اقدام حقوقی اتحادیه‌ی اروپا برای رویارویی با هرزنامه[1]

نویسنده: نیکلا لوگارسی* مترجمان: علی جعفری** عظیم عابدینی***

۱. مقدمه:

امروزه بیش از ۵۰٪ حجم ایمیل (رایانامه)های ارسالی در سطح اتحادیه‌ی اروپا و سراسر جهان «ارتباطات تجاری ناخواسته»[2] است. این مقاله به رویکرد حقوقی اتحادیه‌ی اروپا در برابر این پدیده می‌پردازد. در این مقاله با بررسی سیر قانون گذاری، تلاش می‌شود تا با تعریف هرزنامه از دیدگاه قوانین و مقررات، علت اینکه اتحادیه‌ی اروپا سیستمی را برگزیده که امکان ثبت‌نام در فهرست مجاز برای فرستادن پیام را فراهم می‌کند، بیان و قوانین مربوط به سایر ابعاد این موضوع مشخص شود.

مهم‌ترین علت رویارویی اتحادیه‌ی اروپا با هرزنامه (هرزنامه را ارتباطات الکترونیک تجاری ناخواسته فرض می‌کنیم) این است که هرزنامه بر حقوق اساسی اشخاص اثر می‌گذارد. هرزنامه نه تنها در سطح جهانی مزاحمت، دانسته شده بلکه به طور کلی حریم خصوصی افراد را مخدوش می‌کند. این پدیده جنبه‌ی روشن‌تری از حریم خصوصی اشخاص، یعنی حمایت از داده‌های شخصی او را از بین می‌برد، زیرا با گردآوری و استفاده غیرقانونی آدرس‌های ایمیل (رایانامه)ها و استفاده‌ی نادرست و ناعادلانه از آنها و هم‌چنین کنترل ورود اطلاعات به حریم

---

1. European Union Vs. Spam: A Legal Response.

*. Nicola Lugaresi (lugaresi@jus.unitn.it) Trento University, Law school, via Verdi, 53, 38100 Trento, Italy.

**. عضو شورای علمی گروه فقه و حقوق ارتباطات پژوهشکده باقرالعلوم علیه‌السلام.

***. دانشجوی دکتری مدرسی مبانی نظری اسلام، دانشگاه تهران.

2. Unsolicited commercial communications.

خصوصی آسایش آنها را از بین می‌برد. از این رو با توجه به دستورالعمل‌های اتحادیه‌ی اروپا و دیگر اسناد رسمی آن، می‌توان از برخورد قانونی برای جلوگیری از ایجاد ارتباطات تجاری ناخواسته که با هدف حمایت از حقوق و منافع گوناگون اشخاص است، از چند منظر دفاع کرد.

هرزنامه‌ها بر حقوق افراد، کاربران، مشترکان، مصرف‌کنندگان، شرکت‌ها، بازرگانان بی‌واسطه، خدمات دهندگان اینترنتی، تجار، کارفرمایان، سازمان‌ها، مؤسسات عمومی و بر خود اینترنت اثر می‌گذارد. در چند سال گذشته اتحادیه‌ی اروپا از خطرات نقض حریم خصوصی که به سبب گسترش دسترسی مردم جامعه از راه اینترنت به خدمات ارتباطات الکترونیک بوده، مطلع بوده است.[۱] اتحادیه‌ی اروپا می‌داند که هرزنامه خطراتی را برای ارتباطات الکترونیکی، شبکه‌های متصل به هم، تجهیزات پایانه‌های ارتباطی،[۲] بهره‌وری در کار[۳] و تجارت الکترونیک[۴] در بردارد.[۱] علاوه بر آن، هرزنامه اغلب به ابزاری برای کلاه‌برداری، فرستادن پیام‌های شهوت‌انگیز جنسی، ناسزاگویی و انتقال ویروس تبدیل شده است.

قوانین اتحادیه‌ی اروپا، با توجه به برخی دلائل قضائی و فنی، نمی‌توانند به تنهائی مشکل هرزنامه‌ها را حل کنند. اما با وجود ایمیل (رایانامه)های مزاحم که در کوتاه مدت ایجاد شدند، اتحادیه‌ی اروپا نمی‌توانست در برابر نقض مکرر حقوق اساسی که به سبب هرزنامه‌ها پدید آمد، سکوت کند. قوانین اتحادیه‌ی اروپا دو هدف مهم را دنبال می‌کنند: هدفی عملیاتی برای کاهش حجم هرزنامه‌ها و هدفی اخلاقی در جهت حفظ توانایی افراد برای کنترل ارتباطات و تماس‌های شخصی و کنترل تماس‌های ورودی و خروجی.

---

[1] Article 1, and recital 6, Dir. 2002/58/EC.
[2] Recital 30, Dir.2000/31/EC; recital 40, Dir.2002/58/EC.
[3] EC Communication on "spam" (2004), §1.2.
[4] Recital 60, Dir.2000/31/EC.
1. right to be let alone.

تا زمانی که نظام‌های حقوقی با هم هماهنگ نشوند و مسائل مربوط به صلاحیت و حوزه‌ی قضایی حل نشود، هدف اول چندان محقق نخواهد شد. درباره‌ی هدف دوم، قوانین اتحادیه‌ی اروپا رعایت حریم خصوصی افراد در کلیه شئون زندگی شخصی را در زمره‌ی حقوق اولیه و اساسی قرار داده است[۵] و هرزنامه‌ها را مشکل عمده‌ای می‌داند که نقش بسیار مهمی در ناکامی‌های بازار دارند؛ مگر اینکه قوانین سخت‌گیرانه‌ای وضع و اجرا شود. از چنین رویکردی، با شناخت نقش ارتباطات تجاری در جامعه‌ی اطلاعاتی، حمایت خواهد شد[۶]. اما برای اجرایی کردن این رویکرد، دستورالعمل‌های اتحادیه‌ی اروپا درباره‌ی تمام ارتباطات تجاری ناخواسته که از طریق شبکه‌های داخل اتحادیه‌ی اروپا دریافت یا ارسال می‌شوند، به کار می‌روند.[۷] هنگامی که ایمیلی (رایانامه‌ای) از کشور ثالث (خارج از اتحادیه‌ی اروپا) فرستاده می‌شود، اجرای قانون (و به طور خاص، شناسایی فرستنده‌ی هرزنامه) به دلیل اندک بودن تجربیات در این باره و هم‌چنین وجود موانع مربوط به حوزه‌ی قضائی، به مسأله‌ای بسیار پیچیده تبدیل می‌شود. مسائل مربوط به حوزه‌ی قضائی نیاز به همکاری بین‌المللی برای رویارویی با پدیده هرزنامه را به خوبی نشان می‌دهد. البته، سیاست‌های حقوقی و قوانین اتحادیه‌ی اروپا در این باره نباید راه‌حل نهائی دانسته شود، بلکه باید آنها را تلاشی برای وضع قوانین منطقی و الگوی احتمالی برای ارائه رویکردی هماهنگ برای کاهش حجم هرزنامه‌ها دانست. این رویکرد هماهنگ بر سه عامل استوار است:

اول، نهادهای قانون‌گذار باید اقدامات جدی و مناسبی را برای ضمانت اجرای این قوانین انجام دهند. این اقدامات عبارت‌اند از: به کارگیری مجازات‌های مؤثر، آماده سازی روشی برای رسیدگی به شکایات و جبران خسارت به صورت ملی و فراملی، نظارت، ایجاد همکاری و هماهنگی

[5] Council Decision 1999/168/EC (Annex II, §a.i).
[6] Recital 29, Dir. 2000/31/EC.
[7] EC Communication on "spam" (2004), §3.5.1.

بین دستگاه‌های داخلی، هم‌کاری‌های بین‌المللی و دسترسی به منابع؛ باید با پدیده‌ی هرزنامه مقابله کرد و نه اینکه صرفا به نکوهش آن بسنده کرد.

دوم، برای کنترل پدیده‌ی هرزنامه باید نظام‌ها و سازمان‌های متنوعی ایجاد شوند؛ این نظام‌ها عبارت‌اند از: نظام قانون‌گذاری، سازمان تنظیم مقررات داخلی، ساختارسازی، طراحی راه‌کارهای مختلف برای حل اختلاف‌ها و روش‌هایی که ویژگی خاص آنها انطباق‌پذیری و داشتن ظرفیت مناسب برای انطباق فوری با پدیده‌ها و فناوری‌های جدید است. ارتباط آنلاین (در خط) به فرستادن هرزنامه می‌انجامد، پس باید ابزارهای موجود برای جلوگیری از این کار گسترش یابد. آموزش کاربران و کارکنان بازار، اطلاعات دهی، ایجاد راهنمایی خودآموز و به کارگیری انجمن‌ها و سازمان‌های حمایت از حریم خصوصی در این کار، از جمله‌ی این ابزارها است.[۸] به عبارت دیگر، باید با تمام عوامل دخیل و مرتبط با پدیده‌ی هرزنامه مقابله کرد.

۲. از خروج از فهرست مجاز برای ارسال پیام تا نام‌نویسی در فهرست مجاز

از سال ۱۹۹۵ به بعد، علاوه بر راهبردهای سیاسی گسترده، دستورالعمل‌های اتحادیه‌ی اروپا درباره حریم خصوصی، تجارت و ارتباطات بر مقررات مربوط به هرزنامه اثرگذار بوده است. در آغاز، انگیزه‌ی اصلی این دستورالعمل‌ها ضرورت حمایت از شهروندان و مصرف‌کنندگان در برابر «شیوه‌های فروش اجباری» [۹][1] و «برخی ابزارهای ارتباطی و به خصوص مزاحم»[۱۰] بود. هر چند، با وجود تصویب قانون کنترل تبلیغات تجاری و جنسی ناخواسته موسوم به «کن اسپم»[2] در سال

[8] EC Communication on "spam" (2004), §3-5.
[9] Recital 5, Dir. 97//7/EC.
1. high – pressure Selling method.
[10] Recital 17, Dir. 97//7/EC.
2. Controlling the Assault of Non- solicited pornography and marketing Act (CAN-SPAM).

۲۰۰۳ در آمریکا، اتحادیه‌ی اروپا قانون خاصی را برای رویارویی با پدیده‌ی هرزنامه وضع نکرده است.

دستورالعمل شماره‌ی ۹۵/۴۶ کمیسیون اروپا (چارچوب دستورالعمل حمایت از داده‌ها) به طور خاص، به ارتباطات الکترونیکی مربوط نمی‌شود. با وجود این، مفاد آن که درباره‌ی پردازش داده‌های شخصی است، ممکن است ابزارهایی را برای رویارویی با هرزنامه فراهم کند که به اشتباه به آنها بی‌توجهی شده است. آدرس‌های ایمیل (رایانامه) «اطلاعات شخصی» دانسته می‌شوند[۱۱] و در نحوه‌ی پردازش آنها باید به قوانین موجود در این دستورالعمل توجه شود. علاوه بر این، قبل از گردآوری آدرس‌ها، باید رضایت مخاطب با اختیار و آگاهی او و به طور مشخص[۱۲] و روشن[۱۳] گرفته شود؛ اصول پردازش منصفانه باید رعایت شود؛[۱۴] گردآورندگان آدرس‌های ایمیل (رایانامه) باید برای این کار خود اهداف صریح و قانونی تعیین کنند[۱۵] و درباره‌ی گردآوری و استفاده از آدرس‌های ایمیل (رایانامه) باید اطلاعات کافی در اختیار مخاطب قرار گیرد؛[۱۶] فعالیت‌هایی مانند گردآوری آدرس‌های ایمیل (رایانامه) در مکان‌های عمومی اینترنت مانند وب‌سایت‌ها، اتاق‌های چت، گروه‌های خبری و غیره، به موجب دستورالعمل شماره‌ی ۹۵/۴۶ کمیسیون اروپا، غیرقانونی است، زیرا مصداق پردازش نامنصفانه‌ی داده‌های شخصی بوده، با اصل محدود کردن هدف و پذیرش کافی بودن اطلاعات که پیش‌تر بیان شد، مخالف است.[۱۷]

هم‌چنین، رضایت تلویحی، استفاده از صندوق‌های پستی از قبل کنترل

---

[11] Article 2(a), Dir.95/46/EC.
[12] Article 2(h), Dir. 95/46/EC.
[13] Article 7(a), Dir. 95/46/EC.
[14] Article 6(a), Dir. 95/46/EC.
[15] Article 6(b), Dir. 95/46/EC.
[16]Artt.10, 11, Dir. 95/46/EC.
[17]DPWP, Working Document - Privacy on the Internet (2000), Chapter 4, §IV; DPWP, Recommendation 2/2001, §28; EC Communication on "spam" (2004), §2.3.

شده، و درخواست‌های کلی گسترده برای گرفتن رضایت بـا شـرایط بیـان شده در این دستورالعمل درباره‌ی شـفافیت و منصـفانه بـودن، همـاهنگی ندارد. [۱۸]

جـدای از حمایـت غیرمسـتقیم کـه در دسـتورالعمل شـماره‌ی ۹۵/۴۶ کمیسیون اروپا بیان شده، نخستین اشاره‌ی قانونی احتمـالی و تلـویحی بـه موضوع هرزنامه در دستورالعمل شماره‌ی ۹۷/۷ کمیسیون اروپا (دربـاره‌ی دستورالعمل قراردادهای از راه دور[۱]) به چشم می‌خورد. هر چند مفاد ایـن دستورالعمل نیازمند گرفتن رضایت قلبـی دربـاره سیسـتم‌هـای فراخـوان خودکار[۲] و دستگاه‌های فکس است،[۱۹] در باره سایر «ابزارهـای ارتبـاط از راه دور» (مانند ایمیل) تصریح می‌کند: تنهـا در صـورتی مـی‌تـوان از آنهـا استفاده کرد کـه از سـوی مصـرف کننـده «اعتـراض مشخصـی»[۳] نداشـته باشـد.[۲۰] دسـتورالعمل شـماره‌ی ۹۷/۷ کمیسـیون اروپـا بـرای «اعتـراض مشخص» تعریفی بیان نمی‌کند و به طور سر بسته به روش خارج شدن از فهرست مجاز برای ارسال پیام اشاره می‌کند. علاوه بـر ایـن، دسـتورالعمل شماره‌ی ۹۷/۶۶ کمیسیون اروپا (دستورالعمل حمایت از حریم خصوصـی بخش ارتباطات از راه دور[۴]) که دیگر دارای اعتبار نیست، «قانون ثبت نـام در فهرست مجاز»[۵] برای ارسال پیام را تنها در باره‌ی سیستم‌های فراخـوان خودکار بدون دخالت انسان یا دستگاه‌های فکس در جهت تحقـق هـدف بازاریابی مستقیم تأیید می‌کرد.[۲۱]

---

[18] DPWP, Working Document - Privacy on the Internet (2000), Chapter 4, §V; Chapter 8, §4.

1. Distance Contracts Directive.

2. automated calling system.

[19] Article 10(1), Dir. 97/7/EC.

3 . clear objection

[20] Article 10(2), Dir. 97/7/EC.

4. Telecommunications sector privacy Directive.

5 . opt-in rule

[21] Article 12(1), Dir. 97/66/EC.

درباره‌ی ابزارهای دیگر، مانند ایمیل، کشورهای عضو باید با اتخاذ تدابیر مناسب، تضمین می‌کردند که تماس‌های رایگان و ناخواسته مجاز نیست، و بدین ترتیب این حق انتخاب به هنگام وضع قوانین ملی وجود داشت که کدام یک از سیستم‌های ثبت‌نام در فهرست مجاز برای ارسال پیام، خارج شدن از فهرست مجاز، یا ترکیبی از هر دو را می‌توان اختیار کرد.[۲۲] تعجبی ندارد که در دستورالعمل شماره‌ی ۲۰۰۰/۳۱ کمیسیون اروپا (دستورالعمل تجارت الکترونیکی[1]) این مسئله بدیهی دانسته شده بود که برای ارتباطات تجاری ناخواسته از طریق پست الکترونیکی (رایانامه)، کشورهای عضو می‌توانند از سیستم‌های حاوی امکان خروج از فهرست مجاز برای ارسال پیام استفاده کنند.[۲۳] سیستم ثبت‌نام در فهرست مجاز برای ارسال پیام که برای سیستم‌های تماس تلفنی خودکار و دستگاه‌های فکس انتخاب شده بود، به دلیل تفاوتی که تأیید شده اما سؤال انگیز بود، درباره ایمیل به کار نمی‌رفت.

سرانجام دستورالعمل ۲۰۰۲/۵۸ اروپا (دستورالعمل حمایت از حریم خصوصی ارتباطات الکترونیکی) که دستورالعمل شماره‌ی ۹۷/۶۶ کمیسیون اروپا را لغو کرد، با به کارگیری سیستم مبتنی بر رضایت درباره ایمیل‌ها بر تردیدها و مخالفت‌های موجود نیز فائق آمد.[۲۴] در نهایت این نتیجه به دست آمد که منفعت فرد در خلاص شدن از اطلاعات تجاری ناخواسته، در مقایسه با این نگرانی که سیستم ثبت‌نام در فهرست مجاز برای ارسال پیام ممکن است مانع از گسترش تجارت الکترونیکی شود، اهمیت بیشتری دارد؛ همین مسئله باعث ایجاد تبعیض میان شرکت‌ها در اتحادیه‌ی اروپا شده و احتمالا عوامل مستقیم اثرگذار بر بازار را بر آن می‌دارد که فعالیت‌های خود را به سمت خارج شدن از اتحادیه‌ی اروپا سوق دهند.

---

[22] Article 12(2), Dir. 97/66/EC.

1. Electronic Commerce Directive.

[23] Article 7(2), and recital 14, Dir. 2000/31/EC.

[24] DPWP, Opinion 7/2000, §2, comment to article 13.

۳ ـ هرزنامه چیست؟

اصطلاح «هرزنامه» در هیچ یک از دستورالعمل‌های اتحادیه‌ی اروپا که در بالا نام برده شد، تعریف نشده و به کار نرفته است، اما در عوض به تعاریف دیگری اشاره شده، از جمله: «وسایل ارتباط از راه دور»،[۲۵] «ارتباطات تجاری»،[۲۶] «ارتباطات»،[۲۷] و «نامه‌ی الکترونیکی».[۲۸] ماده‌ی ۱۳ (مربوط به «ارتباطات ناخواسته») دستورالعمل حمایت از حریم خصوصی ارتباطات الکترونیکی، مصوب ۲۰۰۲ به طور خاص، به «نامه‌ی الکترونیکی با اهداف بازاریابی مستقیم» اشاره می‌کند. در سایر اسناد رسمی اتحادیه‌ی اروپا، به جز قوانین مربوط، تعاریف مختلفی برای هرزنامه بیان شده است، از جمله: «ارسال حجم وسیعی از مطالب تبلیغاتی ناخواسته از راه ایمیل برای بازاریابی»؛[۲۹] یا «ارسال ایمیل‌های ناخواسته که معمولا ماهیت تجاری دارند، در حجم وسیع و به طور مکرر برای افرادی که ارسال کننده‌ی پیام قبلا تماسی با آنها نداشته است.»[۳۰] یا « ارسال پیام‌های تجاری ناخواسته به طور مرتب و در سطح وسیع که فرستنده هویت خود را پنهان یا جعل می‌کند». [۳۱]

برخی از مشخصات موجود در تعاریف مذکور، تکراری است. هرزنامه در قالب ایمیل فرستاده می‌شود، ناخواسته است، در حجم وسیعی منتقل می‌شود و ماهیت تجاری دارد. در نتیجه، می‌توان گفت که هرزنامه با ایمیل الکترونیکی ناخواسته، عمده و تجاری مترادف است. اکنون برای تأیید این ادعا به بررسی ماده‌ی ۱۳ دستورالعمل حمایت از حریم خصوصی ارتباطات الکترونیکی مصوب ۲۰۰۲ می‌پردازیم.

هرزنامه ایمیل است. ایمیل یا «نامه‌ی الکترونیکی» در واقع هرگونه

---

[25] Article 2(4), Dir. 97/7/EC.
[26] Article 2(f), Dir. 2000/31/EC.
[27] Article 2(d), Dir. 2002/58/EC.
[28] Article 2(h), Dir.2002/58/EC.
[29] DPWP, Working Document - Privacy on the Internet (2000), Glossary.
[30] DPWP, Opinion 7/2000, §2, comment to article 13.
[31] Commission – Summary of Study Findings (2001), §2.3.

ارتباط الکترونیکی را که نیازمند مشارکت هم‌زمان فرستنده و گیرنده نیست، دربرمی‌گیرد، از جمله انواع ایمیل‌های فراتر از کلاسیک، پیام کوتاه (SMS)، پیام چند رسانه‌ای (MMS)، پیام‌های ضبط شده در دستگاه پیام‌گیر، سیستم‌های خدمات پست صوتی، ارتباطات «فرستاده شده از[1] شبکه» که مستقیما به یک آدرس IP فرستاده می‌شود و خبرنامه‌های فرستاده شده از طریق ایمیل.[۳۲] بنابراین، هرزنامه چیزی بیش از ایمیل «کلاسیک» صرف است.

هرزنامه ناخواسته است. در سیستمی که دارای امکان ثبت‌نام در فهرست مجاز برای ارسال پیام است،[2] ایجاد هرگونه ارتباط ناخواسته ـ یعنی ارسال پیام به کاربر بدون رضایت قبلی او ـ غیرقانونی است. در «سیستم دارای امکان خروج از فهرست مجاز»[3] برای ارسال پیام، این امر، ممکن است غیرقانونی نباشد.[۳۳] ارتباط نوع اول، حتی اگر ناخواسته باشد، تا زمانی که فرستنده از سایر قوانین مربوط به ارتباطات پیروی کند، قانونی خواهد بود. چنان چه دریافت کننده‌ی ایمیل از فهرست مجاز برای دریافت پیام‌های دیگر خارج نشود، ایمیل‌های بعدی نیز ممکن است قانونی باشند، زیرا قابل مدارا و مجاز هستند (اما مطابق خواست کاربر نیستند). بنابراین در سیستم دارای امکان ثبت‌نام در فهرست مجاز برای ارسال پیام، اگر هرزنامه هم زمان با پیام ناخواسته باشد، غیرقانونی خواهد بود. در سیستم دارای امکان خروج از لیست مجاز، برخی ارتباطات ناخواسته قانونی‌اند (قبل از خروج دریافت کننده‌ی پیام از فهرست مجاز)، و برخی غیرقانونی (پس از خروج دریافت‌کننده‌ی پیام از فهرست مجاز). از این جهت، می‌توان گفت که هرزنامه را نباید با پیام «ناخواسته» یکی دانست، بلکه پیامی «غیرقانونی» است که نحوه‌ی فرستادن آن شرایط

1 . net send
[32] DPWP, Opinion 5/2004, §3.1.
2 . opt-in system
3 . opt-out system
[33]Article 7(1), Dir.2000/31/EC.

قانونی لازم را ندارد. همین امر موجب برداشت منفی درباره‌ی اصطلاح «هرزنامه» می‌شود. در این صورت، همان ایمیل ناخواسته‌ای که فرستنده برای اولین بار به دریافت کننده می‌فرستد، در سیستم دارای امکان ثبت‌نام در فهرست مجاز برای فرستادن پیام، هرزنامه (غیرقانونی) دانسته می‌شود، اما در سیستم دارای امکان خروج از فهرست مجاز، هرزنامه نخواهد بود. این مسئله وابسته به تعریفی است که قانون برای اصطلاح «هرزنامه» بیان می‌کند: آیا به موضوع و واقع (ناخواسته بودن) مربوط است، یا به حکم (غیرقانونی بودن).

هرزنامه ماهیت تجاری دارد اما ماده‌ی ۱۳ دستورالعمل حمایت از حریم خصوصی ارتباطات الکترونیکی، مصوب ۲۰۰۲ تنها به «اهداف بازاریابی مستقیم» اشاره می‌کند و صفت «تجاری» موجود در ماده‌ی ۷ دستورالعمل سابق (مصوب ۲۰۰۰) که به تجارت الکترونیکی اشاره دارد، را حذف می‌کند. در دستورالعمل شماره‌ی ۲۰۰۲/۵۸ کمیسیون اروپا، هیچ یک از مفاهیم «بازاریابی مستقیم» یا «تجاری» تعریف نشده است.

درباره‌ی بازاریابی مستقیم[1]،[۳۴] «اهداف بازاریابی» در گزارش شماره‌ی ۳۰ دستورالعمل مربوط به «منشور حمایت از داده‌ها»،[2] مصوب ۱۹۹۵، تعریف شده است. این اهداف می‌تواند به صورت تجاری یا به دست سازمانی خیریه یا یک انجمن یا مؤسسه‌ی دیگری که به طور مثال، ماهیت سیاسی دارد، برآورده شود.

از این جهت، چنانچه بر «بازاریابی» تأکید شود، در نتیجه ماده‌ی ۱۳ دستورالعمل شماره‌ی ۲۰۰۲/۵۸ کمیسیون اروپا، مصوب ۲۰۰۲، هرگونه

1 .Direct marketing

[34]A definition of "direct marketing" has been used in the FEDMA (Federation of European Direct Marketing) European Code of Practice for the Use of Personal Data in Direct Marketing (approved by the DPWP Opinion 3/2003): "The communication by whatever means (including but not limited to mail, fax, telephone, on - line services, etc…) of any advertising or marketing material, which is carried out by the Direct Marketer itself or on its behalf and which is directed to particular individuals."

2 .Frame work Data Protection

روش افزایش فروش، از جمله بازاریـابی مسـتقیم را کـه مراکـز خیریـه و نهادهای سیاسی انجام می‌دهند شامل می‌شود.[۳۵] چنانچه برداشت متفاوتی صورت گیرد و در نتیجه بر تفاوت میان فعالیت‌های دارای اهداف تجـاری و فعالیت‌های سازمان‌های غیرانتفاعی تأکید شود، آن‌گاه مـاده‌ی ۱۳ صـرفا شامل فعالیت‌هـای دارای اهـداف تجـاری خواهـد شـد. از سـوی دیگـر، می‌توان گفت که اهداف بازاریابی مستقیم در مقایسه بـا اهـداف تجـاری، حوزه‌ی محدودتری را در برمی‌گیرند. در نتیجه ماده‌ی ۱۳ هرزنامه‌ای را که با هدف بازاریابی مستقیم فرستاده شده، شامل می‌شود، اما هرزنامه‌ای را که با اهداف تجاری، غیر از بازاریابی مستقیم، فرستاده شده، در برنمـی‌گیـرد. در هر دو صورت، شرط تجاری بـودن (یـا بازاریـابی مسـتقیم) مـی‌توانـد ویژگی جدا سازنده‌ای درباره‌ی هرزنامه باشد یـا نباشـد. بـازهم، در نظـام حقوقی دو گزینه مطرح می‌شود؛ ۱ـ هرزنامه می‌تواند تجاری باشد و غیـر تجاری (هرزنامه غیر تجاری هم داریم)، ۲ـ یا برای آنکه پیـامی هرزنامـه دانسته شود، باید دارای اهداف تجاری (یا بازاریابی مستقیم) باشد.

هرزنامه در حجم وسیعی فرستاده می‌شود. هرچند هرزنامه معمـولا بـه «ارسال پیام در حجم وسـیع»[1] گفتـه مـی‌شـود، تعریـف آن در مـاده‌ی ۱۳ دستورالعمل شماره‌ی ۲۰۰۲/۵۸ کمیسیون اروپا به حداقل میزان ایمیل‌های فرستاده شده که ممکن است آثار سؤال برانگیـزی داشـته باشـد، محـدود نمی‌شود. به طور مثال، یک ایمیل را کـه تنهـا در آن سـوابق کـاری بـرای تقاضای شغل است و برای بررسی فرستاده مـی‌شـود، مـی‌تـوان هرزنامـه دانست، به شرط آنکه فرستادن سوابق کـاری، فعالیـت بازاریـابی مسـتقیم باشد. از سوی دیگر، چنانچه برای هرزنامـه بـودن، رقمـی حـداقلی بـرای پیام‌های تجاری تعیین کنیم، این امر موجب کاهش سطح حمایت می‌شود. از این رو، در نظام حقوقی جاری اتحادیه‌ی اروپا، تعداد، شرط لازم بـرای هرزنامه بودن دانسته نمی‌شود، بـه طـوری کـه در دسـتورالعمل شـماره‌ی

[35] DPWP, Opinion 5/2004, §3.3.

1 . mass mailing

۲۰۰۲/۵۸ کمیسیون اروپا نیامده است که فرستادن ایمیل (یا فکس) تنها در صورتی غیرقانونی است که از مقداری حداقلی فراتر رود.

خلاصه مطلب اینکه هرچند هرزنامه عموما ایمیل ناخواسته، در حجمی وسیع، تجاری (و غیرقانونی) دانسته می‌شود، در اصطلاح حقوقی ممکن است دارای اشکال مختلف و مرکب از ویژگی‌های بیان شده به شکل‌های مختلف باشد و از ارتباطات تجاری ساده تا ایمیل‌هایی با اهداف بازاریابی مستقیم و پیام‌های الکترونیکی غیرقانونی را در بر بگیرد. قانونی بودن یا نبودن هرزنامه به این بستگی دارد که دریافت کننده‌ی پیام‌ها سیستم «دارای امکان ثبت‌نام در فهرست مجاز برای ارسال پیام»[1] را انتخاب می‌کند و یاسیستم «خروج از فهرست مجاز»[2] و نیز به نظام حقوقی مربوط بستگی دارد.

۴ـ نحوه‌ی کسب رضایت[3]

انتخاب «سیستمی که امکان نام نویسی در فهرست مجاز برای فرستادن پیام را فراهم می‌کند»،[4] در دستورالعمل حمایت از حریم خصوصی ارتباطات الکترونیکی، مصوب ۲۰۰۲، بیان‌گر ورود مقررات اتحادیه‌ی اروپا به حوزه‌ی «ارتباطات تجاری ناخواسته»[5] است. قانون‌گذار بر این عقیده بوده است که این سیستم می‌تواند حمایت مؤثرتری را برای افراد فراهم و انتظارات کاربران، خدمات دهندگان اینترنتی و خود صنعت را به نحو بهتری برآورده کند.[۳۶] بعلاوه، این سیستم به چهارچوب قانونی ساده‌تری نیاز دارد، راحت‌تر اجرا می‌شود، امکان تبلیغات کارآمدتری را فراهم می‌کند،[۳۷] و دست‌کم از دیدگاه نظری، قوانین دقیق‌تر و جدی‌تری

1. opt-in.
2. opt-out.
3. The Manner of Consent.
4. opt-in system.
5. unsolicited commercial communications.
[36] DPWP, Opinion 7/2000, §2, comment to article 13.
[37] Commission – Summary of Study Findings (2001).

را برای نظارت بر هرزنامه در اختیار ما قرار می‌دهد.

مطابق ماده‌ی ۱۳دستورالعمل ۵۸ / ۲۰۰۲ کمیسیون اروپا، استفاده از «نامه‌ی الکترونیکی با هدف بازاریابی مستقیم» تنها درباره‌ی مشترکانی مجاز است که پیش‌تر رضایت خود را اعلام کرده باشند.[۳۸] و این به وضوح به سیستم بنیادین «نام نویسی در فهرست مجاز برای فرستادن پیام»[1] اشاره دارد. با وجود این، دستورالعمل شماره‌ی ۲۰۰۲/۵۸ کمیسیون اروپا چند قانون کوتاه و استثنائاتی را نیز برای مدلی که کاملا بر اساس «نام نویسی در فهرست مجاز برای فرستادن پیام» شکل گرفته، معرفی می‌کند که رد پایی را از سیستم سابق که بر اساس «خروج از فهرست مجاز برای فرستادن پیام» شکل گرفته بود، نشان می‌دهد.

مسئله‌ای که باید به آن اشاره کرد، موضوع آدرس‌های ایمیلی است که متعلق به مشترک خاصی نیست، مانند آدرس شرکت‌ها یا خانواده‌ها. در این موارد، چون رضایت قلبی مشترک لازم است، راه حل جبران حمایت نکردن، گرفتن رضایت از مشترکی است[۳۹] که کاربر اصلی نیست.[۴۰] اما از آنچه که آدرس‌های ایمیل، اطلاعات شخصی هستند، در نتیجه دستورالعمل مربوط به منشور حمایت از داده‌ها، مصوب ۱۹۹۵، به طور مستقل از آن حمایت می‌کند.[۴۱] حتی اگر نشانی، برای یک مشترک نباشد و در نتیجه دستورالعمل شماره‌ی ۲۰۰۲/۵۸ کمیسیون اروپا از آن حمایت نکند، برای یک کاربر است و لذا دستورالعمل شماره‌ی ۹۵/۴۶ کمیسیون اروپا از آن حمایت می‌کند.

موضوع مشابه دیگر، مسئله‌ی آدرس ایمیل موجود در فهرست ایمیل‌ها[2] است. ممکن است گفته شود، باید از دارنده‌ی فهرست،[3] رضایت

---

[38] Article 13(1), Dir. 2002/58/EC; recital 17, Dir. 2002/58/EC.

1. opt-in.

[39] Article 2(k), Dir. 2002/21/EC.

[40] Article 2(a), Dir.2002/58/EC.

[41] DPWP, Opinion 5/2004, §3.4.

2. mailing list.

3. Iist owner.

قبلی گرفته شود، یعنی افراد موجود در فهرست تنها با خروج از فهرست می‌توانند حریم خصوصی خود را حفظ کنند یا اینکه می‌توان بر این عقیده بود که هر یک از افراد موجود در فهرست می‌توانند مانع از فرستادن پیام‌های تجاری ناخواسته برای کل افراد فهرست شوند. تا زمانی که راه‌حل‌های فنی امکان اداره‌ی هر یک از نشانی‌های ایمیل موجود در فهرست را به طور جداگانه و با توجه به علت انتخاب هر یک از آنها فراهم نکند، پاسخ مسئله به این تصمیم بستگی خواهد داشت که از چه کسی باید حمایت شود: از دیدگاه قراردادی از مشترک خدمات ارتباطی، یعنی دارنده‌ی فهرست باید حمایت شود و از دیدگاه شخصی‌تر مصرف کننده‌ی خدمات، یعنی فرد موجود در فهرست باید مورد حمایت قرار گیرد.

از جزئیات ارتباط الکترونیکی، که در پی فروش یک محصول یا خدمات دهی به دست می‌آید، ممکن است برای بازاریابی مستقیم محصولات یا خدمات مشابه استفاده شود.[۴۲] این «سیستم نرم نام نویسی در فهرست مجاز برای فرستادن پیام»[1] است. البته این سیستم ممکن است در عمل چندان هم نرم نباشد؛ زیرا باید هم به هنگام گردآوری و هم در صورت فرستادن پی در پی پیام برای بازاریابی مستقیم امکان اعتراض رایگان و راحت درباره‌ی استفاده از جزئیات اطلاعات مشتریان در اختیار آنان قرار گیرد.[۴۳] در کنار دادن جزئیات اطلاعات الکترونیکی به مصرف کننده رضایت او نیز به دست می‌آید.

تفاوت اصلی سیستم نرم با «سیستم سخت»[2] شرایط حقیقی به دست آوردن رضایت و فروش است. اما در هر دو صورت باید داده‌ها هماهنگ با دستور العمل مربوط به منشور حمایت از داده‌ها، مصوب ۱۹۹۵، به دست آید. در حقیقت، فرصت اعتراض به این گونه استفاده، لزوما با دادن

[42] Article 13(2), Dir. 2002/58/EC.
1. soft opt-in.
[43] Recital 41, Dir. 2002/58/EC.
2. hard opt-in.

اطلاعات کافی درباره‌ی نوع استفاده ارتباط دارد. بنابراین موارد استثناء بر «فروش قبلی» به چند طریق محدود می‌شود و باید منحصرا آنها را تفسیر و تبیین کرد.[۴۴] باید فروشی در میان باشد، نه اینکه تنها رابطه‌ی تجاری مبهمی وجود داشته باشد؛ استفاده از جزئیات اطلاعات الکترونیکی تنها به همان شرکت محدود باشد، که به این ترتیب شرکت‌های وابسته[1] یا مادر نمی‌توانند از آن اطلاعات استفاده کنند ؛[۴۵] و بازاریابی مستقیم تنها باید به محصولات یا خدمات مشابه محدود باشد و این شباهت‌ها بر اساس انتظارات متعارف و معقول دریافت کننده ارزیابی خواهند شد.[۴۶]

در چنین شرایطی، چنانچه به طور صحیح عمل شود، گردآوری جزئیات الکترونیکی برای فروش کالا یا خدمات به مثابه روشی برای گفتگو و احتمالا به دست آوردن رضایت قبلی برای ارتباطات تجاری خواهد بود.

دستورالعمل شماره‌ی ۲۰۰۲/۵۸ کمیسیون اروپا از فرستادن نامه‌ی الکترونیکی برای بازاریابی مستقیم، با تغییر دادن یا پنهان کردن هویت فرستنده، یا بدون نشانی معتبر به نحوی که دریافت‌کننده امکان خروج از فهرست مجاز برای فرستادن پیام را داشته باشد، جلوگیری می‌کند.[۴۷] این ممنوعیت نتیجه‌ی اجرای دقیق و مؤثر قوانین کمیسیون اروپاست،[۴۸] اما تا حدودی زائد تلقی می‌شود، زیرا فرستادن پیام‌های ناخواسته در هر صورت، ممنوع است. در «رویکرد دارای امکان خروج از فهرست مجاز برای فرستادن پیام»،[2] تغییر دادن یا پنهان کردن هویت و آدرس بازگشت[3] در ارتباط تجاری، امری غیرقانونی است. در سیستم «امکان نام‌نویسی در

[44] DPWP, Opinion 5/2004, §3.5.
1. subsidiary.
[45] DPWP, Opinion 5/2004, §3.5.
[46] DPWP, Opinion 5/2004, §3.5.
[47]Article 13(4), Dir. 2002/58/EC.
[48] Recital 43, Dir. 2002/58/EC.
2 . opt-out approack.
3. return address.

فهرست مجاز برای فرستادن پیام»،[1] این اقدامات بیشتر موجب تقویت میزان غیرقانونی بودن عمل می‌شود. ممکن است فرستنده‌ی پیام که رضایت قبلی معتبری به دست آورده، قانون را نقض کند، اما این کار بسیار بعید به نظر می‌رسد. اما چنانچه فرستنده‌ی پیام رضایت معتبری به دست نیاورده، احتمال بیشتری برای تغییر دادن یا پنهان کاری وجود دارد. بعلاوه «تغییر شکل و پنهان‌کاری» بر خلاف دستورالعمل مربوط به منشور حمایت از داده‌ها، مصوب ۱۹۹۵، نیز هست؛ زیرا اطلاعات شخصی دیگران بدون رضایت آنها پردازش می‌شود.

در نهایت اینکه دستورالعمل شماره‌ی ۲۰۰۲/۵۸ کمیسیون اروپا می‌گوید: «سیستم امکان نام نویسی در فهرست مجاز برای فرستادن پیام» تنها درباره‌ی اشخاص حقیقی به کار می‌رود. درباره‌ی اشخاص حقوقی، کشورهای عضو باید امکان حمایت کافی را از «مشتریانی که اشخاص حقیقی نیستند» در برابر هرزنامه‌ها فراهم کنند.[۴۹] هر چند تفاوت حقوقی میان اشخاص حقیقی و حقوقی کاملا روشن است، هماهنگی فرستندگان پیام با دو سیستم مختلف ـ سیستم دارای امکان نام نویسی در فهرست مجاز برای اشخاص حقیقی، و سیستم امکان خروج از فهرست مجاز برای اشخاص حقوقی ـ چندان آسان نیست. همیشه نمی‌توان از روی آدرس‌های ایمیل دریافت که آیا گیرنده‌ی پیام، شخص حقیقی است یا حقوقی. در چنین شرایطی، یا فرستنده‌ی پیام باید به طور دقیق ماهیت گیرنده‌ی پیام را بداند.[۵۰] یا خطر ورود به یک عمل غیرقانونی را بپذیرد. تصمیم منطقی و راه‌حل ساده آن است که نام اشخاص حقیقی را به اجبار به سیستم «دارای امکان نام نویسی در فهرست مجاز برای فرستادن پیام» وارد کنیم.

1 . opt-in.
[49] Article 13(5), Dir. 2002/58/EC.
[50] DPWP, Opinion 5/2004, §3.4.

۵ ـ ابزارهای جانبی[1]

درباره‌ی ابزارهای قانونی جانبی و مرتبط با قوانین اساسی که در بالا به آنها اشاره شد، تردیدهایی وجود دارد. با وجود به کارگیری «سیستم امکان نام نویسی در فهرست مجاز برای فرستادن پیام»، دستورالعمل‌های جاری کمیسیون اروپا مطالبی دارد که ابزارهای پیشنهادی آنها درباره‌ی سیستم‌های «امکان خروج از فهرست مجاز» است. دستورالعمل‌های کمیسیون اروپا فیلتر کردن و برچسب‌زنی[2] را ابزارهای مفیدی برای اجرای بهتر قوانین و به ویژه جلوگیری از ایجاد هزینه‌هایی که هرزنامه بر گیرنده‌ی پیام تحمیل می‌کند، به شمار می‌آورند. لذا دستورالعمل حمایت از حریم خصوصی ارتباطات الکترونیکی ۲۰۰۲، از ابتکار عمل صنعت برای فیلتر کردن حمایت کرده و آنها را تشویق می‌کنند.[۵۱] این کار با به کارگیری تدابیری در سیستم‌های ایمیل صورت می‌گیرد که به موجب آن مشتریان می‌توانند فرستنده و موضوع ایمیل را ببینند و بدون دریافت (دانلود) محتوی یا پیوست‌ها[3] پیام‌ها را حذف کنند.[۵۲] معنای این گفته آن است که کشورهای عضو باید اطمینان دهند که این گونه پیام‌های تجاری خدمات دهندگان مستقر در قلمرو آنها، به محض دریافت پیام به طور کاملا روشن و واضح قابل شناسایی است؛[۵۳] برای مثال، در موضوع می‌توان از برچسب «ADV» استفاده کرد. جدای از مباحث مربوط به آزادی بیان و اجباری بودن بیان،[4] که در آمریکا بیش از اتحادیه‌ی اروپا نسبت به آنها حساسیت هست، برچسب «ADV» بیش‌تر با سیستم «امکان خروج از فهرست مجاز برای فرستادن پیام» هماهنگ است، که به موجب آن انواع مختلف پیام‌های تجاری را می‌توان دریافت کرد. در سیستم

1. The ancillary tools.
2. labeling.
[51] Recital 30, Dir.2000/31/EC.
3. attachment.
[52] Recital 44, Dir. 2002/58/EC.
[53]. Article 7, Dir. 2000/31/EC.
4. FORCED SPEECH.

«امکان نام‌نویسی در فهرست مجاز برای فرستادن پیام» پیام‌های تجاری یا قانونی و خواسته شده و همراه با رضایت قبلی هستند، یا قانونی نیستند و در این صورت استفاده از برچسب، آنها را به پیام قانونی تبدیل نمی‌کند.

دستورالعمل شماره‌ی ۲۰۰۲/۵۸ کمیسیون اروپا وظیفه‌ی حمایت از منافع قانونی اشخاص حقوقی را به کشورهای عضو می‌سپرد و آنها باید حمایت کافی را فراهم آورند. در حقیقت، این دستورالعمل می‌تواند محلی را برای ثبت خروج از فهرست مجاز برای فرستادن هرزنامه تعیین کند[۵۴] که با سیستم «امکان نام نویسی در فهرست مجاز برای فرستادن پیام»، هماهنگی ندارد. قبلا در دستورالعمل تجارت الکترونیکی مصوب ۲۰۰۰ به «فهرست نشانی‌های خواستار خروج از فهرست مجاز برای فرستادن پیام»[۱] (یا فهرست نشانی‌هایی که نباید به آنها ایمیلی فرستاده شود)[۲] توجه شده بود و این دستورالعمل خدمات دهندگان را که وظیفه‌ی آنها فرستادن پیام‌های تجاری ناخواسته از راه پست الکترونیکی بود، مجبور می‌ساخت که به طور مرتب نظر مشتریان را جویا شوند و به فهرست نشانی‌های خواهان خروج از فهرست مجاز توجه کنند. در این فهرست‌ها اشخاص حقیقی که نمی‌خواستند این گونه پیام‌های تجاری را دریافت کنند، می‌توانستند نام نویسی کنند.[۵۵]

علاوه بر این ممکن است «فهرست نشانی‌هایی که نباید ایمیل به آنها فرستاده شود» برای حریم خصوصی کاربران خطرناک باشد، مگر آنکه به صورت فهرست‌هایی در سطح دامنه ایجاد شده باشند. فهرست‌های ایجاد شده با نشانی ایمیل، که نشانی‌های ایمیل شخصی در آنها گردآوری و احتمالا افشا می‌شود، به جای حمایت از حریم خصوصی، تهدیدی برای آن محسوب می‌شوند. بعلاوه، این فهرست‌ها، به ویژه درباره‌ی فعالیت‌های

[54] Article 13(5), Dir. 2002/58/EC; recital 44, Dir. 2002/58/EC.

1. OPT – out register.

2 . Do not mail list

[55] Article 7(2), Dir.2000/31/EC; recital 31, Dir. 2002/58/EC.

برون مرزی، ممکن است همراه کارهای سخت و طاقت‌فرسا برای کاربران (به ویژه اگر برای مقابله با هرزنامه، نشانی ایمیل خود را بـه طـور مرتـب تغییر دهند)، عوامل مستقیم بازار (که همواره باید بر آنها نظارت کننـد)، و مراجع یا نهادهایی باشد که وظیفه‌ی آنها اداره کردن و بـه روز نگهداشـتن این فهرست‌ها است. جدای از مسائل امنیتـی، همیشـه ایـن خطـر پـذیری هست که آیا با «برادر بزرگ‌تر»[1] باید به نتیجه رسید یا با برادران کوچک‌تر فراوانی که چندان شناخته شده نیستند، و ایـن کـار برنامـه‌ریـزی را بـرای کاربران و هماهنگی را برای عوامل مستقیم بازار دشوارتر می‌سازد.

وضع مقررات کاری،[2] ابزار دیگری است که در دستورالعمل‌ها بـه آنهـا توجه شده و از دستورالعمل شماره‌ی ۹۵/۴۶ به بعد کمیسیون اروپا به آنها اشاره شده است.[۵۶] پیش از دسـتورالعمل شـماره‌ی ۲۰۰۲/۵۸ کمیسـیون اروپا «خود سامان‌گری»[3] ابزار اصلی سامان‌دهی در مقابله با هرزنامـه بـوده اسـت.[۵۷] دسـتورالعمل شـماره‌ی ۲۰۰۰/۳۱ کمیسـیون اروپـا «گـروه‌هـا و انجمن‌های حرفه‌ای را تشویق می‌کند تا با وضع مقررات کـاری در سـطح جامعه‌ی اروپا، نوع اطلاعاتی را که می‌توان در ارتباطات تجاری جا به جـا کرد، تعیین کنند».[۵۸]

همین دستورالعمل می‌کوشد مقررات کاری، شکل شفاف‌تری بـه خـود بگیرند و از انتشار اختیاری طرح مقررات کاری، دسترس‌پـذیر بـودن آنهـا برای همگان، و «شرکت دادن انجمـن‌هـا یـا سـازمان‌هـا بـه نماینـدگی از مصرف کنندگان در تهیه و اجرای مقررات کاری مؤثر بـرای تـأمین منـافع آنها» حمایت می‌کند.[۵۹]

---

1 . Big brother. مترادف اصطلاح آقا بالا سر در فارسی است.
2. codes of conduct.
[56]Article 27, Dir. 95/46/EC.
3. self – regulation.
[57] Recital 32, Dir.2000/31/EC; see also recital 41, Dir.2000/31/EC.
[58] Article 8(2), Dir.2000/31/EC.
[59] Article 16(2), Dir. 2000/31/EC.

شواهد نشان داده است که خود سامان‌گری به تنهایی برای ایجاد اعتبار و شفافیت بیشتر کارایی ندارد، حتی اگر بر اساس مراحل نظام مند باشد[۶۰]. خودسامان‌گری، با هدف محدود کردن خود،[1] قطعا برای در اختیار داشتن موضوع حساسی چون هرزنامه مناسب نیست، حتی اگر هدف آن «کنترل و تنظیم، مشارکتی»[2] هم باشد نمی‌تواند تنها مرجع تنظیمی (تنها راه ممکن) باشد و به ویژه در مقام اجرا لازم است قوانینی وضع شود. افزون بر آن، خودسامان‌گری، وضع مقررات کاری، استفاده از برچسب کیفیت و اقدامات بازاریابی مناسب در سیستم «امکان نام نویسی در فهرست مجاز» برای فرستادن پیام به اندازه‌ی سیستم «امکان خروج از فهرست مجاز» ضرورت ندارد، زیرا سیستم اول، استقلال و شرایط اجرایی شدن بیشتری دارد و کامل‌تر است.

هر چند دستورالعمل‌های اتحادیه‌ی اروپا کاربرد «صندوق هرزنامه»[3] را ابزار احتمالی مناسبی نمی‌دانند، برخی مراجع ملی حمایت از داده‌ها[۶۱] چنین ابتکار عمل‌هایی را به کار گرفته‌اند که دیگر اسناد اتحادیه‌ی اروپا نیز از آنها حمایت کرده‌اند. کاربران می‌توانند هرزنامه‌های دریافتی را به «صندوق هرزنامه» که DPA ها ایجاد کرده‌اند، فرستاده[4] و ابزارهای اجرایی را فعال کنند. «صندوق هرزنامه»، حتی بدون دادن جایزه، مصرف کنندگان را به گزارش موارد نقض قانون تشویق می‌کند، موجب اجرای قوانین وضع شده در سطح گسترده‌تر و مؤثرتر می‌شود و آمار و اطلاعات خوبی در اختیار DPA ها قرار می‌دهد. «صندوق هرزنامه» راهی آسان، مستقیم و

[60] DPWP, Opinion 3/2003; see also article 30, Dir. 95/46/EC.

1. self- limitation.

2.Participateal co-regulation.

3. spam baxes.

[61]For instance, by the French 'Commission Nationale Informatique et Libertés (CNIL)' and the Belgian 'Commission de la Protection de la Vie Privée (CPVP).

4. forward

ارزان برای شکایت و گزارش تخلفات است که نوعی خط داغ «حذف با یک کلیک»[1] محسوب می‌شود. کاربر تنها باید هرزنامه‌ی ناخواسته را به صندوق هرزنامه بفرستد و نیازی نیست که توضیح دهد پیام به صورت نوشته یا تلفنی درست شده است.

در نهایت اینکه بستن قرارداد می‌تواند به مقابله با هرزنامه کمک کند و این کار از طریق تنظیم مواد و شرایط قرارداد مشتریان بر اساس سیستم «امکان نام نویسی در فهرست مجاز برای فرستادن پیام»[2] صورت می‌گیرد.

خدمات دهندگان اینترنتی[3] (Isp_s)، خدمات دهندگان ایمیل (Esp_s) و خدمات دهندگان تلفن همراه باید با درج تعهداتی در قراردادها مانع از به کارگیری خدمات خود برای فرستادن هرزنامه شوند و درباره‌ی فیلترهای ضد هرزنامه و ابزارهای دیگری که ممکن است مشترکان برای نظارت بر هرزنامه از آنها استفاده کنند، خبر رسانی کنند.[۶۲] همچنین در صورت نقض موارد فوق، باید مجازات‌های قراردادی[4] مؤثرتری در قرارداد پیش‌بینی شود.

۶ـ نتیجه‌گیری[5]

سیر دگرگونی نظام حقوقی اتحادیه‌ی اروپا نشان می‌دهد که خود سامان‌گری و سیستم «دارای امکان خروج از فهرست مجاز برای فرستادن پیام» در مقابله با هرزنامه ناکام بوده است. سیستم «امکان نام نویسی در فهرست مجاز برای فرستادن پیام»، که در دستورالعمل حمایت از حریم خصوصی ارتباطات الکترونیکی، مصوب ۲۰۰۲، پیش‌بینی شده، واکنشی است که اتحادیه‌ی اروپا آن را اقدامی منطقی‌تر، مناسب‌تر و مؤثرتر برای

1. «one- click away.» hotline.
2 . opt-in.
3 . Internet serviceproviders.
[62] EC Communication on "spam" (2004), §4.1.2.
4 . contractual penalties.
5. Conclusion.

حمایت از مهم‌ترین مسئله‌ی موردنظر، یعنی حـریم خصوصـی شخصـی، می‌داند. این تدبیر نه ضرورت امضای موافقت‌نامه‌هـای بـین‌المللـی بـرای هماهنگی سیستم‌های مختلف (سیستم امکان نام نویسی در فهرست مجـاز برای فرستادن پیام و سیستم امکان خروج از فهرست مجاز) را نفی می‌کند و نه مراجعه به سایر ابزارهای تنظیم کننده را نادرست می‌داند (زیرا قـانون به تنهایی کافی نیست). اتحادیه‌ی اروپا هم زمان، هـم بـه وضـع مقـررات می‌پردازد و هم طرحی را برای سیاست گذاری پیشنهاد می‌کند. ماده‌ی ۱۳ دستورالعمل شماره‌ی ۲۰۰۲/۵۸ کمیسیون اروپا، که قوانین اساسی مربـوط به پیام‌های تجاری ناخواسته را در بـردارد، ردپـای سیسـتم قبلـی «امکـان ثبت‌نام در فهرست مجاز برای فرستادن پیام» را نشان می‌دهد که همین امر باعث روانی کم‌تر و ناهماهنگی در برخی از بخش‌های قانون شده است. و در نهایت، باید برای هرزنامه تعریفی بیان شود، زیرا ایـن واژه اصـطلاحی حقوقی نیست و ممکن است باعث برداشت غلط از هدف اصـلی در ایـن باره شود.

منابع:

– EU Directives and Decisions :

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett

Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts

http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31997L0007&model=guichett

Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector

http://europa.eu.int/eur ___ lex/pri/en/oj/dat/1998/l_024/l_02419980130 en 00010008.pdf

/168/1999EC: Council Decision of 25 January 1999 adopting a specific programme for research, technological development and demonstration on a user _ friendly information society (1998 to 2002)

http://europa.eu.int/eur _ lex /pri/en/oj/dat/1999/l _ 064/l _ 06419990312 en 00200039.pdf

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce ")

http://europa.eu.int/eur _____ lex/ pri/ en/ oj /dat /2000 / l _ 178 /l _ 17820000717 en 00010016.pdf

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services ("Framework Directive")

http://europa.eu.int/eur _ lex/ pri/ en/ oj/dat/ 2002/l_108/l_ 10820020424 en

00330050.pdf
Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ("Directive on privacy and electronic communications ")
http://europa.eu.int/eur - lex/ pri/ en/oj/ dat/2002/l_201/l _ 20120020731 en 00370047.pdf
– Data Protection Working Party documents:
Data Protection Working Party – Opinion 7/2000 on the European Commission proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 (2 November 2000)
http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2000/wp36en.pdf
Data Protection Working Party, Working Document, Privacy on the Internet – An Integrated EU Approach to On – line DataProtection (21 November 2000)
http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2000/wp37en.pdf
Data Protection Working Party – Recommendation 2/2001 on certain minimum requirements for collecting personal data on – linein the European Union (17 May 2001)
http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2001/wp43en.pdf
Data Protection Working Party – Opinion 3/2003 on the European code of conduct of FEDMA for the use of personal data indirect marketing (13 June 2003)
http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp77_ en.pdf
Data Protection Working Party – Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC (27 February 2004)
http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp90_ en.pdf
– Other EU documents :
Commission of the European Communities – Unsolicited commercial

communications and data protection _ Summary of Study Findings __ January 2001
http://europa.eu.int/comm/internal_market/privacy/docs/studies/spamsum_en.pdf
Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on unsolicited commercial communications or "spam" (22 January 2004)
http://europa.eu.int/information_society/topics/ecomm/doc/useful_informatio n/ library/communic_reports/spam/spam_com_2004_28_en.pdf.