Encyclopedia of Economic Law Journal

Homepage: https://lawecon.um.ac.ir

Research Article

Vol. 30, No. 24, Fall-Winter 2023 , p. 63-78

Unsolicited Commercial Message (Spam): Prohibited or Permitted?

M. Bakhtiarvand[1]*, S.M.H Ghabooli Dorafshan[2]

1- Associate Professor, Department of Private Law and Intellectual Property Law, University of Qom, Qom, Iran. (*- Corresponding Author Email: m.bakhtiarvand@qom.ac.ir)
2- Associate Professor, Department of Islamic Jurisprudence and Principles of Islamic Law, Ferdowsi University of Mashhad, Mashhad, Iran.

Received: 8 November 2023 Revised: 18 December 2023 Accepted: 15 February 2024 Available Online: 15 February 2024	**How to cite this article:** Bakhtiarvand, M; Ghabooli Dorafshan, S.M.H. (2023). Unsolicited Commercial Message (Spam): Prohibited or Permitted?. *Encyclopedia of Economic Law Journal, 30*(24): 63-78. (In Persian with English abstract) https://doi.org/10.22067/economlaw.2024.85568.1331

1- INTRODUCTION

Unsolicited commercial messages (spam) are sent electronically and in bulk, without the consent of the recipient, through tools such as e-mail or SMS. Apart from the advantages for advertisers, spam can violate the privacy of internet and mobile phone users and cause economic losses and widespread dissatisfaction of consumers and even merchants. This, along with the possibility of disrupting the functioning of systems such as e-mail and SMS, may lead to mistrust of e-commerce and digital economy. The results of this descriptive-analytical article show that some countries allow the sending of spam even without the consent of the recipient, and their subsequent opposition is considered an obstacle to sending, which is called the opt-out method. Other countries require the prior consent of the recipient that it is known as the opt-in method. The two mentioned methods are applied through three legislative approaches namely with tolerance, intermediate and hard, which are divided and named according to the way of dealing with spam senders and remedies and sanctions. The position of Iranian law regarding the prohibition or permission of sending spam is not very clear.

Two turning points can be seen in the history of sending spam: The first message that was considered as spam was a message that was sent by Gary Tuerk, a sales representative of a digital equipment company, in 1978 to 393 Arpant employees. The mentioned company was looking for the development of its market and invited interested consumers to the unveiling ceremony of a new product, and for this purpose, it sent an advertising message to Arpant users. 16 years later, in 1994, two attorneys from the state of Arizona advertised their immigration consulting service by spamming almost every Usenet discussion group. This message was mainly met with negative reactions from users, because it was not related to the target discussion groups. As the newest phenomenon in this field, we can mention sending spam through artificial intelligence, by which artificial intelligence systems can be used to strengthen activities that include sending different types of spam.

So far, many legislative efforts have been made to deal with spam, and countries have either declared spam to be free and give the recipient the right to object to this (opt-out method) or the prior consent of the recipient considered necessary for sending spam (opt-in method). In order to implement the above two methods, three legislative approaches have been formed, which include the soft approach, intermediate and hard Approach. At the same time, legal measures have not had a significant effect in reducing spam. The reason for this should be mainly found in the global nature of the problem, the lack of international measures and the lack of awareness of the users about the problem. Although Bill Gates promised in 2004 that spam would be eradicated within two years, this promise was never fulfilled. With the emergence of new technologies, new and dangerous methods of sending spam have been formed, which affect the world wide web and social networks and cause the emergency situation in this field to continue.

2- PURPOSE

The main purpse of this article is to answer the folloing question: "What is the appropriate legislative method for Iran in dealing with unwanted commercial electronic messages?". Therefore, the authors attempt to find the best slution to the problems associated with Spam in Iran. In order to answer this question first, an adequate imagination of the problem should be provided; so to get familiar with the subject, we will explain the concept of spam and then its history will be mentioned. Then, in order to find the best solution for Iranian law, the existing legal approaches in dealing with spam are examined and analyzed.

3- METHODOLOGY

The authors have adopted a descriptive-analytical method through which different legal approaches towards spam are described and analysed.

4- FINDINGS

The most precise definition of spam is a definition that includes several requirements, including the requirement that it must be an impersonal message in which the identity and circumstances of the recipient are not of importance, a message that has been sent to many other recipients, the recipient has not given the permission to send the message, and in some cases, the message contains an unrealistic prize or reward for the recipient. Some authors have described the basic features of spam as follows: a- unsolicited by the recipient; b- having a commercial nature; And c- sent in bulk. Therefore, according to the authors, the following definition of spam can be appropriate: "bulk electronic commercial advertising message that is sent to the recipients without their request". Obviously, this article focuses on messages that have commercial content and are considered commercial spam.

Many governments and a large part of the international community believe that it is not possible to deal effectively with spam without establishing a law and providing remedies and sanctions of proper implementation. As a result, many countries have passed anti-spam laws, which, of course, have followed different patterns for their implementation; In this way, for example, criminal sanctions, filing of civil lawsuits by governments or the right to file private lawsuits for individuals or Internet service providers are foreseen.

Despite this, some commonalities can be seen in the anti-spam laws; Most of the laws consider spam as illegal when it hides the sender's identity, uses a third party's domain name illegally, or provides misleading information in the subject of the email. In general, these rules adopt either an opt-out method, in which the recipient can opt out of receiving further messages, or an opt-in method that requires prior consent of the recipient. Many of the aforementioned laws require senders to introduce themselves clearly and precisely.

Depending on the way each of the above methods are implenented, we can divide the major legislative approaches in dealing with spam into three categories. First. The soft approach (with tolerance) of the United States; Second. the intermediate approach of the European Union; and the third The hard approach that is followed in countries like Australia and South Korea.

5- CONCLUSION

Sending spam is an attractive and effective way to advertise the goods and services of economic enterprises and even to express different thoughts and opinions and sometimes, it is a tool for committing computer crimes. The main feature of such messages is their bulk sending without the prior consent of consumers, which are often used to advertise commercial products. Regardless of the content of the unwanted electronic message, sending it leads to various losses such as wasting time and property and offending the recipient and violating his privacy. This type of advertising reduces trust in information and communication technologies and is considered an obstacle to the development of e-commerce. After the spread of sending spam and the increase of users' dissatisfaction, the countries of the world tried to deal with it and the result of their efforts are two methods of opt-out and opt-in, which can be seen in the form of three main approaches soft (with tolerance), intermediate and hard (strict). In the meantime, the United States of America, where according to statistics, the most commercial advertising messages are sent, has passed a special law and has established the principle of freedom to send spam by adopting a soft approach. The aforementioned law, under certain conditions, allows advertisers to send promotional e-mails to users, and at the same time, obliges them to provide the possibility of declaring their unwillingness to receive these messages. On the other hand, the European Union has adopted an intermediate approach and has declared that sending spam is prohibited except in the case of the prior consent of the recipient or the existence of a previous relationship. Countries such as Australia and South Korea have also banned the sending of unwanted commercial messages and have provided sanctions for violating such ruling, which is considered strict and severe compared to other countries. In Iranian law, according to Article 55 of the Electronic Commerce Act,

suppliers are required to provide arrangements for consumers to decide whether or not to receive commercial advertisements. Due to the lack of mention of the time of provision of the aforementioned measures, it is not clear whether the Iranian legislator chose the principle of freedom to send spam or, like the European Union, preferred the interests of users over the interests of economic enterprises and the possibility of sending messages to people who wanted to receive them. Indeed, there are scattered and relatively diverse regulations and procedures in the country in dealing with spam, which undoubtedly cannot be as effective as the law approved by the parliament. For this reason, there is a need to enact laws or special provisions in the country in the field of spam. In drafting such law or provisions, it is necessary to clearly state the concept of spam and to prohibit sending it without the prior consent of consumers. Also, it is necessary to establish a specialized institution for the implementation of the law and to provide appropriate civil and criminal remedies and sanctions for the obligations specified in the law.

Keywords: Spam, Commercial Advertisements, Unsolicited Commercial Message, Opt-in Method, Opt-out Method.

دانشنامهٔ حقوق اقتصادی

Homepage: https://lawecon.um.ac.ir

مقالهٔ پژوهشی

دوره ۳۰، شماره ۲٤، پاییز و زمستان ۱٤۰۲، ص ۷۸-٦۳

پیام تجاری ناخواسته (اسپم): ممنوعیت یا آزادی ارسال؟

مصطفی بختیاروند[۱]* - سید محمد هادی قبولی درافشان[۲]

دریافت: ۱٤۰۲/۰۸/۱۷ پذیرش: ۱٤۰۲/۱۱/۲٦

چکیده

پیام‌های تجاری ناخواسته (اسپم) به‌صورت الکترونیکی و انبوه، بدون رضایت گیرنده، از طریق ابزاری چون رایانامه یا پیامک ارسال می‌شوند. اسپم در کنار مزایایی که برای تبلیغ‌کنندگان دارد، می‌تواند موجب نقض حریم خصوصی کاربران اینترنت و تلفن همراه شود و زیان اقتصادی و نارضایتی گستردهٔ مصرف‌کنندگان و حتی تجار را در پی داشته باشد. امری که در کنار احتمال اخلال در عملکرد سامانه‌های مرتبط، ممکن است به بی‌اعتمادی نسبت به تجارت الکترونیکی و اقتصاد دیجیتال منجر شود. نتایج این مقاله توصیفی-تحلیلی نشان می‌دهد برخی کشورها ارسال اسپم را حتی بدون رضایت مخاطب، مجاز و مخالفت بعدی وی را مانع ارسال می‌دانند که روش آن‌ها شیوهٔ کناره‌گیری نامیده می‌شود.کشورهای دیگر، اعلام رضایت قبلی مخاطب را ضروری می‌دانند؛ این راهبرد به شیوهٔ مشارکتی معروف است. دو شیوه یادشده، از طریق سه رویکرد تقنینی همراه با تساهل، معتدل و سخت‌گیرانه اعمال می‌شود که با توجه به نحوهٔ برخورد با ارسال‌کنندگان اسپم و ضمانت‌اجراها، تقسیم‌بندی و نام‌گذاری شده‌اند. موضع حقوق ایران راجع به ممنوعیت یا مجازبودن ارسال اسپم چندان واضح نیست. در این مقاله، تصویب قانون یا برخی مواد قانونی صریح و شفاف راجع به اسپم با اتخاذ شیوهٔ مشارکتی و پیش‌بینی ضمانت اجراهای کارآمد در ایران پیشنهاد شده است.

کلیدواژه‌ها: اسپم، تبلیغات تجاری، پیام تجاری ناخواسته، شیوه مشارکتی، شیوه کناره‌گیری.

طبقه بندی JEL: K23,K24

[۱]. دانشیار گروه حقوق خصوصی و حقوق مالکیت فکری دانشگاه قم، قم، ایران.

[۲]. (نویسنده مسئول: E.mail: m.bakhtiarvand@qom.ac.ir)

[۳]. دانشیار گروه فقه و مبانی حقوق اسلامی دانشگاه فردوسی مشهد، مشهد، ایران.

مقدمه

صاحبان کسب و کارها برای تبلیغ محصولات خود از روش‌های متنوعیاستفاده می‌کنند . جذب مشتریان و موفقیت در فروش کالا یا خدمت، بدون راهبرد و شیوه مناسب تبلیغاتی، امری تصورناپذیر است. ارسال پیام‌های تجاری ناخواسته به‌عنوان یکی از ابزار رایج برای معرفی کالا و خدمت به مخاطبان محسوب می‌شود. اگر چه زمانی گفته می‌شد پیام تجاری ناخواسته به یک نوع مزاحمت برای همهٔ کاربران پست الکترونیکیی تبدیل شده (Parker,2006:628)، امروزه دامنه پیام‌های ناخواسته تبلیغاتی به پیام‌های متنی تلفن‌های همراه هم گسترش یافته است. ارسال پیام‌های ناخواسته عمدتا با اهداف تجاری و بازاریابی انجام می‌شود (Serna,2022:1). در ژانویه ۲۰۲۳، بالاترین آمار رایانامه‌های تجاری ناخواسته (اسپم) در آمریکا با ۸ میلیارد مورد در روز بوده است.[1]

ارسال پیام‌های تجاری ناخواسته، می‌تواند مشکلات متعددی را ایجاد کند. برای نمونه، صرف نظر از مشتمل بودن بر اطلاعات غیرضروری یا غیرمرتبط، اسپم در مواردی دریافت‌کننده را به پیوندهای[2] معین یا نشانگرهای یکنواخت منبع[3] هدایت می‌کند که در صورت کلیک کردن، شخص را با بدافزار یا ویروسی مواجه می‌کند که می‌تواند به سامانه مخاطب آسیب برساند یا داده‌های وی را برباید (Prasetia,Istambul,2021:682). به‌علاوه، پیام‌های تجاری ناخواسته به حریم خصوصی کاربران لطمه می‌زند (Moustakas et al, 2005:1) و مقادیر عظیمی از منابع شبکه را که برای کاربران اهمیت زیادی دارند هدر می‌دهند و زندگی روزمرهٔ آن‌ها را به شدت تحت‌تأثیر قرار می‌دهند. افراد همه روزه باید وقت زیادی را برای بررسی و حذف اسپم صرف کنند (Revar et al,2017:1). حتی در مواردی، محصولات ناقض حقوق مالکیت فکری (مانند ساعت، جواهرات یا موسیقی) یا ناقض مقررات راجع به سلامت (مانند دارو) از طریق اسپم تبلیغ و عرضه می‌شوند (Serna,2022:4). افزایش اسپم عاملی است که سهولت، قابل اعتماد بودن و کارآمدی فناوری‌های اطلاعات و ارتباطات را تهدید می‌کند و هزینه‌هایی نیز از طریق تشدید مصرف منابع شبکه برای انتقال و ذخیره پیام، به ارائه‌دهنده خدمات مخابراتی تحمیل می‌کند (APT,2022:4).

در آمریکا تعداد پیامک‌های ناخواسته ارسالی در نوامبر ۲۰۲۲، ۴۷/۲ میلیارد اعلام شده است. طبق گزارش کمیسیون تجارت فدرال، گروه‌های مصرف‌کننده، خسارت ۲۳۱ میلیارد دلاری ناشی از تقلب‌های صورت گرفته با استفاده از پیامک را در نه ماه اول ۲۰۲۲ گزارش کرده‌اند (FCC,2023:4).[4] در ایران نیز کاربران رایانامه و تلفن‌های همراه از زیان‌های پیام‌های تبلیغاتی تجاری در امان نمانده‌اند و دریافت چنین پیام‌هایی برای کاربران به امری عادی تبدیل شده است و بنابراین، ساماندهی این نوع تبلیغات ضرورتی انکارناپذیر تلقی می‌شود.

تا کنون، تلاش‌های تقنینی زیادی برای مقابله با اسپم انجام شده است و کشورها یا ارسال اسپم را آزاد اعلام کرده‌اند و به گیرنده، حق اعلام مخالفت با این امر را می‌دهند (شیوهٔ کناره‌گیری) یا رضایت قبلی مخاطب را برای ارسال اسپم ضروری می‌دانند (شیوهٔ مشارکتی). جهت اجرای دو شیوه بالا، سه رویکرد تقنینی شکل گرفته است که عبارت است از: رویکرد همراه با تساهل، معتدل و سخت‌گیرانه. در عین حال، اقدامات تقنینی تأثیر زیادی در کاهش ارسال اسپم نداشته‌اند. علت این امر را بیشترباید در ماهیت جهانی مشکل نبود تدابیر بین‌المللی و آگاهی نداشتن کاربران از مسأله جستجو کرد (Serna,2022:2). اگرچه «بیل گیتز» در سال ۲۰۰۴، وعده داده بود که اسپم طی دو سال ریشه‌کن خواهد شد،[5] این وعده هیچ‌گاه محقق نشد. با ظهور فناوری‌های نوین، شیوه‌های جدید و خطرناک ارسال اسپم شکل گرفته‌اند که وب جهانی و شبکه‌های اجتماعی را تحت‌تأثیر قرار می‌دهند و موجب می‌شوند وضعیت اضطراری در این زمینه همچنان پابرجا باشد (Ferrara,2019:1).

با عنایت به آنچه که گفته شد، پرسش اصلی مقاله حاضر به شرح ذیل طرح شده است: «شیوهٔ تقنینی مناسب برای ایران در مواجهه با پیام تجاری ناخواسته الکترونیکی (اسپم) کدام است؟». برای پاسخگویی به پرسش مذکور، ابتدا مفهوم اسپم را بیان می‌کنیم و در ادامه تاریخچه آن ذکر می‌شود. سپس، به منظور یافتن بهترین راهکار برای حقوق ایران، رویکردهای تقنینی موجود در مواجهه با اسپم، بررسی و تحلیل خواهد شد.

---

[1] https://www.statista.com/statistics/1270488/spam-emails-sent-daily-by-country/ (last visited: 12/15/2023).

[2] Links

[3] URLs

[4] Federal Communications Commission.

[5] https://www.nytimes.com/2004/01/26/business/gates-predicts-that-spam-will-go-away.html (last visited: 11/14/2023).

۱. مفهوم اسپم

اسپم علامت تجاری گوشت کنسروشده‌ای است که توسط شرکت هورمل فودز[1] تهیه می‌شود. اما کلمهٔ یادشده ، به‌طور غیرمستقیم، بر کاری دلالت می‌کند که چنان تکرار می‌شود که موجب آزار شدید می‌شود. (Arunkrishna,Mukunthan,2020:826) اسپم در مفهوم مقاله حاضر از قطعه‌ای از یک فیلم طنز راجع به محصول فوق‌الذکر گرفته شده که در آن، گروهی از افراد، عبارت «اسپم، اسپم، اسپم ...» را به‌طور مداوم به‌گونه‌ای همسرایی می‌کردند که مانع شنیده‌شدن مکالمات دیگر می‌شد (Reyero,2007:196). تکرار ملال‌آور کلمهٔ اسپم موجود در منوی غذا در قطعه مذکور، موجب عصبانیت پیشخدمت رستوران نیز شده بود. از آن زمان، اسپم برای توصیف آزار و حالت انزجار ناشی از تکرار مداوم یک چیز به‌کار می‌رود. در مورد اینترنت، منظور از اسپم برخط ایجاد مزاحمت از طریق ارسال پیام‌های ناخواسته به کاربران است. اسپم برخط، کاربران را کلافه می‌کند و برای آن‌ها، حمله بدافزارها، نفوذ و رمزگیری را در پی دارد (Arunkrishna,Mukunthan,2020:826).

روش تعریف اسپم در قانون اهمیت زیادی دارد. ارائه تعریف مضیق از اسپم یا عدم شمول تعریف آن بر انواع مهمی از فعالیت‌های ناقض ممکن است مانع رسیدگی مطلوب به مشکل اسپم شود. در مقابل، اگر قانون قلمرو موسعی داشته باشد ممکن است حقوق بیان تجاری[2] را که از رهگذر حمایت‌های مقرر برای آزادی بیان تضمین شده‌است محدود کند. بنابراین، تعریف اسپم باید تعادل مناسبی بین دو امر یادشده برقرار کند (Dong, Jayakar,2013:12).

همانطور که به درستی گفته شده است تلاش برای ارائه یک تعریف منحصر به یک زمان خاص احتمالا بیهوده خواهد بود زیرا ماهیت مشکل با همان سرعت تغییر فناوری اینترنت و برنامه‌های کاربردی تغییر خواهد کرد. برای نمونه، افراد و سازمان‌های ذیربط، بیان می‌کنند که اسپم به فناوری‌های تلفن همراه مانند پیامک و پیام چندرسانه‌ای گسترش یافته است (Internet Society,2012:1).

دقیق‌ترین تعریف اسپم، تعریفی است که الزامات متعددی را در برداشته باشد، از جمله اینکه باید یک پیامِ شخصی نشده باشد که در آن، هویت و شرایط دریافت‌کننده اهمیتی نداشته باشند، پیامی باشد که برای بسیاری از دریافت‌کنندگان دیگر هم ارسال شده باشد، دریافت‌کننده اجازه ارسال پیام را نداده باشد و در مواردی، پیام، مشتمل بر جایزه یا پاداش غیرواقعی برای دریافت کننده باشد (Serna,2022:3).

تاریخچه اسپم نشان می‌دهد که این موضوع صرفاً به رایانامه‌ها محدود نمی‌شود بلکه فناوری‌های ارتباطی دیگر از قبیل پیامک را در بر می‌گیرد (Mosing,2014:4). این پدیده، در حال حاضر، نه تنها تبلیغ از طریق رایانامه را تحت‌تأثیر قرار می‌دهد، بلکه ارسال و دریافت انبوه پیام‌های تبلیغاتی ناخواسته به حوزه‌های دیگر مانند شبکه‌های اجتماعی یا برنامه‌های پیام‌رسانی فوری نیز گسترش یافته است(Serna,2022:2). بنابراین، برای توصیف اسپم، اشاره به محتوای ناخواسته انبوه پیشنهاد شده است (Mosing,2014:4). بر اساس بخش سه قانون فدرال کنترل تهاجم هرزه‌نگاری و بازاریابی ناخواسته ۲۰۰۳ (قانون کن اسپم) [3] آمریکا، «پیام رایانامه‌ای تجاری عبارت است از رایانامه‌ای که هدف اصلی آن تبلیغ یا ترویج محصول یا خدمت تجاری است (از جمله محتوای یک تارنمای اینترنتی که با هدف تجاری اداره می‌شود)».

در اتحادیه اروپایی، دستورالعمل حریم خصوصی و ارتباطات الکترونیکی،[4] اصطلاح اسپم را تعریف نکرده و آن را به‌کار نبرده است. دستورالعمل یادشده، مفهوم ارتباطات الکترونیکی از طریق رایانامه با هدف بازاریابی مستقیم[5] را به‌کار برده است که به‌طور کلی و در عمل، بیشترِ انواع اسپم را دربرمی‌گیرد. البته مفهوم رایانامه در دستورالعمل، صرفا شامل رایانامه سنتی نیست و پیامک، پیام چندرسانه‌ای و هر نوع ارتباط الکترونیکی را که مشارکت همزمان فرستنده و دریافت‌کننده برای آن ضرورت ندارد دربرمی‌گیرد (Commission of the European Communities,2004:9).

---

[1] Hormel Foods.

[2] بیان تجاری عبارت است از هر بیانی که حداقل نوعی تجارت را تبلیغ کند. برای مطالعه بیشتر در این زمینه نک.
https://www.law.cornell.edu/wex/commercial_speech
(last visited:11/10/2023)

[3] The Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM) Act of 2003 (CAN-SPAM Act).

[4] 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 (E-Privacy Directive).

[5] Unsolicited Communications for Purposes of Direct Marketing.

برخی نویسندگان، ویژگی‌های اساسی اسپم را به شرح زیر بیان کرده‌اند: الف- درخواست‌نشده از سوی دریافت‌کننده؛ ب- ماهیت تجاری داشتن؛ و ج- ارسال به طور عمده (Juneja,Pateriya,2014:1). بنابراین، به نظر نگارندگان، تعریف زیر از اسپم می‌تواند مناسب باشد: «پیام تبلیغاتی تجاری الکترونیکی انبوه که بدون درخواست مخاطب برای وی ارسال می‌شود». بدیهی است که این مقاله بر پیام‌هایی متمرکز است که محتوای تجاری داشته باشند و در اصطلاح اسپم تجاری تلقی شوند.

۲. تاریخچه اسپم

در تاریخچه ارسال اسپم دو نقطه‌عطف مشاهده می‌شود: نخستین پیامی که به‌عنوان اسپم تلقی شد پیامی بود که توسط گری توئرک[1] یک مأمور فروش شرکت تجهیزات دیجیتال،[2] در سال ۱۹۷۸ برای ۳۹۳ کارمند آرپانت ارسال شد. شرکت یادشده در پی توسعهٔ بازار خود بود و مصرف‌کنندگانِ علاقه‌مند را به مراسم رونمایی از یک محصول جدید دعوت کرد و بدین منظور، یک پیام تبلیغاتی برای کاربران آرپانت فرستاد (Serna,2022:3). ۱۶ سال بعد، در سال ۱۹۹۴، دو وکیل از ایالت آریزونا خدمت مشاوره مهاجرت خود را از طریق ارسال پیام تبلیغاتی ناخواسته برای تقریبا همه گروه‌های بحث و تبادل نظرموجود در یوزنت تبلیغ کردند. این پیام، عمدتا با واکنش منفی کاربران مواجه شد، به این دلیل که با گروه‌های بحث و تبادل نظر هدف، ارتباطی نداشت (Hedley,2006:225).

به‌عنوان جدیدترین پدیده در این زمینه می‌توان ارسال اسپم از طریق هوش مصنوعی را ذکر کرد که طی آن سامانه‌های هوش مصنوعی می‌توانند برای تقویت فعالیت‌های مشتمل بر ارسال انواع مختلف اسپم به‌کار روند (Ferarra,2019:89).

۳. رویکردهای تقنینی در مواجهه با اسپم

بسیاری از دولت‌ها و بخش اعظمی از جامعه بین‌المللی معتقدند مقابله مؤثر با اسپم بدون وضع قانون و پیش‌بینی ضمانت اجراهای مناسب ممکن نیست. در نتیجه، بسیاری از کشورها قوانین ضداسپم را تصویب کرده‌اند که البته برای اجرای آن‌ها از الگوهای متفاوتی تبعیت شده است؛ بدین ترتیب که برای مثال، ضمانت اجراهای کیفری، اقامه دعاوی مدنی توسط دولت‌ها یا حق اقامه دعوای خصوصی را برای افراد یا ارائه دهندگان خدمات اینترنت پیش‌بینی شده‌است. با وجود این، برخی اشتراکات در قوانین ضداسپم ملاحظه می‌شود؛ به‌طوری‌که بیشتر قوانین، رایانامه ناخواسته را هنگامی غیرقانونی می‌دانند که هویت فرستنده را مخفی، از نام دامنه شخص ثالث به‌طور غیرمجاز استفاده یا اطلاعات گمراه‌کننده‌ای را در قسمت موضوع رایانامه ارائه کند. به‌طور کلی، این قوانین یا شیوهٔ کناره‌گیری (یا اعلام انصراف)[3] را اتخاذ می‌کنند که در آن، گیرنده می‌تواند از دریافت پیام‌های بعدی اعلام انصراف کند یا شیوهٔ مشارکتی[4] را که مستلزم اجازه قبلی است به‌کار می‌برند. بسیاری از قوانین یادشده فرستندگان را ملزم می‌کنند خود را به‌صورت واضح و دقیق معرفی کنند (Potashman,2006:332).

بسته به روش اجرای هر یک از شیوه‌های فوق، رویکردهای عمده تقنینی را در مواجهه با اسپم می‌توانیم به سه دسته تقسیم کنیم (Serna,2022:5-7):

نخست: رویکرد همراه با تساهل ایالات متحده؛

دوم: رویکرد معتدل اتحادیه اروپایی؛

سوم: رویکرد سختگیرانه که در کشورهایی چون استرالیا و کره جنوبی از آن تبعیت می‌شود.

۱.۳. رویکرد همراه با تساهل[5] در حقوق آمریکا

قانون کن اسپم، مهم‌ترین قانون ضد اسپم در آمریکا است که در پی مشکلات فزاینده ناشی از اسپم و هزینه‌های هنگفت مبارزه با آن توسط کنگره به تصویب رسید (Reyero,2007:200). این قانون بر قوانین ایالتی که به‌طور صریح به اسپم می‌پردازند حاکم است (Figliola,2007:2). نکتهٔ قابل‌توجه این است که قانون یادشده، رایانامه‌های تجاری ناخواسته را ممنوع نمی‌کند، بلکه الزاماتی را برای فرستندگان چنین رایانامه‌هایی مقرر و مجازات‌هایی را برای ناقضان تعیین می‌کند و به دریافت‌کنندگان اجازه می‌دهد عدم ارسال آن‌ها را از فرستندگان درخواست کنند (Moore,May,Coolins,2011:257). در ادامه، الزامات ارسال رایانامه‌های تجاری مطابق قانون مذکور و نقدهای وارد بر آن را بررسی می‌کنیم.

۱.۱.۳. الزامات عمده قانون کن اسپم برای ارسال رایانامه‌های تجاری

مطابق قانون کن اسپم، فرستندهٔ پیام باید به‌وضوح و به‌نحو مشخصی اعلام کند که پیام ارسالی، تبلیغاتی است.[1] این قانون،

[1] Gary Thuerk

[2] Digital Equipment Corporation

[3] Opt-out

[4] Opt-in

[5] Soft Approach.

منظور از این اصطلاحات را بیان نکرده است اما از دیدگاه کمیسیون تجارت فدرال، باید دید که آیا خواننده متعارف (بدون این فرض که خواننده همه رایانامه را خواهد خواند) متوجه می‌شود رایانامه تبلیغاتی است یا خیر (Mathews,2004:11). در صورتی که دریافت‌کننده، رضایت ایجابی پیشین خود را مبنی بر دریافت پیام اعلام کرده باشد، حکم فوق اعمال نخواهد شد.[۲] منظور از رضایت ایجابی این است که دریافت‌کننده در پاسخ به یک درخواست واضح و مشخص برای اخذ چنین رضایتی یا بدون وجود چنین درخواستی، به‌طور صریح به دریافت پیام رضایت داده باشد و اگر پیام از طرف شخصی جز شخصی است که دریافت‌کننده رضایتش را به او اعلام کرده، در زمان اعلام رضایت، به‌صورت واضح و مشخص به وی اخطار شده باشد که نشانی رایانامه‌اش ممکن است با هدف ارسال رایانامه‌های تجاری به شخص مذکور منتقل شود.[۳]

مطابق قانون یادشده، رایانامه تجاری باید یک نشانی رایانامه فعال یا شیوه دیگر مبتنی بر اینترنت را در برداشته باشد که به‌طور واضح و مشخص نمایش داده شود و دریافت‌کننده بتواند، به روش تصریح شده در پیام، از آن برای درخواست عدم دریافت رایانامه‌های تجاری بعدی از فرستنده مذکور به مقصد نشانی الکترونیکی که پیام برای آن ارسال شده است، استفاده کند.[۴] بنابراین، پیام باید به زبان واضح و مشخص که توسط شخص متعارف به‌راحتی قابل درک، خواندن و فهم باشد توضیح دهد که دریافت‌کننده چگونه می‌تواند از دریافت رایانامه‌های بعدی اعلام انصراف کند.[۵] ارسال‌کنندگان رایانامه‌های تبلیغاتی می‌توانند فهرستی را ایجاد کنند که به دریافت‌کننده اجازه می‌دهد از دریافت انواع معینی از پیام‌ها کناره‌گیری کند، اما فهرست باید شامل گزینه متوقف کردن تمامی پیام‌های تبلیغاتی از فرستنده نیز باشد.[۶]

فرستنده مکلف است نظر مخالف دریافت‌کننده را نسبت به دریافت رایانامه‌های تبلیغاتی، طی ده روز کاری بپذیرد.[۷] پذیرش باید بدون هیچ قید و شرطی از قبیل الزام به پرداخت هزینه یا ارائه اطلاعات هویتی باشد.[۸] به‌علاوه، فرستنده نمی‌تواند نشانی رایانامه مخاطب را با هدفی جز رعایت قانون، به دیگری منتقل کند.[۹]

۲.۱.۳. نقد رویکرد قانون کن اسپم

همانطور که در بالا ملاحظه شد، رویکرد قانون کن اسپم، مبتنی بر شیوهٔ کناره‌گیری است که طبق آن، ارسال‌کنندگان اسپم حق دارند هر دریافت‌کننده‌ای را آماج پیام‌های تبلیغاتی کنند مگر اینکه از آن‌ها درخواست شود که ارسال اسپم را متوقف کنند (NG,2005:466). در شیوهٔ کناره‌گیری، معمولا یک پیوند برای دریافت‌کننده جهت کلیک کردن، یک نشانی جهت ارسال رایانامه یا حتی یک شماره تلفن برای تماس گرفتن با هدف حذف نشانی رایانامه دریافت‌کننده از فهرست رایانامه ارسال‌کننده اسپم فراهم می‌شود. اگرچه از دیدگاه عملی همه پیام‌های ناخواسته نوعی ساز و کار حذف را در بردارند، بسیاری از این سازوکارها، حتی با وجود به‌کارگیری، به حذف اسپم کمک نمی‌کنند. هنگامی‌که دریافت‌کننده، سازوکار اعلام کناره‌گیری را به‌کار می‌برد، عمل او در واقع تأیید وجود و اعتبار نشانی رایانامه‌اش است و بنابراین، حاکی از این است که شخصی که در عالم خارج وجود دارد، پیام را دریافت می‌کند و می‌خواند. لذا، حتی در فرضی که ارسال‌کننده اسپم، نشانی دریافت‌کننده را از فهرست خود حذف می‌کند، اطلاعات ارزشمندی را راجع به دریافت‌کننده به‌دست آورده است (Serna,2022:5-6).

هر گاه الگوی انفرادی اعلام کناره‌گیری پذیرفته شود، دریافت‌کنندگان اسپم هزینه پاسخگویی به هر رایانامه را جهت درخواست صریح حذف شدن از فهرست فرستنده متحمل خواهند شد. با عنایت به رشد فزاینده رایانامه‌های اسپم، این امر ممکن است تکلیف غیرمنصفانه‌ای را بر عهده مصرف‌کنندگان بگذارد. به‌علاوه، مخالفان شیوهٔ کناره‌گیری این پرسش را مطرح می‌کنند که چرا دریافت‌کنندگان باید ملزم باشد خود را از فهرستی که هیچ‌گاه خواستار عضویت در آن نشده‌اند حذف کنند. طبق برخی مطالعات، یک چهارم

---

[1] CAN-SPAM Act § 5(a)(5)(A)(i).

[2] CAN-SPAM Act § 5(a)(5)(B).

[3] CAN-SPAM Act § 3(1).

[4] CAN-SPAM Act § 5(a)(3)(A)(i).

[5] https://www.ftc.gov/business-guidance/resources/can-spam-act-compliance-guide-business (last visited: 10/10/2023).

[6] CAN-SPAM Act § 5(a)(3)(B).

[7] CAN-SPAM Act § 5(a)(4)(A)(i).

[8] https://www.ftc.gov/business-guidance/resources/can-spam-act-compliance-guide-business (last visited: 10/10/2023).

[9] CAN-SPAM Act § 5(a)(4)(A)(iv).

بازاریابان حتی پس از دریافت درخواست کناره‌گیری، ارسال اسپم را متوقف نکرده‌اند (NG,2005:467).

در جریان بحث‌های راجع به قانون کن اسپم، گروه‌های متعدد ضد اسپم استدلال کردند که قانون باید ارسال رایانامه تجاری را، جز در صورت اعلام تمایل دریافت‌کنندگان ، ممنوع کند. هشت تشکل آمریکایی طی نامه‌ای به تعداد زیادی از اعضای کنگره گوشزد کردند که شیوه اعلام کناره‌گیری موجب تضعیف کسب و کارهایی خواهد شد که به سلایق مصرف‌کننده احترام می‌گذارند و برای کسب و کارهایی که این سلایق را محترم نمی‌شمارند حمایت قانونی فراهم می‌کند (Smith,2004:11). در واقع، راهبرد اعلام کناره‌گیری، به مفهوم آزادی ارسال اسپم است و به ارسال‌کنندگان اجازه می‌دهد رایانامه‌های ناخواسته انبوه را در صورتی که گمراه‌کننده یا متقلبانه نباشند، هدف پیام را دقیقا مشخص کنند و امکان اعلام کناره‌گیری را برای دریافت‌کنندگان فراهم کنند ارسال کنند (Potashman,2006:333).

به سبب ناکارآمدی قانون ضد اسپم آمریکا، گاهی به طنز از این قانون به‌عنوان «قانون شما می‌توانید اسپم بفرستید»[1] یاد شده‌است (Dong,Jyakar,2013:3). حتی برخی نویسندگان آن را به‌عنوان یک امید واهی توصیف کرده‌اند (Reyero,2007:1). به عقیده بعضی از صاحب‌نظران، قانون کن اسپم ممکن است عملا و به‌طور ناخواسته تعداد رایانامه‌های اسپم را از طریق بیان رهنمودهای واضح راجع به رایانامه‌های مجاز افزایش داده باشد. به علاوه، برخی با تردید در کارآمد بودن قانون، یادآور شده‌اند که کمیسیون تجارت فدرال منابع کافی جهت اجرای جسورانه قانون کن اسپم را در اختیار ندارد؛ محدودیتی که در عوض قدرت، فقط به قانون هیاهو می‌بخشد (Moore,Maye,Collins,2011:257).

یکی دیگر از ایرادات عمده قانون کن اسپم این است که حق اقامه دعوای خصوصی در آن پیش‌بینی نشده و مسئولیت اصلی اجرای قانون بر عهده کمیسیون تجارت فدرال است (Boyne,2018:309). البته علاوه بر کمیسیون مذکور، دادستان‌های ایالتی و کمیسیون ارتباطات فدرال و ارائه‌دهندگان خدمات اینترنتی نیز در شرایط معینی مجری قانون محسوب می‌شوند.[2] علاوه بر این، قانون یادشده در مقایسه با مقررات جدیدتر مانند آیین‌نامه عمومی حفاظت داده اتحادیه اروپایی (که در ادامه به آن پرداخته‌ایم) ضعیف به نظر می‌رسد.

مطالعات انجام شده، کاهش قابل محسوس تعداد اسپم‌ها را از زمان تصویب قانون نشان نداده است (Potashman,2006:333).

در آمریکا، برخی ارسال‌کنندگان اسپم ادعا کرده‌اند مسدود کردن خودکار اسپم، در واقع ناقض حق آزادی بیان آنها است. اما به عقیده بعضی نویسندگان، این استدلال به راحتی خدشه‌پذیر است (Milliet,n.d:6). و در این زمینه به یک پرونده[3] استناد می‌کنند که در آن، خواندگان که ارسال‌کننده رایانامه‌های ناخواسته تجاری بودند استدلال می‌کردند صدور قرار منع ارسال اسپم، با حق آزادی بیان آنها که به موجب متمم اول قانون اساسی حمایت می‌شود در تعارض است و به مصالح عمومی لطمه می‌زند. در مقابل، قاضی اعلام کرد که تعداد بالای رایانامه‌های تبلیغاتی، قابلیت رایانه و ذخیره داده را تضعیف می‌کند، سرعت انتقال داده بین رایانه‌ها از طریق اینترنت را به‌وسیلهٔ بالا بردن ترافیک مسیرهای الکترونیکی انتقال پیام‌ها کاهش می‌دهد و موجب صرف هزینه و زمان دریافت‌کنندگان برای خواندن پیام‌های ناخواسته می‌شود. به عقیدهٔ دادگاه، اگر استدلال‌های مبتنی بر متمم اول خواندگان پذیرفته شود، قابلیت رایانامه به‌عنوان یک ابزار کارآمد ارتباطی برای بقیه جامعه به خطر می‌افتد.

همانطور که می‌دانیم، تلفن‌های همراه می‌توانند دو نوع تبلیغ تجاری ناخواسته دریافت کنند: پیام‌های متنی و تماس‌های تلفنی. اگر پیام متنی از اینترنت به تلفن و مشتمل بر نشانی از دریافت کننده باشد که به یک دامنه اینترنتی اشاره دارد[4] مشمول قانون کن اسپم خواهد بود (DEED,2023:41,Practical Law,2023:6). پیام‌های متنی که از تلفن به تلفن ارسال می‌شوند مشتمل بر دامنه‌های اینترنتی نیستند و بنابراین مشمول قانون کن اسپم و مقررات کمیسیون تجارت فدرال نیستند. پیام‌های متنی از تلفن به تلفن مشمول قانون حمایت مصرف‌کننده تلفنی هستند (DEED,2023:41).[5] اصطلاح رایانامه تجاری ناخواسته که در بیان هدف قانون کن اسپم به‌کار رفته، مؤید این نظر است. تفکیک بین دو نوع پیام متنی یادشده با انتقاد برخی صاحب‌نظران مواجه شده است که گفته‌اند دلیل واضحی برای برخورد متفاوت با پیام‌هایی که از

---

[1] You-Can-Spam-Act

[2] https://www.lexisnexis.com/lexis-practice-advisor/thejournal/b/lpa/archive/2016/11/08/complying-with-the-can-spam-act.aspx (last visited: 10/12/2023).

[3] CompuServe Incorporated v. Cyber Promotions, Inc. and Sanford Wallace 962 F. Supp. 1015, Case No. C2-96-1070 (S.D. Ohio, Feb. 3, 1997).

[4] مانند customername@wirelesscompany.com

[5] همچنین نک. https://www.ftc.gov/business-guidance/blog/2015/08/candid-answers-can-spam-questions (last visited:11/15/2023).

دیدگاه کاربر یکسان به نظر می‌رسند و تأثیر واحدی بر او دارند که به‌طور کلی عبارت است از مزاحمت، وجود ندارد. بنابراین، نویسندگان یادشده، پیشنهاد اصلاح قانون کن اسپم را مطرح کرده‌اند (Figliola,2008:8).

۲.۳. رویکرد معتدل[1] اتحادیه اروپایی

در اتحادیه اروپایی، باوجود درک آثار منفی اسپم، این پرسش همچنان مطرح بود که ارسال اسپم قانونی است یا خیر که سرانجام در جولای ۲۰۰۲، پارلمان و شورای اروپا به ممنوعیت اسپم رأی دادند (Moustakas et al,2005:3)؛ این اقدام در قالب تصویب دستورالعمل حریم خصوصی و ارتباطات الکترونیکی (دستورالعمل حریم خصوصی الکترونیکی)[2] انجام شد که قواعد جدیدی را برای ساماندهی اسپم ارائه داد (Asscher,2004:7). به موجب یادداشت توضیحی شماره ۴۰ دستورالعمل مذکور، فراهم کردن تضمین‌هایی برای مشترکان در برابر نقض حریم خصوصی آن‌ها از طریق ارتباطات ناخواسته با هدف بازاریابی مستقیم به‌ویژه به وسیله تلفن گویا، تلفکس و رایانامه و پیامک ضرورت دارد. در این راستا، ماده ۱۳ دستورالعمل، تحت عنوان ارتباطات ناخواسته، استفاده از سامانه‌های تماس خودکار، دستگاه‌های نمابر یا رایانامه با اهداف بازاریابی مستقیم را صرفا در صورتی مجاز می‌داند که مشترکان، قبلا رضایت خود را در این زمینه اعلام کرده باشند. بنابراین دستورالعمل، شیوهٔمشارکتی را اتخاذ کرده است (Papakonstantinou,2011:43) و در واقع، درخواست صریح افراد برای دریافت تبلیغات تجاری از طریق رایانامه و موارد مشابه ضرورت دارد (Moustakas et al,2005:3). اصطلاح ارتباطات ناخواسته قلمروی اعم از رایانامه دارد و در نتیجه، مواردی چون پیامک را در بر می‌گیرد (Asscher,2004:23). در این زمینه، یادداشت توضیحی شماره ۶۷ دستورالعمل EC/۱۳۶/۲۰۰۹[3] که به منظور اصلاح دستورالعمل حریم خصوصی الکترونیکی تصویب شده است اشعار می‌دارد: «تضمین‌های فراهم شده برای مشترکان در برابر تجاوز به حریم خصوصی آن‌ها از طریق ارتباطات ناخواسته با هدف بازاریابی مستقیم به وسیله رایانامه باید نسبت به پیامک، پیام چندرسانه‌ای و برنامه‌های کاربردی مشابه نیز قابل اعمال باشد».

بند شش ماده ۱۳ دستورالعمل حریم خصوصی الکترونیکی، کشورهای عضو را ملزم می‌کند ضمانت اجراهای قضایی را برای نقض ممنوعیت ارسال پیام‌های ناخواسته مقرر کنند. این تعهد به موجب دستورالعمل EC/۱۳۶/۲۰۰۹ به ماده ۱۳ افزوده شد (FRA,2018:328). به‌عنوان استثنایی بر لزوم اعلام مشارکت، بر اساس بند دو ماده ۱۳ دستورالعمل حریم خصوصی الکترونیکی، هرگاه مشتری در جریان یک خرید پیشین، اطلاعات تماس الکترونیکی خود را در اختیار شخص حقیقی یا حقوقی قرار داده باشد، وی می‌تواند اطلاعات مذکور را برای بازاریابی مستقیم محصولات مشابه خود به کار برد، مشروط بر اینکه برای مشتری امکان مخالفت بدون هزینه به هر روشی را فراهم کند. از این استثنا گاهی با عنوان نظام مشارکتی نرم[4] یاد می‌شود. البته کمیسیون اروپا تأکید کرده است که جهت پرهیز از بیهوده شدن نظام مشارکتی، استثنای مذکور را باید به‌طور مضیق تفسیر کرد (Commission of the European Communities,2004:9).

به موجب ماده ۱۷ دستورالعمل، کشورهای عضو ملزم بودند تا ۳۱ اکتبر ۲۰۰۳، شیوهٔ مشارکتی را در قوانین داخلی خود وارد کنند. نحوهٔ اعمال دستورالعمل در میان اعضای اتحادیه متفاوت است. در حالی که برخی اعضا جریمه‌هایی را برای ارسال رایانامه به مشتریان حقیقی و کسب و کارها پیش‌بینی کرده‌اند، اعضای دیگر صرفا ارسال اسپم به مشتریان حقیقی را جرم‌انگاری کرده‌اند. همچنین، اصطلاح اعلام مشارکت، تاب تفسیرهای متفاوتی را دارد. برای نمونه، در اسپانیا ارسال پیام فقط به کسانی مجاز است که اجازه قبلی خود را اعلام کرده باشند[5] در حالی‌که دانمارک ارسال پیام را جز در صورت تقاضای واقعی دریافت‌کننده غیرمجاز می‌داند (Moustakas et al,2005:3). در آلمان، تحولات رویه قضایی راجع به رقابت غیرمنصفانه، رضایت قبلی برای تمامی تماس‌ها را ضروری می‌داند، اما در ایتالیا، این رضایت به رایانامه‌های تبلیغاتی محدود می‌شود (Serna,2022:6). در فرانسه قانون اعتماد در اقتصاد دیجیتال،[6] مفاد دستورالعمل فوق را به

[1] The Intermediate Approach.

[2] E.Privacy Directive.

[3] DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009.

[4] Soft Opt-in Regime.

[5] مطابق یادداشت توضیحی شماره ۳۲ آیین‌نامه عمومی حفاظت داده اتحادیه اروپایی (که در اسپانیا لازم‌الاجرا است)، رضایت باید به‌وسیله یک عمل ایجابی واضح اعلام شود که بر موافقت آزادانه، صریح و آگاهانه شخص موضوع داده با پردازش داده‌های شخصی مربوط به وی دلالت کند. یادداشت مذکور، اعلامیه مکتوب، شامل اعلامیه الکترونیکی یا اعلام شفاهی را به عنوان مثال‌هایی از عمل ایجابی ذکر کرده است.

[6] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

نظام حقوقی فرانسه وارد کرده است. ماده ۲۲ این قانون (که ماده L. 33-4-1 قانون پست و مخابرات را اصلاح می‌کند) بازاریابی مستقیم، از جمله به‌وسیله رایانامه، با استفاده از داده‌های شخص حقیقی، را جز در صورت رضایت قبلی وی به دریافت تبلیغات مستقیم از این طریق را ممنوع اعلام کرده است.[۱]

مطابق ماده پنج آیین‌نامه عمومی حفاظت داده اتحادیه اروپایی،[۲] یکی از اصول پردازش داده، قانونی بودن آن است. ماده شش آیین‌نامه مذکور شروط قانونی بودن پردازش را بیان کرده است. طبق اولین شرط، فرد موضوع داده‌ها، باید به پردازش داده‌های شخصی خود برای یک یا چند هدف معین رضایت داده باشد. در واقع، آیین‌نامه یادشده نیز ضرورت اعلام مشارکت را برای ارسال ارتباطات مقرر کرده است.

بند یک ماده ۷۹ آیین‌نامه، حق اقامه دعوا و برخورداری از یک جبران قضایی مؤثر[۳] را برای فرد موضوع داده که معتقد است حقوق اعطایی آیین نامه به وی، در نتیجه پردازش غیرقانونی داده‌های شخصی‌اش نقض شده، پیش‌بینی کرده است. به موجب بند یک ماده ۸۲، هر شخصی که در نتیجه نقض آیین نامه ضرر مادی یا معنوی را متحمل شده باشد حق دریافت غرامت از کنترل‌گر یا پردازش‌کننده داده‌ها را خواهد داشت.

دادگاه منطقه‌ای هدلبرگ آلمان در ۱۶ مارس ۲۰۲۲ در پرونده 4S 1/21 با اعمال مواد ۷۹ و ۸۲ از آیین‌نامه عمومی حفاظت داده اتحادیه اروپایی حکم پرداخت خسارت ناشی از اسپم را صادر کرده است.[۴] در این پرونده، خواهان یک نامه الکترونیکی تبلیغاتی مرتبط با یک دوره آموزشی را دریافت کرد که به دریافت آن رضایت نداده بود. وی اعتراض خود را به فرستنده اعلام کرد. با وجود این، دو ماه بعد، او نامه الکترونیکی تبلیغاتی دیگری را برای همان دوره دریافت و متعاقبا دعوای مطالبه خسارت را به خاطر پردازش نامطلوب داده‌ها اقامه کرد. در مرحله بدوی، دادگاه به کنترل‌گر داده‌ها دستور داد ارسال نامه‌های الکترونیکی تبلیغاتی را متوقف کند ولی دعوای جبران خسارت را به دلیل عدم احراز زیان قابل‌توجه رد کرد. دادگاه منطقه‌ای هدلبرگ با نقض حکم، با استناد به ماده ۸۲ آیین‌نامه عمومی، به پرداخت ۲۵ یورو یا ۱۲ یورو و ۵۰ سنت به خاطر هر نامه الکترونیکی دریافت شده حکم داد. بنابراین، دادگاه مذکور، اصطلاح خسارت[۵] به کاررفته در ماده ۸۲ را به گونه‌ای تفسیر کرده است که ارسال دو اسپم برای ورود خسارت و توجیه اقامه دعوا، کفایت می‌کند.[۶] در مقابل این نوع نگرش، دادگاه تجدیدنظر ایتالیا در پرونده‌ای،[۷] دریافت ده رایانامه ناخواسته تبلیغاتی را طی سه سال سبب ورود خسارت تلقی نکرد و خسارت ادعایی تجدیدنظرخواه را فرضی و غیرواقعی دانست که حداکثر عبارت بود از اندکی ناراحتی و احساس عدم آرامش که به‌طور قطع قابل تحمل است و از استفاده معمولی از رایانه ناشی می‌شود. به علاوه، دادگاه به موجب ماده ۹۶ قانون آیین دادرسی مدنی ایتالیا (تحت‌عنوان مسئولیت مشدد)، تجدیدنظرخواه را به خاطر سوءاستفاده از تشریفات دادرسی به پرداخت ۱۵۰۰ یورو جریمه محکوم کرد.[۸]

۳.۳. رویکرد سخت‌گیرانه[۹] استرالیا و کره جنوبی

استرالیا یکی از کشورهایی است که رویکرد سخت‌گیرانه را در مقابله با اسپم اتخاذ کرده‌اند. مطابق قانون اسپم مصوب ۲۰۰۳،[۱۰] پیام‌های تجاری الکترونیکی مشمول قانون، هم پیام‌رسانی در بستر اینترنت مانند رایانامه و پیام‌رسانی هم‌زمان و هم پیام‌رسانی مبتنی بر تلفن همراه از قبیل پیامک و پیام چندرسانه‌ای را دربرمی‌گیرد (Bender,2006:5).

بر اساس قانون اسپم استرالیا، اشخاص نمی‌توانند پیام تجاری الکترونیکی را بفرستند که مشتمل بر یک پیوند استرالیایی[۱۱] است؛

---

[1] Est interdite la prospection directe au moyen d'un automate d'appel, d'un télécopieur ou d'un courrier électronique utilisant, sous quelque forme que ce soit, les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen.

[2] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[3] Effective Judicial Remedy.

[4] https://gdprhub.eu/index.php?title=LG_Heidelberg_-_4_S_1/21 (last visited: 11/14/2023).

[5] Damage

[6] https://focus.namirial.global/gdpr-privacy-spam-emails/ (last visited: 10/17/2023).

[7] Cassazione Civile sez. I n. 3311/17.

[8] https://sentenze.laleggepertutti.it/sentenza/cassazione-civile-n-3311-del-08-02-2017 (last visited: 11/13/2023).

[9] The Hard Approach.

[10] Spam Act of 2003.

[11] Australian Link

همچنین، استفاده از نرم‌افزار جمع‌آوری نشانی الکترونیکی یا فهرست نشانی‌های الکترونیکی جمع‌آوری شده، ممنوع است. قانون یادشده بر سه الزام عمده تأکید دارد: اخذ رضایت برای ارسال پیام‌های تجاری ناخواسته، که تداعی‌کننده رویکرد مشارکتی و به معنی غیرقانونی و قابل مجازات بودن ارسال اسپم در استرالیا است؛ درج اطلاعات دقیق راجع به فرستنده در هنگام ارسال پیام الکترونیکی ناخواسته به کاربران؛ و پیش‌بینی امکان لغو اشتراک در چنین پیام‌هایی (Serna,2022:7).

ضمانت اجراهای قانون یادشده از ارسال اخطارهای نقض قانون به فرد متخلف شروع می‌شود که در صورت ادامه نقض، ممکن است به اعمال قرارهای منع، جبران‌های مدنی و در نهایت توقیف تجهیزات مورداستفاده برای ارسال اسپم منتهی شود (Bender,2006:6). برخی مطالعات، بیانگر کاهش تعداد اسپم از زمان تصویب قانون مذکور است (Manwaring,2009:7).

در کره جنوبی، قانون بهبود اطلاعات و ارتباطات، بهره‌وری از شبکه و حفاظت داده[1] مصوب ۱۹۹۹، در سال ۲۰۱۴ مورد بازنگری اساسی قرار گرفت که مهم‌ترین تغییرات آن به شرح زیر است (Ju et al,2021:3): نخست. شیوهٔ مشارکتی جایگزین شیوهٔ کناره‌گیری شد؛ به‌علاوه، ارسال اطلاعات تبلیغاتی در صورت مخالفت و عدول از رضایت پیشین ممنوع اعلام شد؛ دوم. ارائه اطلاعات کافی برای تماس با فرستنده در هنگام ارسال اطلاعات تبلیغاتی الزامی شد و فرستنده نمی‌تواند نشانی‌های رایانامه مخاطبان را به‌طور خودکار تولید یا جمع‌آوری کند؛ سوم. فرستندگان از نصب بدافزارها منع شدند و مجازات مشدد حبس به مدت حداکثر پنج سال و جریمه حداکثر ۵۰۰۰۰ دلاری پیش‌بینی شد؛ سطح کلی مجازات در مقایسه با قبل، افزایش چشمگیری داشته است و مجازات‌های یادشده نسبت به قوانین سایر کشورها نیز در زمره شدیدترین مجازات‌ها محسوب می‌شوند (Serna,2022:8). چهارم. قانون مسئولیت بیشتری را برای ارائه‌دهندگان خدمات اطلاعات و ارتباطات از طریق الزام آن‌ها به اتخاذ تدابیر جلوگیری از ارسال اطلاعات تبلیغاتی در نظر گرفته است.

٤.٣. رویکرد حقوق ایران

در حقوق ایران، مقررات راجع به تبلیغات الکترونیکی در فصل دوم مبحث اول باب سوم قانون تجارت الکترونیکی تحت‌عنوان «در قواعد تبلیغ» بیان شده است. در این زمینه ماده ۵۵ قانون تجارت الکترونیکی مقرر می‌دارد: «تأمین‌کنندگان باید تمهیداتی را برای مصرف‌کنندگان درنظر بگیرند تا آنان راجع به دریافت تبلیغات به نشانی پستی و یا پست الکترونیکی خود تصمیم بگیرند». در مورد این ماده ذکر چند نکته ضرورت دارد: نخست. قلمرو ماده به پست سنتی و رایانامه محدود می‌شود. بنابراین، نمی‌توانیم آن را نسبت به ارسال پیامک تلفن همراه تعمیم دهیم. این در حالی است که ماده مذکور، تبلیغات کاغذی را هم در برمی‌گیرد زیرا عبارت «دریافت تبلیغات به نشانی پستی»، که در ماده ۵۵ به‌کار رفته است، به تبلیغات سنتی مربوط می‌شود. البته شاید دلیل عدم پیش‌بینی تبلیغات پیامکی در قانون تجارت الکترونیکی، رایج نبودن این نوع تبلیغات در زمان تصویب قانون بوده است، هرچند که بهتر بود قانون به گونه‌ای تدوین شود که نسبت به فناوری‌های مختلف بیطرف باشد و بتواند همه آن‌ها را دربرگیرد. به‌ویژه اینکه قلمرو اجرایی قانون تجارت الکترونیکی در ماده یک به این صورت بیان شده است: « این قانون مجموعه اصول و قواعدی است که برای مبادله آسان و ایمن اطلاعات در واسطهای الکترونیکی و با استفاده از سیستم‌های ارتباطی جدید به‌کار می رود».

دوم. ماده فوق، جهت حمایت از مصرف‌کنندگان تصویب شده است و از تأمین‌کنندگان حمایت نمی‌کند. همانطور که برخی نویسندگان گفته‌اند: این ماده «به نوبه خود، نشان‌دهنده احترام به خواسته‌های مصرف‌کننده است» (Pakzad, Azadikhah:2016:212). به موجب بند «س» ماده دو قانون تجارت الکترونیکی، مصرف‌کننده «هر شخصی است که به منظوری جز تجارت یا شغل حرفه ای اقدام می‌کند».

سوم. قانون‌گذار، تأمین‌کنندگان را مکلف کرده است تهمیداتی را جهت تصمیم‌گیری در خصوص دریافت یا عدم دریافت تبلیغات برای مصرف‌کنندگان فراهم کنند. دقت در متن ماده نشان می‌دهد زمان انجام تکلیف مذکور و فراهم کردن امکان تصمیم‌گیری به طور واضح بیان نشده است. به دیگر سخن، عبارتِ بیان‌کننده تکلیف تأمین‌کننده را می‌توان به دو صورت تفسیر کرد. نخست اینکه تأمین‌کننده می‌تواند محتوای تبلیغاتی را بدون رضایت قبلی مصرف‌کننده برای وی ارسال کند ولی مکلف است امکان مخالفت با دریافت پیام‌های بعدی را برای او فراهم کند. چنین تفسیری با راه‌حل پذیرفته شده در حقوق آمریکا، یعنی شیوهٔ کناره‌گیری، مطابقت دارد. دوم. ارسال پیام تبلیغاتی بدون رضایت قبلی مصرف‌کننده ممنوع است و تأمین‌کننده می‌تواند چنین پیام‌هایی را صرفا برای مصرف‌کنندگانی بفرستد که قبلا به طریقی، رضایت خود را اعلام کرده باشند. این تفسیر با شیوهٔ مشارکتی اتحادیه اروپایی و برخی دیگر از کشورها تناسب دارد. برداشت نخست با ظاهر ماده سازگارتر به نظر می‌رسد هر چند که تفسیر دوم با روح و هدف

[1] Promotion of Information and Communications. Network Utilization and Data Protection.

حمایتی ماده ۵۵ انطباق بیشتری دارد. در هر حال، بهتر بود قانون‌گذار حکم ارسال پیام‌های تبلیغاتی را به‌طور صریح بیان می‌کرد.

چهارم. طبق تبصره دو ماده ۷۰ قانون تجارت الکترونیکی، ضمانت اجرای تکلیف مندرج در ماده ۵۵، عبارت است از بیست میلیون ریال که با توجه به شرایط فعلی اقتصادی، مبلغ ناچیزی محسوب می‌شود و فاقد بازدارندگی است. مشخص نیست چرا قانون‌گذار که در ماده ۷۰، جریمه بیست تا صد میلیون ریالی را مقرر کرده، در تبصره دو، در مورد متخلف از ماده ۵۵، یعنی شخصی که تکلیف فراهم کردن تمهیدات تصمیم‌گیری را انجام نداده، حداقل مجازات را مناسب دیده است.

در زمینه اسپم، شورای عالی فضای مجازی، «سیاست‌های ساماندهی خدمات پیامکی ارزش افزوده و پیامک انبوه در شبکه‌های ارتباطی» را در جلسه بیست و یکم مورخ ۱۳۹۳/۱۱/۱ تصویب کرده است. ماده شش سند مذکور مقرر می‌دارد: «ارائه‌کنندگان خدمات ارتباطی باید امکان فعال‌سازی و یا غیرفعال‌نمودن دریافت پیامک‌های انبوه را برای کاربران فراهم کنند». معلوم نیست که لزوم فراهم‌کردن امکان فعال‌سازی یا غیرفعال‌سازی دریافت این نوع پیامک‌ها به معنی پذیرش شیوهٔ مشارکتی است یا تمایل شورای عالی فضای مجازی را به شیوه اعلام انصراف نشان می‌دهد.

ذکر این نکته نیز ضرورت دارد که کمیسیون تنظیم مقررات ارتباطات سازمان تنظیم مقررات و ارتباطات رادیویی، مقررات حاکم بر ارائه خدمات محتوایی پیامکی را به عنوان مصوبه شماره ۳ جلسه ۲۷۰ مورخ ۱۳۹۶/۱۱/۵، تصویب کرده است که بر اساس بند چهار ماده یک آن، پیامک و پیام چندرسانه‌ای را شامل می‌شود. به موجب بند شش مقررات مذکور، خدمات پیامکی تبلیغاتی عبارت است از «خدمات پیامکی انبوه که در آن محتوای متنی و چند رسانه‌ای با هدف تبلیغ کالا و یا خدمت موردنظر، برای مشترکین ارسال می‌شود و می‌تواند منجر به فروش خدمت و یا کالا شود».
مطابق بند دو از ماده دو مقررات یادشده، ارسال هرگونه خدمات پیامکی انبوه اطلاع رسانی و تبلیغاتی، بدون اخذ اجازه قبلی از مشترک ممنوع است. بنابراین، مقررات مذکور، به طور صریح، شیوه مشارکتی را پذیرفته است که اقدام مناسبی تلقی می‌شود. علاوه بر این، سامانه ثبت و رسیدگی به شکایات سازمان تنظیم مقررات و ارتباطات رادیویی،[1] جهت ثبت شکایت از پیامک‌های انبوه مزاحم و تبلیغاتی طراحی شده است. همچنین، امکان ارسال شماره فرستنده پیامک‌های مذکور به سرشماره ۱۹۵ وجود دارد. پیش‌بینی حق شکایت از ارسال‌کنندگان پیامک‌های تبلیغاتی نیز بیانگر تمایل به پذیرش شیوه مشارکتی است. نکته قابل‌توجه این است که مشترکین تلفن همراه می‌توانند به روش‌های معینی، درخواست عدم دریافت پیامک‌های تبلیغاتی را نزد اپراتورهای تلفن همراه، ثبت کنند.[2] لزوم ثبت تقاضا برای عدم دریافت پیامک تبلیغاتی حاکی از اتخاذ رویکرد کناره‌گیری توسط اپراتورها است که بی‌تردید، با لزوم حفظ حقوق مصرف‌کنندگان تناسبی ندارد. بدیهی است که مشترک زیان‌دیده از دریافت پیامک تبلیغاتی می‌تواند مطابق ماده یک قانون مسئولیت مدنی علیه فرستنده اقامه دعوا و خسارت مطالبه کند. علیرغم تمهیدات پیش‌بینی شده در حقوق ایران، تصویب قانون یا مواد قانونی خاصی راجع به اسپم به طوری که رافع ابهامات موجود و شامل همه احکام مرتبط باشد ضروری به نظر می‌رسد.

از دیدگاه برخی نویسندگان، در تصویب قانون راجع به اسپم باید موارد زیر در نظر گرفته شود (Bambauer et al,2005:16 et seq): تعریف دقیق و واضح محتوایی که ارسال آن ممنوع است؛ وضع قواعد مربوط به برقراری تماس با مخاطبان، بدین معنی که قانون‌گذار مشخص کند تبلیغ‌کننده برای ارسال پیام‌های تبلیغاتی ابتدا باید رضایت مخاطب را جلب کند یا می‌تواند بدون چنین رضایتی نیز پیام تبلیغاتی را ارسال کند و در صورت مخالفت گیرنده، مکلف است از ارسال پیام‌های بعدی خودداری کند؛ سازگار کردن قانون اسپم با قوانین موجود، به نحوی که قانونگذار تصمیم بگیرد قانون مدنظر، به اسپم اختصاص داشته باشد یا برخی مواد قانونی مرتبط با اسپم در ضمن قانون عام دیگری مثل حمایت از داده تصویب شوند یا چنین قانونی شامل احکام عامی باشد که اسپم را نیز دربرگیرند. همچنین تبیین رابطه احکام راجع به اسپم با قوانین دیگر ضرورت دارد و قانون‌گذار باید معین کند که ضمانت اجراهای اسپم، به موارد تصریح شده محدود می‌شود یا اینکه امکان اعمال همزمان ضمانت اجراهای مقرر در قوانین دیگر نیز وجود دارد؛ و در نهایت، پیش‌بینی ضمانت اجراهای متناسب و مؤثر، با قابلیت بازدارندگی حداکثری امری ضروری به نظر می‌رسد. البته به نظر نگارندگان، بهتر است نهادی تخصصی نیز برای اجرای چنین قانونی پیش‌بینی شود.

شایان ذکر است که «طرح حمایت و حفاظت از داده و اطلاعات شخصی» که در ماده یک، هدف از آن «صیانت از حیثیت و کرامت

[1] https://195.cra.ir / (last visited: 11/11/2023).

[2] برای نمونه نک.:

https://mci.ir/not-receiving-promotional-sms

(last visited:11/14/2023).

اشخاص موضوع داده ها و اطلاعات» اعلام شده، در ماده چهار، پردازش داده‌ها و اطلاعات شخصی را به رضایت شخص موضوع آنها مشروط کرده است. طبق همین ماده، رضایت باید پیش از پردازش، آگاهانه و مستند باشد. از آنجا که بر اساس بند ب ماده دو طرح یادشده، پردازش عبارت است از «هرگونه عملیات دستی یا خودکار بر داده‌ها و اطلاعات شخصی»، استفاده از نشانی رایانامه افراد برای ارسال پیام‌های تبلیغاتی بدون رضایت آن‌ها ممنوع خواهد بود. بررسی مواد مختلف طرح نشان می‌دهد تهیه‌کنندگان آن، ماده یا مواد خاصی را به اسپم اختصاص نداده و در واقع از رویکردی تبعیت کرده‌اند که احکام کلی پردازش داده را بیان می‌کند.

نتیجه‌گیری

ارسال اسپم شیوه جذاب و مؤثری برای تبلیغ کالاها و خدمات بنگاه‌های اقتصادی و حتی بیان افکار و عقاید مختلف و گاه، ابزاری برای ارتکاب جرایم رایانه‌ای است. ویژگی عمده چنین پیام‌هایی، ارسال انبوه آنها بدون رضایت قبلی مصرف‌کنندگان است که اغلب برای تبلیغ محصولات تجاری به‌کار می‌رود. صرف‌نظر از محتوای پیام الکترونیکی ناخواسته، ارسال آن، زیان‌های مختلفی از قبیل هدر رفتن وقت و دارایی و رنجش برای مخاطب و تجاوز به حریم خصوصی او را در پی دارد. این نوع تبلیغات اعتماد به فناوری‌های اطلاعات و ارتباطات را کاهش می‌دهد و مانعی برای توسعه تجارت الکترونیکی محسوب می‌شود. پس از گسترش ارسال اسپم و افزایش نارضایتی کاربران، کشورهای جهان در صدد مقابله با آن برآمدند که حاصل تلاش‌های آنها، دو شیوه مشارکتی و کناره‌گیری است که در قالب سه رویکرد عمده همراه با تساهل، معتدل و سختگیرانه مشاهده می‌شود. در این میان، ایالات متحده آمریکا، که طبق آمار، بیشترین پیام‌های تجاری تبلیغاتی در آنجا ارسال می‌شود، قانون خاصی را تصویب و با اتخاذ رویکرد همراه با تساهل، اصل آزادی ارسال اسپم را تأسیس کرده است. قانون مذکور، تحت شرایطی، به تبلیغ‌کنندگان اجازه می‌دهد برای کاربران، رایانامه تبلیغاتی ارسال کنند و در عین حال، آنها را مکلف می‌کند امکان اعلام عدم تمایل به دریافت این پیام‌ها را فراهم کنند. در مقابل، اتحادیه اروپایی رویکرد معتدلی را اتخاذ و ارسال اسپم را جز در صورت اعلام رضایت پیشین مخاطب یا وجود ارتباط قبلی، ممنوع اعلام کرده است. کشورهایی چون استرالیا و کره جنوبی نیز ارسال پیام‌های تجاری ناخواسته را ممنوع و ضمانت اجراهایی را برای نقض این حکم مقرر کرده‌اند که در مقایسه با کشورهای دیگر، سخت‌گیرانه و شدید تلقی می‌شود. در حقوق ایران، مطابق ماده ۵۵ قانون تجارت الکترونیکی تأمین‌کنندگان مکلف شده‌اند تمهیداتی را برای تصمیم‌گیری مصرف‌کنندگان نسبت به دریافت یا عدم دریافت تبلیغات تجاری فراهم کنند. با عنایت به عدم بیان زمان فراهم کردن تمهیدات مذکور، مشخص نیست قانونگذار ایرانی اصل آزادی ارسال اسپم را برگزیده یا همچون اتحادیه اروپایی، منافع کاربران را بر منافع بنگاه‌های اقتصادی ترجیح داده و امکان ارسال پیام برای افرادی که تمایل به دریافت آنها را داشته باشند پیش‌بینی کرده است. البته مقررات و رویه‌های پراکنده و نسبتا متنوعی در کشور در برخورد با اسپم وجود دارد که بی‌تردید نمی‌تواند به اندازه قانونی که توسط مجلس تصویب شود اثرگذار باشد. به همین سبب، نیاز به وضع قانون یا مواد قانونی خاصی در کشور در زمینه اسپم احساس می‌شود. در تدوین چنین قانون یا موادی، لازم است مفهوم اسپم به‌طور واضح بیان و ارسال آن بدون رضایت پیشین مصرف‌کنندگان ممنوع شود. همچنین، تأسیس یک نهاد تخصصی برای اجرای قانون و پیش‌بینی ضمانت اجراهای مدنی و کیفری مناسبی برای تکالیف مندرج در قانون ضروری است.

References

[1] APT (2022), Collaborative Response Measures to Prevent Unsolicited Commercial Messages (Spam) in the Asia Pacific Region, available at: https://www.apt.int/sites/default/files/2023/05/20220220-Collaborative_Response_Measures_to_Prevent_Unsolicited_Commercial_Messages_in_Asia_Pacific_Regionfinal-clean.pdf. (last visited: 12/15/2023).

[2] Arunkrishna, M, Mukunthan, B (2020), Evolutionary Traits In Digital Spam: History ,Types, Techniques and Anti Spam Solutions, International Journal of Advanced Science and Technology, v.29, n.3s, pp. 825-834.

[3] Asscher, L. F. (2004), Regulating Spam: Directive 2002/58 and Beyond, available at: SSRN: https://ssrn.com/abstract=607183. (last visited: 12/13/2023).

[4] Australian Spam Act of 2003.

[5] Bambauer, D. et al. (2005), A Comparative Analysis of Spam Laws: The Quest for a Model Law, ITU.

[6] Bender, M. R. (2006), Australia's Spam Legislation: A Modern-Day King Canute?, Working Paper No. 2, Monash University.

[7] Boyne, Sh. M. (2018), Data Protection in the United States, Oxford University Press.

[8] Commission of the European Communities (2004), 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', available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52004DC0028. (last visited: 11/10/2023).
[9] CompuServe Incorporated v. Cyber Promotions, Inc. and Sanford Wallace 962 F. Supp. 1015, Case No. C2-96-1070 (S.D. Ohio, Feb. 3, 1997).
[10] Congressional Research Service (2008), "Spam": An Overview of Issues Concerning Commercial Electronic Mail, available at:
https://www.everycrsreport.com/files/20080514_RL31953_f6f8e72738bad07a686e2e488581e7b381875096.pdf (last visited: 12/15/2023).

[11] DEED (2023), A Legal Guide To Privacy and Data Security, available at: https://mn.gov/deed/assets/a-legal-guide-to-privacy-and-data-security-2023_ACC_tcm1045-560279.pdf. (last visited: 12/10/2023).
[12] 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 (E-Privacy Directive).
[13] DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009.
[14] Dong, X. S., Jayakar, K. (2013), Can We Can Spam? A Comparison of National Spam Regulations, Telecommunications Policy Research Conference 2013.
[15] FCC (2023), Targeting and Eliminating Unlawful Text Messages, available at:
https://docs.fcc.gov/public/attachments/DOC-391239A1.pdf . (last visited: 12/15/2023).
[16] Ferrara, E. (2019), The History of Digital Spam, Communications of the ACM, v.62,n.8,pp.82-91.
[17] Figliola, P. M. (2007), "Spam": An Overview of Issues Concerning Commercial Electronic Mail, Congressional Research Service.
[18] Figliola, P. M. (2008), Text and Multimedia Messaging: Emerging Issues for Congress, Congressional Research Service.
[19] FRA (2018), Handbook on European Data Protection Law, FRA.
[20] Hedley, S. (2006), A Brief History of Spam, Information & Communications Technology Law, v.15,n.3,pp. 223-238.
[21] https://195.cra.ir/. (last visited: 11/11/2023).
[22] https://focus.namirial.global/gdpr-privacy-spam-emails/. (last visited: 10/17/2023).
[23] https://gdprhub.eu/index.php?title=LG_Heidelberg_-_4_S_1/21 (last visited: 11/14/2023).
[24] https://mci.ir/not-receiving-promotional-sms. (last visited:11/14/2023).
[25] https://sentenze.laleggepertutti.it/sentenza/cassazione-civile-n-3311-del-08-02-2017 . (last visited: 11/13/2023).
[26] https://www.ftc.gov/business-guidance/blog/2015/08/candid-answers-can-spam-questions. (last visited:11/15/2023).
[27] https://www.ftc.gov/business-guidance/resources/can-spam-act-compliance-guide-business. (last visited: 10/10/2023).
[28] https://www.law.cornell.edu/wex/commercial_speech. (last visited:11/10/2023).
[29] https://www.lexisnexis.com/lexis-practice-advisor/thejournal/b/lpa/archive/2016/11/08/complying-with-the-can-spam-act.aspx. (last visited: 10/12/2023).
[30] https://www.nytimes.com/2004/01/26/business/gates-predicts-that-spam-will-go-away.html. (last visited: 11/14/2023).
[31] https://www.statista.com/statistics/1270488/spam-emails-sent-daily-by-country/. (last visited: 12/15/2023).
[32] Internet Society (2012), Combating Spam: Policy, Technical and Industry Approaches, available at:
https://www.internetsociety.org/resources/doc/2012/combating-spam-policy-technical-and-industry-approaches/. (last visited: 11/10/2023).
[33] Iranian Electronic Commerce Act of 2002.
[34] Ju, J. et al. (2021),Can It Clean Up Your Inbox? Evidence from South Korean Anti-spam Legislation, Production and Operations Management Society, v.0,n.0, pp.1-17.
[35] Juneja, P. G., Pateriya, R.K. (2014), A Survey on Email Spam Types and Spam Filtering Techniques, International Journal of Engineering Research & Technology (IJERT), v.3, issue 3, pp.2309-2314.
[36] Korean Act on the Promotion of Information and Communications, Network Utilization and Data Protection of 1999.

[37] LG Heidelberg - 4 S 1/21.
[38] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

[39] Manwaring, K. (2009), Canning the Spam Five Years on: a Comparison of Spam Regulation in Australia and the US, *Computers & Law November 2009*, pp.5-11.
[40] Mathews, K. J. (2004), Understanding & Complying with the "CAN-SPAM" ACT, Washington Legal Foundation.
[41] Milliet, M. (n.d), The regulation of spam A theoretical and practical analysis, available at: https://www.e2m.lu/sites/default/files/files/spam.pdf. (last visited: 12/15/2023).
[42] Moore, Roy L, May, Carmen, Collins, Eric L (2011), Advertising and Public Relations Law, Routledge.
[43] Mosing, M. W. (2014), Spamming in the EU Solutions for Unsolicited Electronic Mail Ahead ?, available at: https://www.it-law.at/wp-content/uploads/2014/09/mosing-spam-eu.pdf. (last visited: 12/10/2023).
[44] Moustakas, E. et al (2005), Combating Spam through Legislation: A Comparative Analysis of US and European Approaches, International Conference on Email and Anti-Spam.
[45] NG, K. (2005),Spam Legislation in Canada : Federalism, Freedom of Expression and the Regulation of the Internet, University of Ottawa Law & Technology Journal, v. 2, n. 2, pp. 447-491.
[46] Pakzad, B., Azadikhah, M.H. (2016), The Foundations of Criminalization of Sending Unsolicited Electronic Messages, Penal Law and Criminology Studies, v.3, n.2, pp.195-217. (In Persian).
[47] Papakonstantinou, V. (2011), The Amended EU Law on ePrivacy and Electronic Communications. New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights, J. Marshall J. Computer & Info. L. v.29, issue 1, pp. 29-74.
[48] Parker, Y. M. (2006), Unsolicited Commercial E-mail, Privacy Concerns Related To Social Network Services, Online Protection of Children, and Cyberbullying, Journal of Innovations in Digital Marketing, v.3,n.1, pp. 1-11.
[49] Practical Law (2023), Direct Marketing in the US: Overview, available at: https://www.privacyworld.blog/wp-content/uploads/sites/41/2023/07/Direct-Marketing-in-the-US-Overview-5-500-4203.pdf. (last visited: 11/7/2023).
[50] Prasetia, A. R., Istambul, R. (2021), The Problems of Sending Spam E-Mails To People In Indonesia, *Turkish Journal of Computer and Mathematics Education*, v.12, n.8, pp.681-686.
[51] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural
[52] persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[53] Revar, P. et al (2017), A Review on Different types of Spam Filtering Techniques, International Journal of Advanced Research in Computer Science, v.8 n.9, pp. 2720-2723.
[54] Reyero, J. (2017), The CAN-SPAM Act of 2003: A False Hope, *SMU Science and Technology Law Review*, v. XI, pp. 195-226.
[55] Serna, F. J. A. (2022), The Legal Regulation of Spam: An International Comparative Study, Journal of Innovations in Digital Marketing, v.3,n.1, pp.1-11.
[56] Smith, M. S. (2004), "Spam": An Overview of Issues Concerning Commercial Electronic Mail, Congressional Research Service.
[57] The Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM) Act of 2003 (CAN-SPAM Act).