مادّهٔ ٤ آن قانون که در این قانون به عنوان جرم رایانه‌ای جرم‌انگاری شده است، خواهد بود، ولی ارسال اسپم برای دریافت اطلاعات محرمانه و خصوصی افراد را که به عنوان جرم رایانه‌ای جرم‌انگاری نشده است، شامل نمی‌شود؛ بنابراین اگر اطلاعات مزبور به وسیله تدابیر امنیتی حفاظت شده باشد، در این صورت دسترسی به چنین اطلاعاتی از راه ارسال تروا و پایش‌افزار به پُست الکترونیکی افراد می‌تواند مشمول مادّهٔ ۱ قانون جرایم رایانه‌ای قرار گیرد.

۴ـ۳. جرایم مرتبط با محتوا

جرایم مرتبط با محتوا «content related crimes» در مفهوم گسترده، ناظر به دسته‌ای از جرایم‌اند که به وسیلهٔ محتوا یا مطالب رایانه‌ای ارتکاب می‌یابند (عالی‌پور، ١٣٨٤، ص ١٦٥). مقررات کیفری موجود دربارهٔ جرایم مربوط به نشر مطالب غیرقانونی که قانون مجازات اسلامی و دیگر قوانین کیفری، ارسال آنها از راه اسپم را پوشش می‌دهد، فراوان‌اند؛ مواردی مانند تبلیغ علیه نظام (مادّهٔ ٥٠٠)، در اختیارگذاردن اطلاعات سیاست داخلی و خارجی به افراد فاقد صلاحیت، به گونه‌ای که متضمن جاسوسی باشد (مادّهٔ ٥٠١)، مواد مربوط به تحریک افراد نیروهای مسلح به عصیان، فرار، تسلیم یا عدم اجرای وظایف نظامی (مادّهٔ ٥٠٤)، توهین به مقدسات (مادّهٔ ٥١٣)، توهین به رهبری (مادّهٔ ٥١٤)، توهین به افراد و کارکنان دولت (مواد ٦٠٨ و ٦٠٩)، تهدید و اکراه (مواد ٦٦٨ و ٦٦٩)، افترا (مادّهٔ ٦٩٧) و هجو (مادّهٔ ٧٠٠)، در قانون مجازات اسلامی از آن جمله‌اند. مواد گوناگونی از قوانین پراکندهٔ خاص همچون مادّهٔ ۱ قانون مجازات تبلیغ تبعیض نژادی مصوب ١٣٥٦ دربارهٔ نشر هر نوع افکار مبتنی بر تبعیض براساس نژاد یا جنس و نفرت نژادی و یا تحریک به تبعیض براساس نژاد و یا جنس، به وسیلهٔ یکی از وسایل‌تبلیغ عمومی علیه هر گروه که از جهت نژاد، جنس، رنگ و قومیت متفاوت باشند نیز در این باره وجود دارند که به فضای واقعی محدود نیستند و فضای سایبر را نیز پوشش می‌دهند.*

* دربارهٔ قانون اخیر که وسایل تبلیغ عمومی را مورد اشاره قرار داده است، باید توجه داشت که پُست الکترونیکی و کوته‌پیام، اساساً وسیله‌هایی برای تبلیغ یا ارتباط عمومی محسوب نمی‌شوند، بلکه یک

با توجه به نقص قوانین سنّتی، قانون جرایم رایانه‌ای نیز دربارهٔ جرایم مرتبط با محتوا که از راه فضای سایبر ارتکاب می‌یابند، موادی را پیش‌بینی کرده است. تولید، ارسال، انتشار، توزیع یا معاملهٔ محتویات مستهجن و مبتذل یا نگهداری، تولید و ذخیرهٔ آنها به قصد ارسال، انتشار یا تجارت (مادّهٔ ١٤)، تحریک، ترغیب، تهدید، تطمیع یا فریب افراد برای دستیابی آنان به محتویات مستهجن یا مبتذل و یا تسهیل و آموزش روش دستیابی به آن محتویات (بند «الف» مادّهٔ ١٥)، تحریک، ترغیب، تهدید، دعوت یا فریب افراد برای ارتکاب جرایم منافی عفت یا استعمال مواد مخدر و روان‌گردان، خودکشی، انحرافات جنسی یا اَعمال خشونت‌آمیز یا تسهیل و آموزش روش ارتکاب آنها (بند «ب» مادّهٔ ١٥)، هتک حیثیت افراد با تغییر فیلم، صوت یا تصویر دیگری و انتشار آن یا انتشار آن با علم به تغییر و تحریف (مادّهٔ ١٦)، انتشار یا در دسترس‌گذاردن صوت یا تصویر و یا فیلم خصوصی یا خانوادگی یا اسرار دیگری بدون رضایت او به گونه‌ای که منجر به ضرر یا عرفاً باعث هتک حیثیت او شود (مادّهٔ ١٧) و نشر اکاذیب و اظهارات خلاف واقع (مادّهٔ ١٨)، موادی از قانون مزبورند که به جرایم مرتبط با محتوا می‌پردازند و حسب مورد، ارسال پیام‌های حاوی این مطالب را پوشش می‌دهند.

۴. جرم‌انگاری صِرف ارسال پیام‌های ناخواسته

آیا صِرف ارسال پیام ناخواسته نیز باید جرم باشد؟ آیا ارسال اسپم، حتی اگر متضمن

ابزار ارتباط خصوصی ـ همچون تلفن ـ هستند؛ بنابراین قسمت اخیر مادّهٔ مزبور، ابزارهای خصوصی ارسال پیام را دربرنمی‌گیرد.

برخی از جرایمی که پیش‌تر به آنها اشاره شد، در واقع در ردیف جرایم علیه امنیت ملی قرار می‌گیرند؛ با این حال، از نظر محتوا می‌توان آنها را در ردیف جرایم مرتبط با محتوا نیز قرار داد. برخی از جرایم همچون افشای اسرار خصوصی یا تجاری (مادّهٔ ٦٤ قانون تجارت الکترونیکی) یا سوء استفاده از علایم تجاری یا نام‌های دامنه (مادّهٔ ٦٦ قانون تجارت الکترونیکی)، نقض مقررات تبلیغ آنلاین (مادّهٔ ٧٠ قانون تجارت الکترونیکی) و نقض حقوق مالکیت فکری (براساس قانون حمایت حقوق مؤلفان، مصنفان و هنرمندان مصوب ١٣٤٨/٩/٣ و قانون ترجمه و تکثیر کتب و نشریات و آثار صوتی مصوب ١٣٥٢/٩/٢٦ و قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای مصوب ١٣٧٩/١٠/٤ و نیز مادّهٔ ٧٤ قانون تجارت الکترونیکی) و قوانین دیگر نیز از راه ارسال پیام‌های ناخواسته، قابل ارتکاب‌اند که باید مورد توجه قرار گیرند.

محتوایی مجرمانه نباشد نیز جرم است؟ آیا جرایم دیگری در جهت صِرف ارسال اسپم ـ صرف‌نظر از محتوای آن ـ قابل تصور است؟ با مختصر نگاه تطبیقی به مقررات کشورهای دیگر می‌توان جرایم ذیل را در ارتباط با صِرف ارسال اسپم شناسایی کرد:

۱. ارسال پیام‌های الکترونیکی ناخواسته، بدون توجه به رضایت گیرندهٔ پیام (اعم از رضایت اولیه opt-in یا ثانویه opt-out)؛
۲. اقدامات متقلبانه در جهت ارسال پیام‌های الکترونیکی ناخواسته؛
۳. جمع‌آوری غیرقانونی آدرس‌های الکترونیکی یا قراردادن آن در دسترس دیگران؛
٤. عدم رعایت مشخصات شکلی در پیام ارسالی.

۱ـ۴. ارسال پیام بدون رضایتِ گیرنده

در منع ارسال پیام‌های الکترونیکی ناخواسته، چند مسئله واجد اهمیت است: اولاً، چه پیام‌هایی باید مشمول ممنوعیت قرار گیرند؟ ثانیاً، ارسال پیام‌های غیرقانونی در چه تعدادی ممنوع است؟ ثالثاً، رضایت گیرندهٔ پیام در این باره چه نقشی دارد؟

۱ـ۱ـ۴. پیام‌های الکترونیکی ممنوعه

بررسی قوانین کشورهای گوناگون نشان می‌دهد که تقریباً بیشتر آنها فقط ارسال پیام‌های الکترونیکی تجاری را که به تبلیغ کالاها و خدمات تجاری می‌پردازند، ممنوع کرده‌اند و از این جهت ارسال بسیاری از انواع پیام‌های ناخواسته همچون پیام‌های دارای تبلیغات سیاسی و نیز پیام‌هایی که برای امور عام‌المنفعه یا مانند آن ارسال می‌شود، از شمول قوانین مربوطه خارج است. البته چنانچه بیان شد، این امر مورد انتقاد قرار گرفته است (Arora, 2006, P. 8-9).

۲ـ۱ـ۴. تعداد پیام الکترونیکی

برای جرم‌انگاری صِرف ارسال اسپم، برخی کشورها نصابی را مشخص کرده‌اند. ایالات متحده در قانون Can-Spam این میزان را «صد پیام پُست الکترونیک در ٢٤ ساعت، بیش از هزار پیام پُست الکترونیک در سی روز یا بیش از ده هزار پیام پُست الکترونیک در یک سال» دانسته است (Fingerman, 2004, P. 10). اتریش نیز در قانون ارتباطات

«telecommunication act» مصوب ۲۰۰۳، این تعداد را پنجاه پیام تعیین کرده است، ولی برخی کشورها مانند ایتالیا، حد نصابی را تعیین نکرده‌اند.

۳ـ۱ـ۴. رضایت گیرندهٔ پیام

چنانچه پیش‌تر بیان شد، به اعتقاد برخی، ارسال پیام بدون توجه به رضایت گیرندهٔ آن، مغایر با «حریم خصوصی» و «حق خلوت» (right to be alone) وی تلقی می‌شود، هرچند برخی دیگر این امر را مخالف حق آزادی بیان و آزادی نشر اطلاعات می‌دانند. این رضایت ممکن است «رضایت پیشینی یا اذن» باشد که به آن Opt-in اطلاق می‌شود؛ یعنی ارسال‌کنندهٔ پیام باید قبل از ارسال پیام به گیرنده، رضایت وی را در این باره بگیرد و یا اینکه «رضایت پسینی یا اجازه» باشد که به آن Opt-out گفته می‌شود و بدین معناست که در صورتی که مخاطب پیام از ارسال‌کنندهٔ پیام نخواهد پیامی دیگر ارسال کند، این امر رضایت ضمنی وی در دریافت پیام‌های بعدی محسوب می‌شود.* کشور ایتالیا آنقدر برای مسئلهٔ رضایت پیشینی گیرندهٔ پیام اهمیت قائل است که براساس مادهٔ ۱۳۰ «قانون حمایت از اطلاعات شخصی» (personal data protection code) مصوب ۲۰۰۳، بدون توجه به تعداد پیام ارسالی، ارسال حتی یک پیام را نیز بدون توجه به رضایت گیرندهٔ پیام، ممنوع و مستوجب کیفر دانسته است. با این حال، کشوری مانند ایتالیا در این باره یک استثناست.

۲ـ۴. اقدامات متقلبانه در جهت ارسال پیام‌های الکترونیکی ناخواسته

این اقدامات در دو دسته به ترتیب ذیل قرار می‌گیرند:

* سیستم opt-in بیشتر به نفع گیرندهٔ پیام است و مسئولیت گرفتن رضایت و نیز اثبات مسئلهٔ گرفتن رضایت، در صورت بروز اختلاف را بر عهدهٔ ارسال‌کنندهٔ پیام می‌گذارد، در حالی که سیستم opt-out، هم به نفع ارسال‌کنندهٔ پیام و هم به نفع تبلیغات در تجارت الکترونیک است و مسئولیت اعلام عدم رضایت و اثبات آن در صورت بروز اختلاف را بر عهدهٔ گیرندهٔ پیام می‌گذارد. ایالات متحده سیستم رضایت پسینی را در قانون Can-Spam اعمال کرده است. براساس گزارش کمیسیون تجارت فدرال (FTC) در سال ۲۰۰۷، از زمان تصویب این قانون تا آن سال، حدود سی دعوی توسط آن نهاد در مراجع قضایی مطرح شده است که حدود هشتاد درصد آنها به عدم تحصیل رضایت پسینی (اجازه) در ارسال اسپم محدود بوده است (spam summit report, P. 7).

۱ـ۲ـ۴. قلب هویت (spoofing)

«spoofing» در لغت به معنای فریب‌دادن، جازدن و وانمودسازی است و می‌توان آن را «قلب هویت، جعل هویت یا جازدن و وانمودسازی متقلبانه» نیز نامگذاری کرد. از جهت اصطلاحی، تعاریف گوناگونی از spoofing ذکر شده است. spoofing محدود به ارسال پیام‌های الکترونیکی نیست و در تعریف عام در فضای سایبر عبارتست از نسبت‌دادن عملی به شخصی دیگر، به گونه‌ای که شخص متقلب طوری وانمود کند که اقدامات از جانب آن شخص صورت گرفته است؛ به عنوان مثال، در IP spoofing، از نشانی IP یک کاربر دیگر برای دستیابی به یک کامپیوتر یا شبکه استفاده می‌شود (فرهنگ تشریحی اصطلاحات کامپیوتری مایکروسافت، ۱۳۸۱، ص ٦٩٧).

در ارسال پیام‌های ناخواستهٔ الکترونیکی، با این کار، آدرس فرستندهٔ نامه الکترونیکی قلب می‌شود، به گونه‌ای که منشأ اسپم مخفی می‌ماند و چنین وانمود می‌شود که پیام از یک منبع قانونی شناخته‌شده ارسال شده است. به این کار «spoofing email» اطلاق می‌شود. طبق تعریف «سازمان توسعه و همکاری اقتصادی» (OECD) در سال ۲۰۰۵، spoofing email عبارتست از تغییر منشأ نرم‌افزاری نامه‌های الکترونیکی به گونه‌ای که نشانگر صدور نامه از یک منبع صحیح و قانونی باشد. این اقدام معمولاً از سوی ارسال‌کنندگان اسپم برای ترغیب دریافت‌کنندگان اسپم به دادن پاسخ به کار می‌رود (OECD task force on spam report, 2005, P. 7). واژه munging گاهی با spoofing اشتباه می‌شود، در حالی که منظور از آن این است که شخص در نامه‌هایی که به یک وبگاه عمومی (همچون گروه خبری) می‌فرستد، آدرس خود را (یعنی آنچه در قسمت فرستنده یا from نوشته می‌شود) طوری مخدوش کند که اگر یک نفر از آن استفاده کند و به آن، پیامی ناخواسته ارسال کند، این نامه متضمن اسپم هرگز به دست طرف مقابل نمی‌رسد؛ زیرا آدرس ارسالی صحیح نخواهد بود، پس munging برای مقابله با ارسال پیام‌های ناخواسته و به عنوان یک اقدام ضداسپم به کار می‌رود (نِد، ۱۳۸۰، ص ۲۸۳). تقلب در ارسال پیام‌های الکترونیکی در چند شکل گوناگون قابل ارتکاب است:

۱ـ۱ـ۲ـ۴. تقلب در اطلاعات نمایه (header information) پیام

در تعریف کلی، «اطلاعات نمایه» هرگونه اطلاعات ارائه‌شده در آغازِ مجموعه‌ای از داده‌ها و اطلاعاتی است که ارائه یا ذخیره شده باشند. این داده‌ها و اطلاعات ممکن است بسته‌های داده (data packets)، فایل‌های گرافیکی یا زبان‌های برنامه‌نویسی باشند. به اطلاعاتی که در پی اطلاعات نمایه ارائه می‌شود «اطلاعات بدنه یا پیکره» (body یا payload) اطلاق می‌شود. اطلاعات نمایه به پیام الکترونیک محدود نیست، ولی در پیام‌های پُست الکترونیکی، اطلاعات نمایه اطلاعاتی است که نشانگر شخص ارسال‌کننده، گیرنده، موضوع پیام، زمان ارسال، زمان دریافت و آخرین کارگزاران (سرویس‌دهندگان) انتقال‌دهندهٔ نامه «final mail transfer agents» و مانند آن است.* بسیاری از ارسال‌کنندگان اسپم برای آنکه نرم‌افزارهای پویش «scan» و پالایش «filter» پیام نتوانند آنها را رصد، شناسایی و متوقف کنند، با تقلب در اطلاعات نمایهٔ پیام، به گونه‌ای وانمود می‌کنند که پیام از راه یک آدرس الکترونیکی قانونی (فرضاً با ذکر نام یکی از دوستان کاربر به عنوان ارسال‌کنندهٔ پیام) به مخاطب ارسال شده است.

۲ـ۱ـ۲ـ۴. تقلب در اطلاعات موضوع پیام (subject line)

چنانچه بیان شد، اطلاعات موضوع پیام، خود قسمتی از اطلاعات نمایهٔ پُست الکترونیکی یا هر پیام الکترونیکی دیگر است که بیانگر محتوای آن پیام است. ارسال‌کنندگان اسپم با قلب موضوع پیام ارسالی که خود راه‌های گوناگونی دارد؛ اولاً، باعث می‌شوند پیام از کمند نرم‌افزارهای پویش و پالایش بگریزد و به دست گیرندهٔ پیام برسد؛ ثانیاً، باعث می‌شوند گیرنده‌ای که پیام را دریافت می‌دارد به آنها اطمینان کند، پیام را بگشاید و مورد مشاهده قرار دهد؛ برای مثال، اگر موضوع نامهٔ یک پُست الکترونیکی ارسالی ظاهراً نشانگر ارسال کارت تبریک الکترونیکی و در باطن، متضمن برنامه‌های مخرب باشد، در این صورت ارسال‌کنندهٔ پیام هویت واقعی موضوع پیام را قلب کرده، کاربر را فریب می‌دهد تا محتوای پیام را ببیند.**

* http://en.wikipedia.org/wiki/Header_information_technology.

** در سال ۲۰۰۷، کمیسیون تجارت فدرال (FTC) در پروندهٔ Jumpstart Technologies ادعا کرد که

۳ـ۱ـ۲ـ۴. تقلب در آدرس الکترونیکی یا نام دامنهٔ دیگران

ارسال‌کنندگان پیام پُست الکترونیکی ناخواسته گاهی برای مخفی نگه‌داشتن هویت واقعی خود، از آدرس الکترونیکی یا نام‌های دامنهٔ مشروع دیگران استفاده می‌کنند. این امر معمولاً برای گریز از کمند پویش و پالایش پیام‌های الکترونیکی ناخواسته صورت می‌گیرد. آدرس الکترونیکی یا نام دامنهٔ آدرس الکترونیکی از اجزای اطلاعات نمایه است و ارسال‌کنندهٔ پیام با ارسال آنها طوری وانمود می‌کند که پیام به وسیلهٔ یک آدرس الکترونیکی قانونی به او ارسال شده است.*

مشتکی‌عنه به دروغ در عنوان پیام، ارسال بلیط‌های رایگان را درج کرده بود، در حالی که بلیط‌ها واقعاً رایگان نبود. حتی کاربرانی که این پیام را حذف می‌کردند تا هفته‌ها همچنان آن پیام را دریافت می‌داشتند. مرتکب، به پرداخت نهصد هزار دلار جریمه محکوم شد (FTC v. Jumpstart Technologies, 2006). در پرونده‌ای مشابه، شرکت Adteractive برای ارسال پیام‌هایی مبنی بر فروش رایگان کالا در قسمت موضوع پیام، در حالی که در متن پیام‌ها کالاها دارای قیمت بودند، محکوم شد (FTC v. Adteractive, 2007).

* شایان ذکر است که قسمتی از آدرس پُست الکترونیکی افراد، نشانگر نام دامنه یا نام قلمرو پُست الکترونیکی آن شخص در اینترنت است. هر آدرس پُست الکترونیکی از سه قسمت تشکیل شده است: نام مشترک، نام دامنه و پسوند نام دامنه؛ به عنوان مثال، آدرس پُست الکترونیکی ali@yahoo.com دارای سه قسمت است: نام مشترک پُست الکترونیکی (ali) که به آن قسمت محلی یا مکانی (local part) گفته می‌شود؛ نام دامنه (domain part) یا قلمروی که نمایانگر موقعیت رایانهٔ کارگزار ثبت‌کنندهٔ حساب پُست الکترونیکی آن کاربر در اینترنت است. در آدرس مثالی مذکور، ارائه‌دهندهٔ این خدمات که رایانهٔ کارگذار را در اختیار دارد، yahoo است که خدمات پُست الکترونیک را به مشترک ارائه داده است و پسوند com که نشانگر نوع قلمرو نام دامنه و نمایانگر اختصاری سه حرف اول واژهٔ commercial یا تجاری است. این آدرس نشان می‌دهد که ali بر روی یکی از رایانه‌های کارگزار (کامپیوتر سِرور) ارائه‌کنندهٔ خدمات yahoo، دارای یک حساب پُست الکترونیکی است که امکان دریافت، ذخیره و ارسال پیام الکترونیکی را به وی می‌دهد. نام دامنه ممکن است توسط یک ثبت‌کنندهٔ نام دامنهٔ ملی یا بین‌المللی ثبت شود. نام‌های دامنه در دید کاربران اینترنتی به صورت الفبایی است، ولی آدرس الفبایی مذکور برای رایانه یک عدد به حساب می‌آید. این عدد، عددی همچون 194.72.244.100 است که نمایانگر یک پروتکل اینترنتی (IP) است و برای تسهیل کار رایانه‌ها که با عدد سازگارترند، ایجاد شده است. در واقع آدرس مزبور نمایانگر رایانهٔ کارگذاری در اینترنت است که نشان می‌دهد آن مشترک بر روی آن رایانه حساب پُست الکترونیکی دارد. به همین دلیل ترکیب، ظاهراً الفبایی و در واقع عددی است که به آدرس‌های اینترنتی «الفبا عددی» (alphanumeric) اطلاق می‌شود (فرهنگ تشریحی اصطلاحات کامپیوتری مایکروسافت، ۱۳۸۱، ص ۲۴۵).

۴ـ۱ـ۲ـ۴. تقلب در IP رایانهٔ منشأ پیام الکترونیکی

در این حالت نیز ارسال‌کنندهٔ پیام الکترونیکی با قانونی جلوه‌دادن IP رایانه‌ای که پیام ابتدا از آن ارسال شده است، به گونه‌ای وانمود می‌کند که پیام از رایانه‌ای قانونی ارسال شده است تا نرم‌افزارهای پویشگر و پالایشگر نتوانند براساس لیست سیاه موجود IP رایانه‌های غیرقانونی که رایانه‌های کارگذار آنها را در اختیار دارد، آن پیام را متوقف سازند. از عمدهٔ ترفندهایی که برای مخفی نگه‌داشتن منشأ پیام صورت می‌گیرد، استفاده از رایانه‌های دیگران با استفاده از نرم‌افزارهایی مخصوص به نام روبوت‌های ارسال پیام است که به رایانهٔ میزبان وارد می‌شود و از آنجا به رایانهٔ کارگزاری که به عنوان مرکز «فرمان و کنترل» عمل می‌کند، دسترسی می‌یابد و از توسط آن به ارسال اسپم اقدام می‌کند. در بسیاری موارد قربانیان از اینکه سیستم آنها وسیله‌ای برای ارسال اسپم شده است، آگاهی ندارند که این موضوع مصداق آشکار تجاوز به حریم خصوصی آنها محسوب می‌شود. قانون Can-Spam ایالات متحده، عدم دریافت رضایت در این باره را جرم‌انگاری کرده است.*

از روش‌های دیگر برای مخفی نگه‌داشتن IP رایانهٔ مبدأ می‌توان به استفاده از «رایانه‌های کارگزار آزاد ارسال پُست الکترونیک» (open email relaying servers) اشاره کرد. اکنون فشار جامعهٔ جهانی و به‌خصوص کشورهایی که بیشتر با مشکل اسپم مواجه‌اند، این است که دارندگان رایانه‌های کارگزار، ارسال پُست الکترونیکی آنها را تحت کنترل دقیق قرار دهند و در حد امکان نسبت به جمع‌آوری آنها اقدام شود.**

* در پروندهٔ FTC علیه Dugger، شرکت مزبور به خاطر ارسال پُست الکترونیکی تجاری دارای محتوای آشکار جنسی، با استفاده از رایانهٔ کارگذار دیگران، بدون رضایت و آگاهی آنها محکوم شد (FTC v. William Dugger, 2006).

** عمدهٔ تبعاتی که این روش به همراه دارد، عبارت‌اند از: عدم دریافت پیام‌های ارسال‌شده از این رایانه‌ها توسط گیرنده، به این دلیل که این رایانه‌ها در لیست سیاه قرار دارند و رایانهٔ گیرندهٔ پیام، این پیام‌ها را دریافت نمی‌کند و این امر به ضرر افرادی است که به صورت قانونی فعالیت می‌کنند، کاهش اعتبار ارائه‌کنندگان خدمات اینترنتی که از چنین رایانه‌هایی استفاده می‌کنند، به اتهام عدم کنترل دقیق بر رایانه‌هایشان، کاهش اعتبار ارائه‌کنندگان خدمات اینترنتی به این دلیل که ارسال‌کنندگان اسپم نام کاربر یا صندوق پستی را در دامنهٔ (domain) آنها جعل می‌کنند، قطع خدمات به کاربر با این اتهام که وی از دامنهٔ خود اسپم ارسال می‌کند یا اجازهٔ ارسال اسپم را از دامنهٔ خود

۵ـ۱ـ۲ـ۴. تقلب در مرجع ثبت آدرس الکترونیکی

در چنین مواردی ارسال‌کنندگان اسپم خود را مرجعی که خدمات ارسال پیام ـ همچون خدمات پُست الکترونیکی ـ ارائه می‌دهد، معرفی می‌کنند و مشترکان با ثبت آدرس پُست الکترونیکی خود در آن مرجع، آدرس پُست الکترونیکی خود را در اختیار ارسال‌کنندگان اسپم قرار می‌دهند؛ غافل از اینکه ارسال‌کنندگان اسپم ممکن است از آن آدرس برای ارسال پیام‌های پُست الکترونیکی سوءاستفاده کنند.

۲ـ۲ـ۴. جمع‌آوری غیرقانونی آدرس‌های الکترونیکی (address harvesting)

ارسال‌کنندگان اسپم برای آنکه بتوانند پیام‌های تبلیغاتی خود را به دیگران ارسال کنند باید آدرس‌های پُست الکترونیکی معتبر و در مقادیر فراوان در اختیار داشته باشند. به دست آوردن آدرس‌ها یا به اصطلاح «جمع‌آوری و گردآوری» چنین آدرس‌هایی برای آنان حیاتی است. در بسیاری مواقع این کار را شرکت‌هایی که کارشان فقط یافتن، جمع‌آوری و فروش آدرس‌های پُست الکترونیکی است، انجام می‌دهند. گردآوری آدرس‌های معتبر الکترونیکی به راه‌های گوناگونی صورت می‌گیرد و ارسال‌کنندگان اسپم با استفاده از نرم‌افزارهای خاص یا به وسیلهٔ پاسخ‌دادن کاربر به پیام متوجه می‌شوند که آدرس الکترونیکی موجود همچنان معتبر است یا خیر. یافتن آدرس‌های پُست الکترونیکی افراد نیز معمولاً به وسیلهٔ «روبوت‌های جستجوگر» (explorer robots) آدرس پُست الکترونیکی صورت می‌گیرد. در برخی موارد ممکن است جمع‌آوری آدرس‌های الکترونیکی و امتحان اعتبار آنها از راه «حملات دیکشنری» (dictionary attacks) صورت گیرد. حملهٔ دیکشنری یکی از تکنیک‌هایی است که هرچند فقط به وسیلهٔ ارسال‌کنندگان اسپم مورد استفاده قرار نمی‌گیرد، ولی برای جمع‌آوری آدرس‌های ایمیل بسیار مورد استفاده قرار می‌گیرد. در این حمله، ارسال‌کنندهٔ اسپم (اسپَمِر) به صورت اتفاقی «random» میلیون‌ها پیام را به آدرس‌هایی فرضی ارسال می‌کند؛ به عنوان مثال، اگر نامی همچون John را در نظر بگیریم که ممکن است احتمالاً آدرسی متضمن نام وی جزء آدرس‌های ثبت‌شده

می‌دهد و نیز مشکلات پی‌جویی و یافتن منشأ ارسال پیام (برای مطالعهٔ بیشتر ر.ک به: Michael McCafferty, 2002, P. 2-3).

به وسیلهٔ ارائه‌کنندهٔ خدمات پُست الکترونیک «یاهو» باشد، مهاجم به ارسال پیام در مقادیر بسیار زیاد به آدرس‌های فرضی با ترتیب خاص مانند: john1984@yahoo.com, john_1983@yahoo.com, john_1982@yahoo.com و مانند آن اقدام می‌کند؛ زیرا احتمال دارد شخصی به نام John سال تولد خود را به همراه نام خود به عنوان آدرس پُست الکترونیکی‌اش ثبت کرده باشد. البته این حملات به وسیلهٔ رایانه‌ها و نرم‌افزارهای مخصوصی که بدین‌منظور طراحی شده‌اند، صورت می‌گیرد. بدین‌ترتیب، هریک از این پیام‌ها با آدرس‌های فرضی را می‌توان مانند تیری دانست که به وسیلهٔ ارسال‌کننده در تاریکی رها می‌شود؛ به این امید که یکی از میلیون‌ها تیر رهاشده به صورت اتفاقی به هدف برخورد کند. آنچه بیشتر ارسال‌کنندگان اسپم را در موفقیت در این حمله امیدوار می‌کند، آن است که بیشتر کاربران آدرس‌های پُست الکترونیکی خود را معمولاً از نام کوچک، نام فامیل، سال تولد یا ترکیبی از آنها می‌سازند و این موضوع احتمال موفقیت آنها را زیاد می‌کند؛ بنابراین این حملات را باید جزء حملاتی دانست که برای جمع‌آوری آدرس پُست الکترونیکی اشخاص (email harvesting, email gathering) صورت می‌گیرد. پیام‌های ارسالی کدی دارند که در صورتی که واقعاً چنین آدرسی موجود باشد، رسیدن پیام به گیرنده را به ارسال‌کنندهٔ اسپم اطلاع می‌دهند تا وی مجدداً برای ارسال پیام از آن آدرس‌ها استفاده کند. این حمله‌ها منابع رایانه‌های کارگذار را برای پردازش هر پیام ارسالی و تطبیق برای وجود یا عدم وجود چنین آدرسی به خود مشغول می‌کند. البته باید توجه داشت که حملات دیکشنری، مخصوص یافتن آدرس پُست الکترونیکی افراد نیست و در واقع در کنار حملات Brute Force برای یافتن گذرواژهٔ افراد و رمزیابی نیز مورد استفاده قرار می‌گیرند.*

۳ـ۲ـ۴. عدم رعایت مشخصات شکلی در پیام ارسالی

قوانین برخی کشورها شرایطی شکلی را برای ارسال‌کنندگان پیام‌های ناخواستهٔ تبلیغاتی مقرر کرده‌اند. هرچند بیشتر کشورها عدم رعایت این شرایط را مستوجب کیفر نمی‌دانند، ولی برخی کشورها مانند ایالات متحده، استثنائاً عدم رعایت این شرایط را در

* http://www.webopedia.com/TERM/D/dictionary_attack.html.

برخی موارد، جرم‌انگاری کرده‌اند. این شرایط عبارت‌اند از:

۱ـ۳ـ۲ـ۴. مشخصات ارسال‌کنندهٔ پیام و ذکر آدرس تماس برگشت (return address)

براساس قوانین برخی کشورها، ارسال‌کنندهٔ پیامی که براساس قانون به ارسال پیام تجاری اقدام می‌کند، باید هویت خود را به طور دقیق اعلام کند و حتی آدرس فیزیکی خود را نیز در پیام درج کند. در برخی کشورها ذکر «آدرس برگشت» مانند آدرس پُست الکترونیکی که گیرندهٔ پیام را به تماس با ارسال‌کنندهٔ پیام قادر سازد، لازم دانسته شده است. این موضوع در کشورهایی که سیستم Opt-out را برای اعلام عدم رضایت دریافت پیامی دیگر به وسیلهٔ گیرندهٔ پیام پذیرفته‌اند، ضروری است.

۲ـ۳ـ۲ـ۴. نصب برچسب به پیام (labeling)

در برخی کشورها قانونگذار ذکر عبارت‌ها، علایم یا اشکالی را در پیام ضروری دانسته است که پیش از اینکه پیام گشوده شود و به وسیلهٔ گیرندهٔ پیام مورد مشاهده قرار گیرد، نمایانگر محتویات آن باشد. این موضوع در پیام‌هایی مانند پیام‌های متضمن محتوای مستهجن که برای کودکان مناسب نیست، ضروری است تا کودکان از آسیب‌های محتوای چنین پیام‌هایی در امان باشند. برای چنین پیام‌هایی برچسب‌هایی همچون عبارت ADLT که مخفف عبارت Adult به معنای «بزرگسالان» است و نشان می‌دهد که محتوای پیام فقط برای بزرگسالان مناسب است، لازم است و نقض این شرایط گاهی مجازاتی به میزان مجازات انتشار یا ارائهٔ محتویات مستهجن دارد. همچنین برای پیام‌های تجاری و تبلیغاتی، نصب برچسبی مانند واژهٔ ADV که مخفف عبارت «advertisement» است، لازم دانسته شده است تا کاربر و مشترکی که نمی‌خواهد محتوای آن پیام‌ها را بخواند، با مشاهدهٔ آن برچسب آن را مشاهده نکند و یا حذف کند. چنین برچسب‌هایی این مزیت را برای کاربران و مشترکان دارد که بدون اینکه وقت خود را تلف کنند یا هزینه‌ای اضافی برای مشاهدهٔ پیام‌ها بپردازند، بلافاصله آنها را حذف کنند.*

* یکی از اتهامات شرکت Dugger که به آن اشاره شد، علاوه بر استفاده از رایانه‌های دیگران برای ارسال پیام، ارسال پیام‌های دارای محتوای آشکار جنسی، بدون نصب برچسب بود (spam summit report, P. 10).

۵. رویکرد ایران

با توجه به مطالب پیش‌گفته، پرسش جدی دربارهٔ رویکـرد کشـور مـا در بـه‌کـارگیری سیاستی برای مبارزه با صِرف ارسال اسپم مطرح می‌شود و آن اینکه آیا به رغم گسترش ارتباطات الکترونیکی در ایران و نیز افزایش میزان پیام‌های ناخواسـته، هنـوز ضـرورتی جدی برای وضع مقررات جهت کنترل اسپم ـ به ویژه مقررات کیفری ـ وجود دارد؟

مادّهٔ ۵۵ قانون تجارت الکترونیکی دربـارهٔ تنظـیم قواعـد تبلیـغ در بسـتر ارتباطـات الکترونیکی، اشعار می‌دارد: «تأمین‌کنندگان باید تمهیداتی را بـرای مصـرف‌کننـدگان در نظر بگیرند تا آنان دربارهٔ دریافت تبلیغات به نشانی پُستی و یا پُست الکترونیکـی خـود تصمیم بگیرند». مادّهٔ ۷۰ و تبصرهٔ ۲ آن قانون نیـز تـأمین‌کننـدهٔ متخلـف را بـه حـداقل مجازات مندرج در مادّهٔ ۷۰ یعنی یکصد میلیون ریال (ظاهراً جزای نقدی) محکوم کرده است.** بند «ع» مادّهٔ ۲ این قـانون، «تـأمین‌کننـده» (supplier) را عبـارت از شخصـی دانسته است که بنا به اهلیت تجاری، صنفی یا حرفه‌ای فعالیت می‌کنـد. اگـر «دریافـت پیام‌های تبلیغی» را با اندکی مسامحه «دریافت تبلیغـات» بـدانیم، ایـن امـر تبلیـغ از راه پُست الکترونیکی را هم دربرخواهد گرفت. با این حال، از مجموع مواد پیش‌گفته و بـه ویژه مادّهٔ ۵۵ که نشانی فیزیکی را نیـز در کنـار پُسـت الکترونیکـی ذکـر کـرده اسـت، مشخص می‌شود که اولاً، این مادّه بـه ارسـال اسـپم از راه پُسـت الکترونیکـی محـدود نیست؛ ثانیاً، به تبلیغات تجاری محدود است و پیام‌هـای دیگـر تبلیغـی ماننـد تبلیغـات سیاسی را دربرنمی‌گیرد؛ ثالثاً، ارسال پیام به وسـیلهٔ ابزارهـای الکترونیکـی دیگـر ماننـد

شایان ذکر است که مبارزه با اسپم به لحاظ طبیعت جهانی اینترنت باید با همکاری دولت‌ها صـورت گیرد و صِرف راهکارهای داخلی، حتی وضع قوانین کیفری کوبنـده پاسـخگو نیسـت. ایـن امـر نیازمند بسترسازی حقوقی جهت همکاری با کشورهای دیگـر اسـت کـه مـی‌تـوان بـا تصـویب توافقنامه‌های دوجانبه و چندجانبه، آن را آغاز کرد؛ به عنوان مثال، ایـالات متحـده در پرونـدهٔ FTC علیه (Spear Systems, Inc) براساس قانون (Safe Web Act) علیه ارسال‌کننـدگان اسـپم از کانـادا و استرالیا اقدام کرد. (FTC v. Spear Systems, Inc., 2007).

** قانون مزبور تصریحی در اینکه این مبلغ جزای نقدی است یا جریمه‌ای است که به خـاطر تخلـف گرفته می‌شود، ندارد. به کاربردن عبارت «تخلف» در مادّه، برداشت دوم را تأیید می‌کند، ولی فحوای مادّه و اینکه عنوان آن باب قانون (باب چهارم) که این مادّه در آنجا آمده «جرایم و مجازات‌ها»ست و بیشتر بر جزای نقدی‌بودن آن تأکید دارد.

تلفن همراه را پوشش نمی‌دهد؛ رابعاً، براساس مادّهٔ ۵۵، ارسال پیام ناخواسته، آزاد و قانونی است و قانون فقط تأمین‌کننده (تبلیغ‌کننده) را موظف می‌سازد که دربارهٔ گرفتن رضایت کاربر برای دریافت پیام، تمهیداتی را بیندیشند؛ به گونه‌ای که اگر وی به دریافت پیام از راه پُست الکترونیکی خود مایل نباشد، بتواند با اعلام به تأمین‌کننده، مجدداً پیام دریافت نکند. چنانچه بیان شد، این روش در اظهار برای عدم ارسال پیام‌های ناخواسته، به روش Opt-out مشهور است که پیش‌تر به آن پرداختیم. قانون مزبور اشاره‌ای کلی به «تمهیدات» دارد و انواع آن را مشخص نکرده است. با این حال، به نظر می‌رسد منظور از تمهیدات دربارهٔ پیام‌های ارسالی تبلیغی، ذکر مشخصات ارسال‌کنندهٔ پیام و ذکر آدرس تماس برگشت به گیرندهٔ پیام است تا در صورتی که گیرندهٔ پیام نخواهد مجدداً پیامی دریافت کند آن را به اطلاع فرستنده برساند. مادّهٔ ۵۵ دربارهٔ نصاب پیام‌های قابل ارسال، اشاره‌ای ندارد و این اطلاق از یک تا بی‌نهایت پیام را دربرمی‌گیرد. به طور کلی قانون مزبور، ارسال پیام را آزاد دانسته است، ولی دربارهٔ پیام‌های تبلیغاتی، رضایت ثانویه و پسینی گیرندهٔ پیام تجاری را مبنا قرار داده است و فقط دربارهٔ «عدم ارائهٔ تمهیداتی» برای اعلام عدم رضایت کاربر ـ و نه ارسال پیام ـ جرم‌انگاری کرده است.

اقدامات دیگری در جهت تدوین لوایحی به وسیلهٔ دولت نیز برای جرم‌انگاری ارسال پیام‌های ناخواسته صورت گرفته است که از آن جمله می‌توان به «لایحهٔ پیام‌های ناخواستهٔ الکترونیکی» ارائه‌شده به وسیلهٔ وزارت ارتباطات و فناوری اطلاعات در سال ۱۳۸۷ اشاره کرد. لایحهٔ مزبور در هیئت دولت به تصویب نرسید. متعاقب آن، وزارت فرهنگ و ارشاد اسلامی «پیش‌نویس لایحهٔ پیام دیجیتال» را تدوین و ارائه کرد. لایحهٔ مذکور که قاعدتاً به خاطر عنوان آن باید به حوزهٔ «پیام‌های دیجیتال» محدود می‌شد، چیزی بسیار فراتر از آن بود و دربارهٔ شبکه‌های رایانه‌ای و بسیاری مسائل دیگر نیز مقرراتی پیشنهاد کرده بود که در جای خود جای تأمل دارد. پرسش اینجاست که آیا در واقع با یک پیش‌نویس دربارهٔ پیام‌های دیجیتال می‌توان مشکلات فضای سایبر در کشورمان را به سامان رساند و از یک لایحه، به عنوان فرصتی برای تصویب خواست-های یک وزارتخانه، برای تنظیم و کنترل فضای سایبر به شکل دلخواه بهره جُست؟

با توجه به عدم تصویب لوایح پیش‌گفته، پرسش اساسی همچنان باقی می‌ماند و آن اینکه آیا در کشور ما ضرورتی قابل دفاع برای وضع مقررات کیفری در کنترل پیام‌های ناخواسته ـ افزون بر مقررات کیفری موجود ـ وجود دارد؟ از نظر ارائه‌کنندگان خدمات پُست الکترونیکی که بیشترین ضرر را از اسپم متحمل می‌شوند، باید توجه داشت که بیشتر هموطنان ما از خدمات ارائه‌کنندگان پُست الکترونیکی خارجی برای دریافت و ارسال پُست الکترونیکی استفاده می‌کنند؛ بنابراین اگر ضرر و هزینه‌ای از جهت ارسال اسپم به ارائه‌کنندگان وارد است، معمولاً متوجه ارائه‌کنندگان خدمات در خارج از کشور ماست. از سوی دیگر، فناوری‌های کنترل اسپم در سالیان گذشته آنقدر پیشرفت داشته است که ارائه‌کنندگان خدمات مزبور با به‌کارگیری آنها ـ حداقل دریافت مستقیم اسپم توسط کاربران ـ را تا حدود زیادی کنترل کنند. براساس گزارش کمیسیون تجارت فدرال در ایالات متحده در سال ۲۰۰۷، ارتقای سیستم‌های نوین پالایش نقش بسیار مؤثری در کاهش پیام‌های ناخواسته داشته‌اند. گسترش فناوری‌های نوین قطعاً در آینده نیز راهکارهای مؤثرتری ارائه خواهد داد (spam summit report, P. 31). به نظر می‌رسد در کشور ما ارسال اسپم از نظر کاربران مقوله‌ای جدی به شمار نمی‌رود؛ هرچند در این باره تحقیقی میدانی و جامع به عمل نیامده است، با این حال یک بررسی اجمالی نشان خواهد داد که اسپم برای آنان آنقدر آزاردهنده نیست که برخورد کیفری با اسپم را از دیدگاه آنان توجیه کند.

مادهٔ ۵۵ قانون تجارت الکترونیکی ـ هرچند مقصود واضعان آن در بدو تصویب، محدود به اسپم نبوده باشد ـ با برگزیدن راه حل پسینی در رضایت گیرندهٔ پیام تبلیغی، هم حق آزادی ارسال پیام را برای ارسال‌کننده پیام پذیرفته است و هم رضایت کاربر را به عنوان حقی دیگر به رسمیت شناخته است؛ بنابراین این ماده راه حلی بینابینی ارائه می‌دهد که فعلاً برای کنترل اسپم در کشور ما کافی به نظر می‌رسد. با این حال، وضع قانون دربارهٔ اقدامات دیگر غیرقانونی مربوط به ارسال اسپم، همچون ارسال اسپم به صورت سازمان‌یافته یا اقداماتی همچون جمع‌آوری آدرس‌های الکترونیکی افراد و ارسال ایمیل به صورت متقلبانه به آدرس پُست الکترونیکی آنان ـ که پیش‌تر به آنها پرداخته شد ـ در یک حرکت موازی جهانی برای کنترل فضای سایبر شاید یک

ضرورت باشد. در عین حال، باز هم لازم نیست لزوماً در این باره به جرم‌انگاری پرداخت یا از ضمانت اجراهای کیفری استفاده کرد. کشورهایی مانند استرالیا با تصویب قانون spam act، روش‌های مدنی و جبران خسارت را برای این منظور به کار گرفته‌ا ند که خود می‌تواند تدبیر حقوقیِ درخور توجهی باشد.

نتیجه

ارسال پیام‌های ناخواسته که بیشتر در جهت اهداف تجاری و تبلیغی صورت می‌گیرد، در جهان رو به گسترش است و این موضوع هزینه‌های بسیاری را ـ به ویژه بر دوش ارائه‌کنندگان خدمات ـ تحمیل می‌کند. کشورهایی که کمتر با این مشکل مواجه بوده‌اند، معمولاً مقررات ویژه‌ای را برای کنترل اسپم وضع نکرده و تلاش کرده‌اند که از راه روش‌های فنی و آموزشی، به مبارزه بروند یا از قوانین موجود خود ـ اعم از کیفری یا حقوقی ـ در جهت مبارزه با آثار مخربی که محتوای پیام‌ها می‌تواند داشته باشد، بهره گیرند. با این حال، کشورهایی که این موضوع را معضل جدی‌تری بر جامعهٔ اطلاعاتی خویش می‌دانسته‌اند، مقرراتی ویژه را بدین‌منظور وضع کرده‌اند و علاوه بر مقررات موجود خویش که ناظر بر محتوای پیام‌های ارسالی است، رضایت گیرندهٔ پیام‌ها را در دریافت پیام‌ها لازم دانسته‌اند. افزون بر این، برخی کشورها ارسال پیام‌های ناخواسته با روش‌های متقلبانه، جمع‌آوری آدرس‌های الکترونیکی و نیز عدم رعایت موازین شکلی در ارسال پیام را ممنوع کرده است و در جهت نقض آنها، ضمانت اجراهایی حقوقی یا کیفری را تصویب کرده‌اند. در ایران علاوه بر قانون تجارت الکترونیکی که مقرراتی در این باره دارد، تاکنون دو لایحه، یکی به وسیلهٔ وزارت ارتباطات و فناوری اطلاعات و دیگری به‌وسیلهٔ وزارت ارشاد، تنظیم و به هیئت دولت ارائه شده است که هرچند هیچ‌یک به تصویب نرسیده‌اند، ولی نشانگر شکل‌گیری رویکردی کیفری‌محور با این پدیده در کشورمان است. مادهٔ ۵۵ قانون تجارت الکترونیکی، ناظر به لزوم ارائهٔ تمهیداتی به گیرندهٔ پیام به وسیلهٔ پُست الکترونیکی است که مخاطب پیام بتواند عدم رضایت دریافت پیامی دیگر را به ارسال‌کنندهٔ پیام اطلاع دهد. مادهٔ ۷۰ قانون مزبور نیز ضمانت اجرای کیفری را در جهت نقض این حکم قانونی در نظر گرفته است. با این

حال، به نظر نمی‌رسد موضوع دریافت پیام‌های ناخواسته در کشور ما آنقدر جدی باشد که وضع مقرراتی ویژه را بدین‌منظور ضروری جلوه دهد. کاربران در کشور ما بیشتر از ارائه‌کنندگان خدمات پُست الکترونیک خارجی استفاده می‌کنند و از این جهت ضـرری متوجه ارائه‌کنندگان خدمات داخلی نیست. در ضمن، اسپم از نظـر کـاربران نیـز آنقـدر موضوع آزاردهنده‌ای نیست که لـزوم وضـع مقرراتـی کیفـری را در ایـن حـوزه ـ کـه شدیدترین نوع کنترل اجتماعی به شمار می‌آید ـ توجیه کند. بر این اسـاس، چنـین بـه نظر می‌رسد که فعلاً وضع مقررات کیفری برای کنترل پیام‌های ناخواسته در کشـورمان، افزون بر مقررات موجود، توجیه قابل اقناعی ندارد.

منابع

الف) کتاب‌ها و مقاله‌ها

۱. عالی‌پور، حسن؛ «جرایم مرتبط با محتوا: محتوای سیاه فناوری اطلاعات»؛ **مجموعه مقالات اولین همایش حقوقی فناوری اطلاعات**، معاونت حقوقی و توسعهٔ قضایی قوهٔ قضائیه با همکاری شورای عالی اطلاع‌رسانی، شورای عالی توسعهٔ قضایی، تهران: سلسبیل، ۱۳۸٤.

۲. ـــــــ؛ «کلاهبرداری رایانه‌ای»؛ **مجلهٔ پژوهش‌های حقوقی**، سال سوم، ش ٦، پاییز و زمستان ۱۳۸۳.

۳. فضلی، مهدی؛ «تخریب و اختلال در داده‌ها و سیستم‌های رایانه‌ای»، **مجموعه مقالات اولین همایش حقوقی فناوری اطلاعات**، معاونت حقوقی و توسعهٔ قضایی قوهٔ قضائیه با همکاری شورای عالی اطلاع‌رسانی، شورای عالی توسعهٔ قضایی، تهران: سلسبیل، ۱۳۸٤.

٤. نِد، اسنل؛ **اینترنت مقدماتی و پیشرفته**؛ مترجم: کیوان فلاح مشفقی، چ ۵، تهران: مرکز فرهنگی نشر گستر، ۱۳۸۰.

۵. هیئت مؤلفان و ویراستاران انتشارات مایکروسافت؛ **فرهنگ تشریحی اصطلاحات کامپیوتری مایکروسافت**؛ مترجم فرهاد قلی‌زاده نوری، چ ۱، تهران: نشر سینا تصویر، ۱۳۸۱.

6. Brenton, Chris, Hunt, Cameron; **Mastering Network Security;** Sybex Publication, Second Edition, USA, October 2002.

7. Chissick, Michael and Kelman, Alister; **Electronic Commerce Law and Practice;** Third Edition, Sweet and Maxwell, 2002.

8. Encyclopedia of Privacy; Vol. 2, Edited by William G. Staples,

Greenwood Press, USA, 2007.

9. Fingerman, Dan; **Spam Canned Throughout the Land?** Summary of the CAN ـ SPAM Act With Commentary, Journal of Internet Law, Vol. 7, issue 8, February 2004.
10. Stacy L. Edgar; **Morality and Machines;** Jones And Bartlett computer Science Publication, Second Edition, 2003.

ب) منابع اینترنتی

1. Arora, Vivek, The CAN_SPAM Act: An Inadequate Attempt to Deal With a Growing Problem, spring 2006, https://litigation ـ essentials.lexisnexis.com
2. Blanke, Jordan M., Canned Spam: New State and Federal Legislation Attempts to Put a Lid on It, 2004, http://www. studentorgs.law.smu.edu/Science ـ and ـ Technology ـ Law.../Blanke.aspx
3. FTC v. Adteractive, Stipulated Final Judgment for Civil Penalties and Permanent Injunctive Relief, 2007, http://www.ftc.gov/opa/ 2007/11/free.shtm.
4. FTC v. Jumpstart Technologies, Consent Decree and Order for Civil Penalties and Injunctive and Other Relief, 2006, http://www.ftc.gov/os/caselist/0423176/0423176JumpstartTechnologiesConsentDecree.pdf.
5. FTC v. Spear Systems, Inc., Temporary Restraining Order, 2007, http://www.ftc.gov/os/caselist/0723050/index.shtm.
6. FTC v. William Dugger et.al, Final Judgment and Order for Permanent Injunction, 2006,

7. Geist, Michael, Untouchable? A Canadian Perspective on the Anti ـ Spam Battle, 2005, http://www.michaelgeist.ca/ geistspam. pdf
8. http://en.wikipedia.org/wiki/Header_information_technology
9. http://www.ftc.gov/os/caselist/0523161/060731duggerfinaljdgmnt .pdf.
10. http://www.m5computersecurity.com/research/OpenRelay ـــ analysis ـ 1.2.pdf
11. Malik, Dale W., FTC Spam Forum, April 30 ـ May 1, 2003, http://www.ftc.gov/bcp/workshops/spam/presentations/malik.pdf
12. McCafferty, Michael, Statistical Analysis of Open E ـ mail Relaying on the Internet, 2002,
13. Messagelabs Intelligence Report, August 2010, http://www. messagelabs.co.uk/resources/mlireports.aspx
14. Messagelabs Intelligence Report, November 2010, http://www. messagelabs.co.uk/resources/mlireports.aspx
15. Messagelabs Intelligence: 2009 Annual Security Report, http://www.messagelabs.co.uk/resources/mlireports.aspx
16. Moustakas, Evangelos, Duquenoy, Penny, Service Provider Responsibility for Unsolicited Commercial Communication (Spam), School of Computing Science, Middlesex University, London, UK, 2003, http://eprints.mdx.ac.uk/2064/
17. Moustakas, Evangelos, Ranganathan, C., Duquenoy, Penny, Combating Spam through Legislation: A Comparative Analysis of US and European Approaches, 2nd Conference on Email and Anti ـ Spam (CEAS 2005) ـ Stanford University, USA,21 ـ 22 July 2005, www.ceas.cc/papers ـ 2005/146.pdf

18. OECD Task Force on Spam Report,15 Nov. 2005, www.oecd ـــ antispam.org
19. Recognizing and Avoiding Email Scams, US ـــ Cert, 2008, www.us ـ cert.gov/reading_room/emailscams_0905.pdf
20. SOPHOS Security Threat Report, Mid ـــ year 2010, http://www.sophos.com
21. Spam Summit Report, the Next Generation of Threats and Solutions, A Staff Report by Federal Trade Commission, Division of Marketing Practices, 2007, http://www.ftc.gov/bcp/workshops/spam/index.shtml
22. Sullivan, Bob, Spam wars: How Unwanted Email is Burying the Internet, 2003, http://www.spamsolutions.net/1059.asp
23. The "Nigerian" Scam: Costly Compassion, Federal Trade Commission (FTC), Bureau of Consumer Protection, July 2003, www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt117.pdf
24. Wayne Crews Jr., Wayne Crews Jr., Why Canning Spam Is a Bad Idea?, 2001, http://www.cato.org/pubs/pas/pa408.pdf.