Journal of Innovations in Digital Marketing

ISSN: 2765-8341 | Open Access
Vol. 3, No. 1 | https://doi.org/10.51300/jidm-2022-44

LUMINOUS INSIGHTS

Check for updates

Review Article

The Legal Regulation of Spam: An International Comparative Study

Francisco José Aranda Serna

Department of Law, Faculty of Law and Business, Catholic University of Murcia, Murcia, Spain

ABSTRACT

Spam is the massive sending of messages over the Internet. This activity is carried out mainly for commercial and marketing purposes and causes a series of harm and conflicts of great relevance in the digital world. It is the responsibility of the Law to regulate this activity and protect the rights of the citizens. The objective of this article is to study this phenomenon, starting from its origin, establishing a clear definition, pointing out the most relevant types that have the greatest impact, and addressing the legal problems that derive from it. Through the analysis of documentary sources such as scientific articles, legislation, and practical guides related to spam, the different aspects of the legal systems of the most relevant countries have been reviewed to evaluate a single legal model that would allow facing the problem. Accordingly, a series of proposals and recommendations can be extracted to aim at a legal harmonization that is more adequate and more effective for the regulation of spam, as well as to point out the legal aspects at the international level that need to be improved.

KEYWORDS

digital marketing, e-mail marketing, spam, international regulation, law of new technologies

ARTICLE HISTORY

Received: 10 October 2021
Revised: 19 December 2021
Revised: 17 January 2022
Accepted: 18 January 2022

1. Introduction

In the present day, the use of new technologies is such a common practice that people are dependent on them without realizing it. Everyone is part of this "digital" society which is a product of the Digital Age and the Technological Age makes a considerable impact and causes great changes in business, marketing, industry, and in almost all activities that rely on the use of the Internet. The network has become the medium par excellence of the times to come, the Internet is undoubtedly a basic element of the society that no one can avoid and the fundamental tool that allows entering into the "Knowledge Era" (Esteban, 2001).

Advertising and publicity have grown along with the release of the Internet, and in the 21st century, it is obvious that digital marketing uses the net for selling products and services, so it is become the fundamental element of today's commerce and constitutes a revealing factor for business activity. The progressive growth of the Internet, particularly in its commercial branch related to businessmen and consumers, has led to the emergence of new ways of advertising by those who offer goods and services through it. It is an optimal way to achieve advertising objectives quickly and affordably (Jaime, 2008).

The Internet supports advertising for the development of campaigns that allows the receivers to interact in various ways, favoring the emergence of online advertising as a crucial factor for the expansion of the number of persons exposed to their messages and an extraordinary increase in their effectiveness, together with the development of new formats for dissemina-

Corresponding author:
Francisco José Aranda Serna | fjaranda@ucam.edu | Department of Law, Faculty of Law and Business, Catholic University of Murcia, Murcia, Spain.

tion, interactivity, and direct and bidirectional communication. Online activities are probably the most important element of advertising, allowing the delivery of the message in the most direct, effective, and individualized way possible, hence the Internet provides a great variety of instruments and mechanisms for advertising (González, 2003).

The Law, as a regulatory order of behaviors, is not exempt from the impact of new technologies. However, sometimes the harm caused is not compensated and certain activities remain unpunished because they are not contemplated in the legislation. One of these unpunished conducts is observed every day when people, because of spam or unwanted electronic mail, found their mailboxes invaded with advertisements that violate their privacy and intimacy (Delpech, 2001).

For years the use of e-mail, which is the medium where spamming behavior originated, has been governed by the rules of good use, morality, and social respect, standards that have been accepted and used by the majority of Internet users. These rules simply guided the user on how to send, receive and reply to e-mails, but unfortunately, when in 1978 Digital Equipment Corporation decided to send the first unsolicited commercial electronic communication to ARPANET, they did not perceive the future consequences it would trigger (Perry et al., 1988).

Since then, the fight against spam has been a task for network administrators and defenders of network quality, only in recent years has the fight against spam found allies in the legislative bodies of some countries. Concerned by the proliferation of this practice, they have devoted efforts to creating mechanisms to combat it from a legal point of view. These efforts have been insufficient mainly due to the global nature of the problem, the lack of global measures, and the lack of user awareness of the issue (Marín, 2005).

The new information technologies have changed the way people communicate, being the use of electronic mail truly transcendental. Indeed, the use of this new form of communication between people has greatly benefited organizations, facilitating internal communication among their members and also with the outside world. Spam not only affects advertising through e-mail right now, the massive sending and receiving of unsolicited advertising messages are also present in other areas, such as social networks or instant messaging applications Spamming involves all practices which use the resources of the users and also those of the Internet servers, misuse the private information of citizens, and periodically bombard them with e-mail messages that were never requested, advertisements, chain messages, information with viruses, or merely notices that are of no interest (Wu & Geylani, 2020).

2. Methodology and objectives

This study includes the analysis of documentary sources such as scientific articles, legislation, and practical guides related to spam, the essential aspect of the information coming especially from the legislative evaluation. The information is analyzed to obtain a global perspective of the subject to suggest possible explanations and gather concepts and descriptions which will allow formulating a hypothesis to recognize which spam is harmful and must be regulated. The latter might provide clues to improve the current proposals and regulations so that all the legal measures that are adopted reflect diverse points of view that stop spam not only from a legal context but from other aspects such as business or informatics. Given that spam is a global problem, the laws involved and the different perspectives presented by countries should include also aspects such as consumer protection, data protection, and others.

A comparative study is carried out to establish how spam is regulated, the jurisdictions being restricted to Europe (especially Spain), the United States, Australia, and South Korea, which are clear examples of the different approaches taken to regulate spam. The objective is to analyze the different legal mechanisms and to do a comparative study of the legal strategies that have been accomplished in the most important and relevant countries regarding spam, a study which, to the best of our knowledge, is almost nonexistent in the literature. Considering that the enactment of legal norms aimed at protecting the abusive use of information gathered and processed through the use of computers is a complex process, this investigation will help to envisage legisla-

tive proposals focused on the protection of the rights of citizens threatened by spamming.

3. Spam's framework

The first message considered as spam was sent to the 393 employees of ARPANET in 1978, the creator of this mail was Gary Thuerk, a Digital Equipment Corporation salesman. This company wished to expand its market and invited possible consumers to the launch of a new product, for this purpose they sent an advertising message to a list of ARPANET users. The information sent was of interest to some of the receivers, however, the problems it caused in the system initiated the debate on whether or not to control the mail and, in some way, to censor mass mailings (Khong, 2001).

Subsequently, the use of spam opened a door for the benefit of businesses, but at the same time, it also allowed the onset of many other conducts that favored the growth of the uncontrolled sending and forwarding of these unwanted messages, together with other security threats, such as malicious code (trojans, spyware, etc.) or phishing, all of which exposed the potential advantages of this practice but also the considerable number of adverse effects that it could cause. Solutions based exclusively on the law have proven to be only partially effective, and for this reason, they must be combined with technical mechanisms that truly help to resolve the issue (Ferrara, 2019).

3.1. Concept and characteristics of spam

The most accurate definition of spam is one that fulfills several requirements, including that it should be a non-personalized message in which the receiver's identity and context are irrelevant, being the message applied to many other receivers, that the receiver has not given the permission for the message to be sent, and in some cases, that the message contains a false prize or reward for the receiver (Hayati et al., 2010).

The Spanish Data Protection Agency currently defines spam or "junk mail" as any type of unsolicited communication sent by electronic means. Spam is thus understood as any unsolicited message that is normally intended to offer, market, or try to arouse interest in a product, service, or company, the latter being the most commonly used among the general public.

In addition to the requirements cited in the previous definition, several characteristics can be associated with this phenomenon. Though spam is sent electronically (electronic messages), being e-mail its currently main channel, messaging systems such as short messages or multimedia are already the target of spam attacks, being also present in instant messaging applications such as WhatsApp (Agencia Española de Protección de datos, 2018).

Spam is typically sent in large quantities (mass shipping) without the consent of the receiver; however, some spammers use the strategy of splitting their lists to circumvent the controls set by providers. Spam generally has a commercial purpose, nonetheless, there are also messages with other types of content that are considered spam, an example of this are messages with political content, virus shipments, deception, fake news, etc. Email addresses are obtained or sold without the consent of the owner, frequently a spammer obtains his address list illegally. Third parties use spam ware to improperly collect addresses to later sell them to spammers, and in some cases, algorithms are used which allow them to combine certain criteria to try to guess the email addresses of a specific domain (Islam et al., 2021).

Spam is commonly considered unwanted and useless by the receiver, the message is indiscriminate and without a clear objective. Many of the spam messages are repetitive and many others show slight variations to avoid detection. Spam is a mechanism used by many to promote offensive and illegal content (falsification of titles or certificates and scams) and it cannot be stopped easily. Spam receivers rarely manage to remove their addresses from spammers' lists, because of the protection mechanisms. Finally, spam is sent in a way that it is difficult to identify its origin, because consistently the message headers and source addresses are false (Marín, 2005).

3.2. Types of spam

The techniques used by spammers are increasingly ingenious, sophisticated and tend to change as the mechanisms that try to stop them evolve, for this reason, the classification of the different types of spam is complex. Some classifications are transversal,

for example, the type of spam termed "fraud to companies" corresponds to the well-known phishing (social engineering technique by which an attacker tries to acquire confidential information from a victim fraudulently, posing as a trusted third-party) or the so-called brand spoofing (a technique of spoofing the identity of the brand of an imitated company) (Ahmad et al., 2018).

There is also generically spoofing (identity or personality theft), which impersonates the person with the identification of their sensitive and confidential data that has been stolen frequently through phishing. The receivers of spam emails are not limited to email, but there is an increasing number of new forms of spam that have spread to new destination targets such as instant messaging (WhatsApp, Facebook, Twitter, etc.), through pop-up windows, or pop-ups (when browsing the Internet), in newsgroups, in forums, on blogs, they even extend to mobile telephony (via SMS or MMS). It is interesting to note that people suffer similar phenomena in their daily lives, although it is not defined as spam, these activities are carried out through systems such as fax and traditional telephone, in automatic systems for sending and receiving calls, door to door, through brochures and other promotions that reach homes or businesses, etc. (Nakum & Vaghasia, 2016).

The Spanish Data Protection Agency has proposed a classification based on the purpose pursued by spam mail. It includes spam for commercial purposes, which is considered the original form of spam, and whose intention is to spread the usefulness of a product or the possibility of acquiring it at a lower price than the market price. In some cases, the commercial spam is related to some form of crime, since products that violate intellectual property laws, patents, or health regulations are currently being offered through this procedure (medicines, watches, jewelry, or music are usually proposed) (Revar et al., 2017).

The other type of spam includes the hoax, which is an e-mail message with false or misleading content, generally sent in a chain that asks the receiver for subsequent sending continuing the chain. These hoax messages tell a somewhat credible story related to injustices, abuses, social problems, or interesting topics for the receiver, to capture email addresses (which are accumulated in the forwarding process) that will be used later as a spam destination. There is a problem with its legal regulation since it does not in itself constitute an infringement of the law, as it is not a commercial communication (Simon, 2009).

3.3. The need to regulate spam

Spam poses a compelling challenge not only for individuals that use the Internet but also for providers of the services and the international legal system. The harm caused by spam is very serious as the number of messages increases every day endangering the utility of electronic mail communication. The expenses include the time spent removing undesired messages, the cost involves wasting resources of software, hardware, and utilities conceived to stop spam, the cost of bandwidth to operate communication, and the damage to keep the data in the servers and the process required to handle the spam messages. Furthermore, there are unobservable disturbances like authentic user's messages that are incorrectly filtered by the spam blocking systems, users who stop trusting email systems because they are not reliable, and ultimately damage to Internet domains because their reputation is erroneously identified as fraudulent (Bolin, 2006).

The response to the challenges of spam has been carried out from several perspectives, including technical solutions such as filters for messages identified as spam, educational solutions or guiding users not to open spam messages, private legal steps such as trespass or breach of contract suits, and legal reforms such as laws that ban spam messages. All these measures have been insufficient to stop the flow of unwanted messages. The reason why the laws that ban spam are not efficient is that this type of electronic communication is mobile and goes beyond national barriers, posing a challenge for its legal regulation. Unlike other objects of legal regulation, spam can affect people regardless of the country in which they resided, a spammer can send a message outside his country, and there is no limit other than the use of the Internet itself (Attas, 1999).

Prevention software helps to protect systems from

spam, but this might not be sufficient to completely control the problem. As it will be analyzed, stronger legislation helps too, but to be effective, it would require national and international legislative coordination, as spammers usually work out of jurisdiction borders. The best solution to handle the danger of phishing emails is user education, which is then followed by software-based defense approaches such as protection of the network, mechanisms for authentication, and tools that the client and server can use to prevent or combat phishing attacks, such as searching-based detection, whitelisting and blacklisting (Silva et al., 2020).

4. Comparative study of the different approaches to regulate spam

The strengths and weaknesses of each relevant legislation at the international level will be analyzed in pursuance to obtain a global vision of spam regulation, emphasizing the common characteristics and the points of disagreement to detect a series of parameters that could harmonize legal regulation of spam (Bambauer et al., 2005).

In the United States, many states including also the federal government have legislated against spam, other countries in Europe have made laws under the political leadership of the European Union, and diverse countries outside the US and the EU also have legislated about the unwanted emails (Hamilton & Fleck, 2010).

The main objective of the investigation is not the pure legislative analysis of the norms, but to know the spirit of the law, taking into account the approaches of different countries regarding the regulation of spam. In this way, it will be possible to verify how the approaches of each country are different, some countries have not even carried out an effective or extensive regulation of spam while other countries have carried outlaws or directives that are very strict in this regard.

4.1. The "soft" approach: United States

The United States is the country responsible for almost 90 percent of the world's spam. By pointing to the reputation of the United States as the birthplace of spam, Internet authorities around the world have begun to question whether laws in the United States will reduce the flow of spam that originates within its borders. Some authors indicated that the existing law to date could work, while others maintain that even new laws will not stop spam, but only will act as a deterrent and that a global technical solution will be necessary in any case. At the international level, the United States is the most important country because, in addition, to having settled the ground rules for the rest of the Internet legislation, it is the one that has developed most of the regulation of electronic commerce (Klass, 2020).

Although a lot of specific anti-spam regulations are active in the United States, these laws seem to be useless right now and unaware to most. The majority of the states have some form of anti-spam regulation, but the most important anti-spam state law is the CAN-SPAM ACT of 2003[1]. For example, Alaska has a very soft law, which indicates that if the sender of sexually explicit unwanted commercial email knows that the receiver lives in Alaska, the message only has to have a header with an acronym that indicates that it has adult content (Mcnealy, 2017).

On the other hand, in California, the law states that any commercial email sent to a person that lives in that state requires explicit consent by the receiver. The legislation of many states requires a way to unsubscribe from a mailing list in their spam regulation, this rule needs some choice before an email is ever sent. In the case of California and Delaware, specific authorization must be allowed or a certain business relationship must exist for an individual to receive the message (Boyne, 2018).

The opt-out mechanism is the most frequent in United States legislation, and consists of a link for the receivers to click, or an email address to write to or even a telephone number to call, with the aim that the receiver's email address could be withdrawn from the spammer's mailing list. Although practically all spam messages already have some type of exclusion mechanism, many of these mechanisms do not serve to elim-

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

inate spam, since it persists even after they have been used. When the receiver uses the opt-out mechanism, what he is doing is confirming that his email address exists and is a valid one, therefore, indicating that a real person is receiving and reading the message. So even in the case, the spammer removes the receiver's address from his list, he already has obtained worthy information about the receiver (Scott, 2003).

The federal legislation of the United States has tried for years to improve the regulation of spam. Is distinctive of the American society that the pressure groups and lobbies participate and influence in the elaboration of the law, in this case, the most relevant lobby for the ban on spam is the Coalition Against Unsolicited Commercial Email (CAUCE). This type of association is also present in other countries, such as the EuroCauce in Europe and similar in Australia or India. Although many measures have been presented at the Senate and House of Representatives by these pro and anti-spam advocates, none of them have been converted to an effective law (Khong, 2001).

The threat of email spam is almost forty years old, and, yet, it does not appear to be disappearing. Spam has been disseminated to other Internet platforms including social media Web sites. It seems that the many State anti-spam statutes have been unsuccessful in regulating the sending of the unsolicited commercial email (Mcnealy, 2017).

4.2. The "intermediate" approach: Europe and the case of Spain

The European Commission identified four directives that are relevant in regulating spam: the General Data Protection Regulation (2018), the Telecommunications Privacy Directive (1998), the Distance Selling Directive (1998), and the Electronic Commerce Directive (2000). The European Union Directive proposes a general regulation of the provision of services of the Information Society, of commercial communications, the legal validation of the celebration of electronic contracts, specific protection of consumers, the promotion of the establishment of codes of conduct, and the out of court solution of disputes and speed in the judicial process (Agencia Española de Protección de datos, 2018).

The first anti-spam directive was adopted by the European Union in 2002, the Privacy and Communications Directive includes guidelines for an opt-in system for addressing spam in European member countries. The European members were supposed to have implemented their opt-in anti-spam legislation in 2003. Several member countries have already legislated anti-spam legislation, including Austria, Belgium, Denmark, Finland, Greece, France, Italy, Norway, Portugal, Spain, and Sweden. At present, Austria, Denmark, Finland, Germany, and Italy have laws to regulate commercial or unwanted emails. In Austria, the law requires the prior revocable consent of the receiver. In Denmark, unwanted emails are banned, it is also very similar in Finland, where sending unwanted commercial emails to private persons and newsgroups is illegal. In Germany, prior consent is required for all contacts through the development of case law on unfair competition, but in Italy, this is only confined to emails for advertising purposes (Soler, 2002).

As for the particular example of Austria, it is forbidden to send messages without the consent of the receivers, unless your address has been obtained in the context of a sale and it is used to advertise similar products. In any case, the receivers are allowed to object at any time unsolicited commercial emails, including SMS, if they are sent to more than 50 receivers or if the content of the email is for marketing purposes. It is forbidden to send messages without the data of the person on whose behalf the messages are sent or without a valid address (Iser & Brandtweiner, 2021).

In Belgium, the law introduces the opt-in system, which means that the sender of the mail is the one who must prove that the receiver consented to receive it, it is important to note that consent will not be necessary for the context of a prior contractual relationship on similar products or services. Likewise, the receiver may object at any time, nor is express consent necessary for sending spam to legal entities if the sending email addresses are impersonal. If the receiver expresses the will not receive any more advertising emails, the sender of such emails must send him a notification acknowledging that he has received the request, take the necessary measures to enforce it as well as keep an updated

list of customers who have decided not to receive advertising (Soler, 2002).

In Spain, the regulation of sending advertising by email is governed by the following rules: the LOPD 2018 and the LSSI-CE 2002[2]. On October 12, 2002, the Law on Services of the Information Society and Electronic Commerce (LSSI) came into force, it requires the express consent of the receiver as a condition before sending the advertising email. Article 21 refers to the subject, as follows: "It is forbidden to send advertising or promotional communications by email or other equivalent electronic means of communication that had not previously been requested or expressly authorized by the receivers of the same."

This norm demands one of these two requirements: that the advertising had been previously requested by the receivers, or expressly authorized by the same. The spam regulation in Spain was highly criticized by the associations of companies that operate on the Internet for considering themselves discriminated. The promulgation of the LSSI, caused great protests since it contradicted the directive 2002/58/CE of the European community according to academic, political, and business areas (Agencia Española de Protección de datos, 2018).

The LSSI is radical when it comes to regulating spam because it simply prohibits it, the LSSI provides for large fines, while other European laws are more permissive. As a way to end such discussion, Spain opted for creating the General Telecommunications Law (2014) instead of modifying the LSSI. This law establishes the right of consumers and end-users not to receive automated calls without human intervention, fax messages, emails, or data messages on fixed or mobile terminals, for direct sales purposes without having given their prior consent (Catalán, 2010).

4.3. The "hard" approach: Australia, New Zealand, and South Korea

Australia has been regulating spam since 2003, the Spam Act Australian law provides that a person must not send a commercial electronic message that has an Australian link and also prohibits the use of address-harvesting software or a harvested-address list. Australia adopted its anti-spam law in December 2003 and assented to it in April 2004[3]. The Spam Act focuses on three main requirements: consent before unsolicited communications can be sent, which, in turn, invokes the opt-in requirement making spam illegal and punishable by law in Australia; accurate sender information when unsolicited mail is sent to end-users; and an unsubscribe facility in such e-mails (Vaile, 2004).

Australian legislation enacted in 2003 provides imprisonment for cybercriminals, sentences of years in prison that may be applied to anyone who violates the security and integrity of data stored in a computer or electronic communications. The sanctions contained in the Australian SPAM act begin with a series of warnings that the subject is committing a crime, these warnings are usually continued by precautionary measures, civil penalties, and the seizure of electronic equipment. This legal regime acts as a deterrent, the Australian Federal Government reported that the overall percentage of spam originating in Australia had decreased since the enactment of this law (Bender, 2006).

Several years later and following the Australian example, New Zealand recognized the exponential global and national problem of spam, and for this reason, The Unsolicited Electronic Act (2007) was created, aimed at companies and individuals alike. It is also the responsibility of the New Zealand government and law enforcement agencies to carry out public education and law enforcement tasks about spam[4]. In New Zealand, the law protects freedom of speech, both oral and written, regardless of the nature of the message or the medium by which it is conveyed, and this is important when limiting communications via email, contrary to what happens in the case of Australia, where the law is more considered when introducing measures that can limit the use of the Internet or even when its sanction the spammers,

[2] Organic Law on Data Protection of 2018, and Law on Services of the Information Society and Electronic Commerce, commonly called the Electronic Commerce Law or LSSI of 2002.

[3] Spam Act 2003 of Australia.

[4] Unsolicited Electronic Messages Act 2007 of New Zealand.

so as not to interfere with the rights protected by law (Kellett, 2005).

Australia and New Zealand are good precedents of a jurisdiction that is conscious of the growing problem of spam and is actively implicated in establishing actions to fight spam and ensure adequate protection. Australia is also intense in the worldwide field playing its part by forming partnerships with other countries and organizations in an attempt to fight spam. The implementation of a many-sided solution has also proved to be effective in minimizing spam within Australia's borders and also limiting the spam leaving its frontiers (Bender, 2006).

South Korea's first law on the regulation of spam is the Law for the Promotion of the Use and Protection of Information on Information and Communication Networks (2001), its main objective was to prohibit advertising communications not required by users. Over the years, subsequent legislative revisions have been aimed at tightening the law and discouraging potential spammers (Chung, 2003)[5].

With the evolution of computer software, sending spam is becoming easier and users are more vulnerable, hence the Korean government carried out a major revision of the law in 2014, this date is the capital for South Korean law and represents a before and after in the regulation of spam, setting the Korean law as the strongest and most restrictive against spam from all over Asia. With the purpose of more firmly dissuading sending unsolicited messages on the Internet, this law has been subjected to successive minor revisions. However, as spamming skills expand and Internet users became more susceptible to receiving spam messages, the government took a major revision of the legislation in 2014, this revision includes several evident changes like the previously set opt-out default setting of sending commercial emails replaced by an opt-in scheme for the first time in the country (Ju et al., 2021).

Also, it became imperative to indicate the sender's detailed contact information when transmitting advertising information and the sender cannot automatically generate or collect the recipients. Also, the revision prohibited senders from installing malicious programs and enhanced punishment of imprisonment. The legislation placed more responsibility on information and communication service providers by requiring them to take measures to prevent the transmission of advertising information (Ju et al., 2021).

Korean legislation presents the following characteristics, it prohibits any advertising information that has been rejected by the receiver or whose prior consent has been denied, it is also mandatory to specifically transfer the sender's data and it is banned to make automatic lists (for example, emails), promoting corporate responsibility. Furthermore, senders are forbidden to install computer programs that contain malicious applications or those related to viruses and spyware, the sanctions can lead to imprisonment. When Korean law is compared with those of other countries, it is clear that the spam penalties are some of the toughest in the world. This legislation also makes information and communication service providers responsible, as it requires them to take measures so that no message is sent that has not been required by the receiver, this is an unprecedented novelty (Ju et al., 2021).

5. Discussion and conclusion

The legislations that the different countries have enacted on the regulation of spam differ in several aspects: on the definition of the problem; on which should be the control zone, if it is necessary to focus on the senders or the message itself; who are the authorities that must apply the laws; and which penalties should be applied to spammers. At least there is one point in common, that the laws must establish some kind of restriction, which if violated will involve a sanction for the spammer.

The debate resides in the international perspective because if the spammer is not physically in the country or the computer resources are also outside the national jurisdiction, the legislation will have problems controlling this conflict. There are also differences concerning the type of restriction that is established, so in Spain, senders are not allowed to send

[5] Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001 of South Korea.

unwanted messages by email to natural persons without their consent, while the United States does allow unwanted messages until the receivers indicate that they no longer want to receive them.

In this context, in Spain, indiscriminate spamming activities would be strictly prohibited since they would violate the law, but this would not be the case in the United States. Therefore, in the absence of a hypothetical agreement between the two countries, Spain would have a difficult time enforcing the law of a sender that lives in the United States. Therefore, it would be very necessary to establish coordination on spam legislation, making the laws more effective and being more coherent at the international level, in this way it would be clear for users what activities can be carried out and which ones cannot (Bambauer et al., 2005).

In general, laws and regulations are not proving to be effective, since spam has not decreased over the last few years, nor have been successful other types of electronic or technical measures. However, other ways seem to be promising, such as guidelines for companies to restrict uncontrolled electronic marketing, especially taking into account business reputation (the fear of having a bad business reputation, it is especially effective in Asian countries). Legislation in this regard is most effective as a deterrent than threatening with large fines and prison penalties (Moustakas et al., 2005).

International legislation has established two main procedures to address the situation of how a receiver can refuse to receive an unwanted message. One of these mechanisms is that of opt-in or voluntary subscription, in which the receiver must be the one who permits a message to be sent; the other mechanism is the opt-out or voluntary exclusion, in which the receiver must reject the reception of future messages, but at least one message has already been received. There is indeed no magic recipe against spam, the fight against spam cannot be considered merely from a legal point of view, but an approach that includes complementary organizational, behavioral, technical, and economic measures are necessary (Schryen, 2007).

Nowadays, the continued advance of technology allows smartphones to use algorithms to remove the messages that contained spam, the combination of these mathematics algorithms with the clustering elements will compose a valuable ally in the fight against spam (Peng et al., 2020).

The legislation of the different countries that have been analyzed are variable and are not clear, for that reason, if a spammer violates the legislation of their own country, but there are actors from other countries involved, the judicial process will be already complicated in advance due to this international component. Regulation of spam has many dark spots because, eventually, the judicial processes that are involved with spam are ruled by national legislation, and due to this the only task of the international factor is to assign which is the correct national legislation and therefore the competent jurisdiction. Irregularity, heterogeneity, and lack of transparency are the best allies of spamming (Schryen, 2007).

This variety of law, together with the progressive advance of new technologies, encourages spammers to carry out their activities in countries that have the softest legislation, and this implies that spammers avoid sanctions and also that they have an advantage over competitors who act by the law, which also encourages illegal advertising activities from certain countries. This issue can also create incentives for countries to develop laws that are tolerant to spam, or directly to not create laws in this regard, because doing so may have economic benefits by hosting this type of spam services. To improve and facilitate the application of the law, to specify the illegal activities, and to reduce the problem of spam, it would be very convenient to harmonize the legislation on spam by adopting, if possible, a law that is common in the most relevant aspects. This should have several benefits for most of the countries that have a problem with spamming (Bambauer et al., 2005).

The capability of anti-spam regulation also depends on the ability of law enforcement and the range of competencies held by public authorities. A crucial function in the process of applying the law is performed by the opportunities for international cooperation with internet service providers and organizations. The minimal guideline that a harmonized anti-spam regulation

should include is at least the prohibition of the abuse of e-mails for commercial purposes. The national legislation should be as technically neutral as possible, so it would be possible to apply anti-spam regulations in the case of changing technologies used for marketing purposes.

Also, the responsibility for sending spam should be carried out by operators benefiting from wrongful spam practices and not only those who make the transmission. In that sense national authorities should be given a wide range of power and opportunities, being mandatory to guarantee successful cooperation between national competent authorities. This involves authorities and laws in different areas like personal data protection and criminal and telecommunications laws (Kurek, 2017).

The advantage of having a coherent guideline for the countries would imply that the senders have an easier way to know what rules and laws are applied, and in this way, they would not have to be aware of different jurisdictions. Countries that do not have specific laws to regulate spam, could be inspired by this model to improve elements of their legislation. The authorities could enforce the laws more effectively, since sanctions, precautionary measures and agreements would be much easier to apply as they are harmonized. One of the conclusions of the comparative study is that the rules that are strict and severe work against spam, therefore the legislation that provides for illegal communications should strengthen the laws that address this type of activity. By reducing the countries that lack legislation or that allow spamming, spammers will find it more difficult to locate themselves in jurisdictions that are beneficial to them, and at the same time pressure will also be placed on those countries that do allow these activities as they would be a minority.

Funding statement

The author(s) received no financial support for the research, authorship, and/or publication of this article

Conflict of interest

No potential conflict of interest was reported by the author(s).

ORCID

Francisco José Aranda Serna
| https://orcid.org/0000-0002-5768-2773

Cite as

Aranda Serna, F.J. (2022). The Legal Regulation of Spam: An International Comparative Study. *Journal of Innovations in Digital Marketing*, 3(1), 3-13. https://doi.org/10.51300/jidm-2022-44

References

Agencia Española de Protección de datos (2018). Manual de legislación europea en materia de protección de datos. Luxembourg: Publications Office for the European Union. Retrieved from https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_es.pdf

Ahmad, S., Pathak, A., & Jaiswal, S. (2018). A survey about spam detection and analysis using users' reviews. *Malaya Journal of Matematik*, *1*, 1-4. https://doi.org/10.26637/MJM0S01/01

Attas, D. (1999). What's Wrong with "Deceptive" Advertising? *Journal of Business Ethics*, *21*, 49-59. https://doi.org/10.1023/A:1005985723779

Bambauer, D.E., Palfrey, J.G., & Abrams, D.E. (2005). A Comparative Analysis of Spam Laws: The Quest for a Model Law. Retrieved from https://cyber.harvard.edu/archived_content/publications/papers/2005_papers/Palfrey%20Bambauer%20Abrams_Comparative_Analysis_%20of_Spam_Laws.pdf

Bender, M. (2006). Australia's Spam Legislation: A Modern-Day King Canute? https://doi.org/10.2139/ssrn.916724

Bolin, R. (2006). Opting Out of Spam: A Domain Level Do-Not-Spam Registry. *Yale Law & Policy Review*, *24*, 399-435.

Boyne, S.M. (2018). Data Protection in the United States. *The American Journal of Comparative Law*, *66*, 299-343. https://doi.org/10.1093/ajcl/avy016

Catalán, R.G. (2010). La protección de los destinatarios del spam a través de la telefonía móvil: una visión práctica. *Revista Aranzadi de Derecho y Nuevas Tecnologías*, *23*, 35-45.

Chung, H.B. (2003). Anti-spam regulations in Korea. *Privacy Law and Policy Reporter*, (10), 1-1.

Delpech, H.F. (2001). *Internet: su problemática jurídica. Abeledo Perrot*. Buenos Aires: Editorial Abeledo-Perrot.

Esteban, M.L.F. (2001). Internet y los derechos fundamentales. *Anuario jurídico de La Rioja*, *6-7*, 321-356.

Ferrara, E. (2019). The History of Digital Spam. *Communications of the ACM*, *62*(8), 82-91.

González, M.D.R. (2003). Régimen jurídico de la publicidad en Internet y las comunicaciones comerciales no solicitadas por correo electrónico. *Revista de Derecho Mercantil*, *250*, 1587-1614.

Hamilton, K.L., & Fleck, R.A. (2010). Can Spam Be Legislated? *Journal of Applied Business and Economics*, *10*(5), 51-61.

Hayati, P., Potdar, V., Talevski, A., Firoozeh, N., Sarenche, S., & Yeganeh, E. (2010). Definition of Spam 2.0: New Spamming Boom. In *IEEE International Conference on Digital Ecosystems and Technologies*.

Iser, B., & Brandtweiner, R. (2021). Role of awareness to prevente personal disasters: reducing the risks of falling for phising by strengthening user awareness. In G. Passerini, F. Garzia, M. Lombardi, ... (Eds.), *Disaster Management and Human Health Risk VII: Reducing Risk, Improving Outcomes*, volume 207 (pp. 79-88). .

Islam, K., Amin, A., Islam, R., Mahbub, N.I., Showrov, I.H., & Kaushal, C. (2021). Spam-Detection with Comparative Analysis and Spamming Words Extractions. In *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)* (pp. 1-9). IEEE.

Jaime, D.J.R. (2008). Del charlatán al spam: publicidad molesta y libertad informática. Tutela judicial el consumidor y acciones de cesación. *Boletín del Ministerio de Justicia (estudios doctrinales)*, *2066*, 2537-2564.

Ju, J., Cho, D., Lee, J.K., & Ahn, J.H. (2021). Can It Clean Up Your Inbox? Evidence from South Korean Anti-spam Legislation. *Production and Operations Management*, *30*(8), 636-2652. https://doi.org/10.1111/poms.13398

Kellett, S. (2005). Legislative Definition of Spam for New Zealand. *Victoria University of Wellington Law Review*, *36*, 607-621.

Khong, W.K. (2001). Spam Law for the Internet. *The Journal of Information, Law and Technology*, *3*, 1-3.

Klass, G. (2020). False Advertising Law and New Private Law. In A. S. Gold, J. C. P. Goldberg, D. B. Kelly, E. Sherwin, H. E. Smith, ... (Eds.), *Oxford Handbook of New Private Law*. UK: Oxford University Press.

Kurek, J. (2017). Safety of Electronic Communication - Problem of Anti-spam Regulations. *Internal Security*, *9*(1), 21-37.

Marín, V.H.Q. (2005). El SPAM y otros abusos del correo electrónico. *Comunicaciones y Nuevas Tecnologías*, *1*, 143-169.

Mcnealy, J.E. (2017). Spam and the First Amendment Redux: Free Speech Issues in State Regulation of Unsolicited Email. *Communication Law and Policy*, *22*(3), 351-373.

Moustakas, E., Ranganathan, C., & Duquenoy, P. (2005). Combating Spam thourgh Legislation: a comparative Analysis of US and European Approaches. In *Second Conference on Email and Anti-Spam* CEAS.

Nakum, P., & Vaghasia, M. (2016). Survey on review SPAM detection. *International Journal of Engineering Development and Research*, *4*(4), 507-511.

Peng, L., Zhu, X., & Peng, Z. (2020). An Efficient Model for Smartphone Forensics SMS Spam Filtering. In *3rd International Conference on Hot Information-Centric Networking*.

Perry, D.G., Blumenthal, S.H., & Hinden, R.M. (1988). The ARPANET and the DARPA Internet. *Library Hi Tech*, *6*(2), 51-52. https://doi.org/10.1108/eb047726

Revar, P., Shah, A., Patel, J., & Khanpara, P. (2017). A Review on Different types of Spam Filtering Techniques. *International Journal of Advanced Research in Computer Science*, *8*(5), 2720-2723.

Schryen, G. (2007). Anti-spam legislation: An analysis of laws and their effectiveness. *Information & Communications Technology Law*, *16*, 17-32.

Scott, S. (2003). Spam Should Not be Legislated. *CiteSeerx*.

Silva, J.A.T.D., Al-Khatib, A., & Tsigaris, P. (2020). Spam emails in academia: issues and costs. *Scientometrics*, (122), 1171-1188.

Simon, H. (2009). Technologies for spam detection. *Network Security*, (1), 11-15.

Soler, J.C.P. (2002). La regulación de los correos electrónicos comerciales no solicitados en el Derecho español, europeo y estadounidense. *Revista del poder judicial*, (68), 61-103.

Vaile, D. (2004). Spam canned-new laws for Australia. *Internet Law Bulletin*, *6*(9).

Wu, Y., & Geylani, T. (2020). Regulating Deceptive Advertising: False Claims and Skeptical Consumers. *Marketing Science*, (pp. 1-19).