Consumer Protection from Abuses in Commercial Communications sent via Radiofrequency

Submitted: 28/11/2017
Revised: 19/12/2017
Accepted: 12/03/2018

David López Jiménez[*]
Eduardo Carlos Dittmar[**]

Abstract

Purpose – The aim of this work is to analyze the commercial communications sent by radiofrequency on the *bluetooth* network.
Methodology/approach/design – An analysis of Spanish and European regulations on commercial communications and data protection.
Findings – Industry self-regulation can complement (in several aspects) the regulations applied to this field.
Practical implications – The analysis in this article can be of considerable use to all actors who operate in this setting (society, and the public and private sectors).
Originality/value – This investigation emphasises the usefulness of self-regulation in the industry (codes of conduct) regarding commercial communications sent by radiofrequency. These instruments constitute an improvement on the regulations, close certain loopholes and can be updated more quickly than the law, and this can enhance user and/or consumer protection.

Keywords: Electronic communications, consumer, privacy, regulation, telecommunications.

Introduction

The development of the new information technologies has brought about a significant change in the innumerable facets of our social lives. This is clear to see in the way people relate to each other, search for information, receive commercial communications and acquire goods and/or services, mainly because of the establishment of the network of networks, which represents one of the most visible innovations of recent times.

Any company that wishes to prosper in today's competitive global market must apply new technologies to their day-to-day business activities in order to be

[*]Ph.D. (with European mention), Universidad de Sevilla (Spain), and Ph.D., Universidad Rey Juan Carlos (Spain). Research professor at the EAE Business School. Madrid, Spain. E-mail: dlopezjimenez@gmail.com.
[**]Ph.D., Universidad de Huelva (Spain). Associate Dean. EAE Business School. Madrid, Spain. E-mail: ecdittmar@eae.es.

JIMÉNEZ, D. L.; DITTMAR, E. C. *Consumer protection from abuses in commercial communications sent via radiofrequency*. **The Law, State and Telecommunications Review**, Brasilia, v. 10, n. 1, p. 37-60, May 2018. [DOI: https://doi.org/10.26512/lstr.v10i1.21499]

constantly attuned to trends in sales, through the new media technologies. In this sense, one of the most interesting aspects of the contract made with the consumer is the pre-contractual phase, which refers to all those activities developed between the parties before consent is granted for the perfection of the contract. In this phase, the consumer and/or user is normally made aware of the essential characteristics of the product and/or service that interests them, and about which they can be informed by advertising that reaches them – both by traditional or by virtual channels.

The protection that Spanish legislation affords recipients of electronic commercial communications on their mobile devices mostly derives from awareness of the supposed risks that arise when these communications are sent to a medium of communication that is owned by the recipient. In other words, in the cases we analyze, the advertisement is not sent out indiscriminately to an indeterminate collective of subjects but targeted to specific individuals in a personalized way. And for the electronic commercially-oriented message to be received by the owner of the device –in our case the mobile device- requires the sender to know a series of data that identifies that recipient or makes them identifiable.

This study focuses on the electronic communications sent for commercial purposes to mobile devices, in particular those transmitted by radiofrequency via the *bluetooth* wireless network. We do not include in our analysis the activity of file-swapping between individuals via *bluetooth* given that it is not covered by the concept of information society services as determined by Law 34/2002, 11 July, on the information society and electronic commerce services (LSSI-CE in Spanish).

Electronic commercial communications in relation to mobile devices: the effects on privacy

For advertising to be disseminated via personal mobile communication media, advertisers need to have access to databases that are not always available in the public sphere – unlike, for example, landline phone numbers (STAZI, 2004).

Mobile media have two ways in which electronic advertising communications can be received. One can be defined as traditional, as in browsing a *Web* page or opening and reading an e-mail sent to the recipient's e-mail in-tray; the other, in the case of mobile phones or devices with *bluetooth* technology, consists of receiving short text messages (SMS) and/or messages that include images and/or videos – *Multimedia Messaging System* (MMS).

In the latter cases, access to Internet, via *wifi* networks or mobile phone technology – *WAP* 2.0 –, determines that the personal information obtained when

these channels are used can be captured in a way that differs from fixed networks. In the case of mobile phones, knowing the IP – *Internet Protocol* – address associated to that device could give the sender access to a lot of personal data about the owner of that line, which is invaluable when executing personalized promotional activities.

Here is where the difficulties arise, with the possible violation of the privacy of mobile phone users. In effect, if the mere use of Internet involves risks to the user's privacy, the application of certain advertising techniques further encroaches on it, in that the user can then be identified, individualized and even monitored. Some authors (MESSÍA, 2004) have stated that mobile devices can be installed with electronic mechanisms that enable user behaviour to be monitored – such as *cookies* – which, combined with the geolocation, enable total identification of the user (PÉREZ, 2012).

According to article 3 of European Directive 2002/58/CE, the same can be applied to the treatment of personal data in relation to the provision of electronic communication services to the public on the EC's public communication networks. In application of article 4 of European Directive 95/46/EC, the national legislation applicable is that decreed by the Member State where the entity responsible for the treatment of the data is domiciled. This assumes that in the European Community, the treatment of location data is subject to the national regulations of the Member State in which the entity responsible for the data treatment is established, and not to the regulations of the Member State in which the interested party resides as a national. In the event that the body responsible for the treatment – the service provider with added value – is not established in a Member State, the location data can only be transferred from the electronic communication operator to the body responsible for the treatment under conditions established in chapter IV of European Directive 95/46/EC that relates to the transfer of personal data to third countries.

To prevent such electronic practices from flagrantly violating the prevailing legislation on personal data protection, the affected party should authorize consent and be informed of the conditions of the treatment of their data – article 9 of European Directive 2002/58. This declaration of consent should be given in a free, specific, informed and unequivocal way (LESMES, 2008). There are various ways to execute this declaration. For example, it could be done by an acceptance of the general clauses of the contract for the use of a mobile terminal or the wireless network that gives access to Internet, or by the configuration of the mobile device to enable the user to be located and, consequently, receive personalized advertising, or each time they use the service in question. In the case where consent has been given by acceptance of the general clauses, the interested parties must be able to consult the information again at a later stage, whenever

desired and in simplified form like, for example, by providing users with a dedicated section on a *Web* site.

In accordance with European Directive 2002/58/EC – Consideration 35 –, in cases where users have given their consent, users must be provided with a simple free-of-charge procedure that enables them to temporarily halt the treatment of their location data. The permanent recognition of the right to oppose treatment of location data is essential given their especially sensitive nature.

A commercial technique habitually resorted to in the case of mobile devices in general, and mobile phones in particular, is the sending of SMS/MMS. These messages can be received via the operator's network to which the phone line belongs or via *bluetooth.*

In the case of mobile phones, in order for the use of the phone number to be legal, it is necessary for the advertiser to have, as we have already mentioned, the consent of the line's owner for the purpose of the transmission of an SMS/MMS that contains a commercial message. As we shall see later, in accordance with article 21 of the LSSI-CE, if two assumptions concur, then the provision of consent will not be necessary. On the one hand, this relates to the owner of the mobile phone line being a client of a particular entity and, on the other, that the products and/or services on offer in the SMS/MMS received are similar to those that were the object of the contract in its time. It is important to note that it is a legal requirement –article 20 of the LSSI-CE-, that the word "advertising", or "advert" in the abbreviated form, must be clearly visible at the head of the commercial text or multimedia messages, and that the legal entity or natural person in whose name the messages are sent must also be clearly visible. If the electronic messages are received on the mobile device without the consent of the person affected or concordance with the assumption of article 21 of the LSSI-CE, then it will be considered an illegal act, and can therefore treated as unsolicited commercial communications, or *spam.*

Bluetooth as an instrument for sending advertising

Bluetooth is the norm or specification that defines a global standard of wireless communication that enables voice and data transmission between different devices via a radiofrequency link in mobile or static communication settings. *Bluetooth* technology has become a global technological specification for the establishment of wireless communications between portable devices, computers of all types and peripherals. Of the functionalities of this technology, and which we analyze here, the most important are data exchange and file synchronization without the devices needing to cable connected, and the sending of advertising communications (ESTRELLA, 2016; GARRIGA, 2016).

The reception of commercial communications to mobile devices with bluetooth technology needs prior consent. This must be distinguished from certain illicit techniques that have nothing to do with them. In fact, we face an issue in which illicit techniques even go ahead of the security mechanisms implemented by the technologies, in our case bluetooth. In this sense, we will mention briefly below some of them, and it must be taken into account that there are probably more in addition to those listed.

1. Bluejacking: It is a way of sending messages with personalized messages, at zero cost, to any bluetooth device, without asking permission to the owner of the device.

2. Blackdoor. This is an attack based on the idea of pairing with the victim device, and the attacker will never appear in the victim's known names list. Unless the improbable moment that the victim finds it out, the attacker is conecting to the device and will have all the privileges. These not only allow to know the information of the attacked device, but also to accede to GPRS or to Internet without the approval of the victim.

3. BlueSnarf. This is the most frequent attack in the devices equipped with bluetooth. The objective of such practice is to obtain the contact list, images, call records, entries in the calendar, identification number of the mobile terminal or IMEI (International Mobile Equipment Identity). Unlike bluejacking, which requires the interaction of the victim, bluesnarf does not need any computer program to access the mobile.

4. Bluebug. It has a more extensive and damaging behaviour than the previous one. Its purpose is to use the network operator of the mobile card in which the device is connected. This bug can make calls, send SMS, export contacts and SMS, access to Internet, and introduce new contacts.

All the abovementioned techniques constitute a clear infringement of privacy and in many cases, cause a significant economic damage. Regardless of the reproach and supression that they deserve, according to the sanctions imposed by the justice courts, the most desirable and obvious solution is to educate the potential users and raise awareness about the risks that the use of certain services may involve. We understand that this task must be carried out through initiatives that could be included in the so-called self-regulation.

The *bluetooth* terminal code as personal data characteristic

The question in this section requires a description of the concept of personal data, and this, in accordance with article 3 a) of the personal data protection law (LOPD in Spanish), must be understood as relating to any information that concerns the natural persons identified or identifiable. Based on this definition, in order for the data to be considered to be of a personal nature, it

is sufficient that the data to whom they refer can enable the person to be identifiable.

In terms of mode of operation, the devices enabled to receive messages via *bluetooth* technology contain known data of two types. These are the MAC – *Media Access Control* – the address of the device's network card, or, the name assigned to the *bluetooth* device, either personalized or by default. In the latter case, the mass-produced *bluetooth* devices normally carry the name and mobile device model of its manufacturer. For example, if we have a Nokia N73, the *bluetooth* device will carry the name of Nokia N73 by default, in reference to the brand and model of the terminal, which *a priori*, does not raise difficulties in terms of owner identification. More complicated in terms of the possible infringement of the user's privacy – which is considered risky in terms of the data revealed, but which are voluntarily provided –, would be the supposition that the *bluetooth* device is identified by the mobile phone number, the personal email address or full name of its owner. In this case, if the user activates the device and makes it visible, the user then becomes identifiable, which can lead no end of problems. Even if the user does not agree to receive commercial communications – unsolicited –, actions of an unknown nature and, consequently, even less consented, can develop that enable the behaviour of the device's user to be monitored.

It should be noted that the MAC address constitutes a unique identifier associated to the *hardware* of the mobile phone it corresponds to and these include mobile phones, laptops, video consoles, cameras, and MP3 and MP4 devices. In this case, not being linked to any personal data means that the Organic Law 15/1999, 13 December, on Personal Data Protection (LOPD) is not applicable, consequentially it would not be compulsory to register the database with the Spanish Data Protection Agency if they were going to store the MAC address in the *bluetooth* emission points. However if, via *bluetooth* technology there occurred, prior to the consent given by the affected party, a temporary access event to the databases stored on the devices to which it is connected, and if personal information was collected in order to proceed to treatment of those data, there would clearly be a case for applying the LOPD, as well as the roll-out of its rules – especially the obtaining of personal data, information on the interested parties and the creation and maintenance of personal data files.

General electronic commercial communications

Spam is understood to be all unsolicited advertising communications (which, normally, has the purpose of offering, commercializing or trying to arouse interest in a particular product, service and/or company) that deposit themselves in the user's email in-tray – one of the most widely used instruments on Internet – as well as landing in other spaces (GUILLÉN, 2005; SCHRYEN, 2007; RIVERA,

2013). The term *spam* or *spamming* – *pourriel* in French – has its origins in the ancient Anglo-Saxon practice of gifting poor quality ham – *spiced ham* – to purchasers of meat products at the butcher's, drawing attention to a product that is received but not, in principle, desired.

Although it was predicted some years ago that *spam* might disappear, reality has shown that recourse to this commercial practice that clearly invades privacy is greater than ever. The reasons that might explain the extraordinary proliferation of this type of messages are the lack of an international consensus subject to various, or even non-existent, legal interpretations, the possibility of reaching a large number of potential clients who *spammers* would not normally be able to access, and ease of use of the technological resources to hide the identity of the senders and which enable them to send huge numbers of messages, as well as low costs, etc.

The States that aim to combat *spam* through legislative means should decide first of all whether to choose an *opt-in* (consent expressed or voluntary inclusion) or *opt-out* (explicit rejection or voluntary exclusion) system. The *opt-in* option only allows commercial communications to be sent to those who had given prior specific consent. *Opt-out* allows commercial communications to be sent except in the case when the addressee rejects reception. As we shall see shortly, the *opt-in* system is most widely used in the EC while the *opt-out* system is more popular in the United States.

There are two maxims related to the sending of commercial communications that still prevail, in accordance with the LSSI-CE. On the one hand, the commercial communications disseminated electronically are subject to Organic Law 15/1999, 13 December, on the Protection of Personal Data (LOPD), with regard to obtaining data, information on interested parties, and the creation and maintenance of files – article 19 of the LSSI-CE –, and on the other, these commercial communications must be clearly identifiable, and must indicate the natural person and legal entity in whose name the communications are made, as well as including the word "advertising" or "advert", in accordance with the modification stated in Law 56/2007, 28 December, on Impulse Measurements in the Information Society, when the commercial communication is sent via electronic mail or another communication medium – article 20 of the LSSI-CE. Given that the abbreviation unequivocally informs of its advertising content, with the addressee's rights remain undiminished, the communication can be sent to small-screen devices.

However, if the intention of the legislator is, by the mention of the word "advertising" or "advert", that the intended addressee does not have to read, if the addressee deems it appropriate, the entire commercial communication or, in the best case, to proceed to opening the email, then the allusion that this word must be clearly stated at the start of the message is not understood. It would have been

better to establish the obligation that this expression be clearly stated in the message's subject area. In this way, conflicts of interpretation would be avoided that could be controversial in terms of whether the legal obligation has been complied with or not when the word advertising or advert is included but printed in small lettering at the start of the main part of the message.

The wording that currently appears in article 21 of the LSSI-CE derives from the reform that comes under the General Telecommunications Law. The regulation of commercial communications is based on a general principle: the requirement of the consent of the addressee, although there are exceptions linked in any case to compliance with certain assumptions that ensure that this is a question of extraordinary consent and which, in such a case, even guarantees that the addressee can express opposition via a simple free-of-charge procedure, as well as the transparency of the message (APARICIO, 2005). In this sense, it is important to note that the part of article 21 that we are analyzing could contradict article 15 of the LOPD (Royal Decree 1720/2007, 21 December). This article – let us not forget its regulatory nature – indicates that if the entity responsible for treatment requests the consent of the party affected, it must allow the affected party, during the process of the formation of the contract for ends that bear no direct relation to the maintenance, development or control of the contractual relation, to manifest his/her rejection of the treatment or communication of data. This precept constitutes a manifestation of the *opt-out* system. Let us take note that in any case the nature of the precept that we are analyzing – article 21 of the LSSI-CE – is more restrictive than the LOPD, as commercial communications cannot be sent out without the prior consent of the affected party, not even in the event that the data come from sources open to the public.

It is worth briefly pondering the fact that the being free-of-charge does not extend to the potential costs of transmitting this rejection of the treatment of personal data for advertising purposes, which in any case would be charged to the initial recipient, a negative aspect that is not dealt with in the LSSI-CE, but *is* covered by Consideration 41 of European Directive 2002/58/EC, although not treated in detail in its articles (VEGA, 2005).

It is important to point out that consent for the sending of electronic commercial communications must be express. It is not sufficient to be tacit. Generic authorization requests for receiving advertising in abstract are illegal, for as we have anticipated, consent must be expressly given.

It is important to note that the addressee of the commercial communications could have already given consent by virtue of different commercial practices. For example, electronic tick boxes that are ticked by default, requests for confirmation of the register operated by a particular *Web* site, etc.

We also must evaluate the fact that non-compliance with the legal requirements that we have described so far, as well as the possible legal-private effects among interested parties, constitutes an infraction that is liable to administrative sanction by the Ministry of Industry (BERCOVITZ, 2007). It should be noted that in certain suppositions, in which it is understood that the one we are examining is included, the legislation on advertising material – General Law 34/1988, 11 November, on Advertising- and Law 3/1991, 10 January, on Unfair Competition –, are both simultaneously applicable, although certain antinomies exist between the two (LARA, 2007; PÉREZ, 2008), which amount to a lack of legislative coordination (MASSAGUER, 2006), giving rise to legal uncertainty (BERNARD, 2002). Such contradictions are inadmissible (LÓPEZ, 2009).

As we have already emphasised, when electronic commercial communications are sent out without the consent of the recipient, they are by nature unwanted, and so normally defined as *spam.* Although there are certain special features, according to the technological medium and advertising format by which they are disseminated, the regulations currently in force seem to link the same consequences to this practice that infringes privacy. In other words, the electronic messages received are considered *spam* regardless of whether they have been received by electronic mail, instant messaging or SMS/MMS through the mobile operator, etc. In any case, doubts could arise given that on certain occasions the current regulations do not refer expressly to the *spam* that targets mobile devices in general.

In the European Community, there are two directives that regulate on the question we cover here. Firstly, European Directive 2000/31/EC, 8 June, relating to certain legal aspects of electronic commerce in the internal market, regulates in article 6 on the sending of electronic commercial communications without differentiating the media by which they are disseminated, while article 7 refers to the States as being able to admit or reject *spam* only via electronic mail. Secondly, article 13 of the European Directive 2002/58/EC, 12 July, relating to the treatment of personal data and privacy protection in the electronic communications sector, expressly establishes the media by which electronic commercial communications can be transmitted – electronic mail, automatic calls and fax. It is also important to emphasise that the current wording of article 13.1 of the European Directive on privacy assumes that the person is connected to the network via which the communication is transmitted, such as an SMS/MSS, a phone call, an email or a fax. This precept was reformed in the European Directive 2009/136/EC, 25 November. In any case, it might be apt, following the principle established in Consideration 4 of this directive, to allude expressly to the assumption of *bluetooth*, taking into account its special characteristics, both in the article we analyze and in Consideration 40 – or, in a new article – of the same.

In Spain, regarding the minimum established in the EC dispositions mentioned, article 21 of the LSSI-CE refers to the possibility that the electronic commercial communications can be sent by email or another equivalent medium. If we consider the meaning of the precept, one initial consequence deduced from the wording is that we have a *numerus apertus* of media by which the electronic advertising can be transmitted. The doubt, as emphasised by a certain sector of the doctrine (BRONDMO, 2001), could arise in the expression "equivalent". According to this opinion, the controversy could manifest around this expression, with the legislator using this wording to allude to an electronic communication to refer to, among others, *Web* pages, *Internet Relay Chat*, mobile phones, and videoconferencing, or a similar medium to email that allows personalized communication. The doctrinal tend that we follow (JAUME, 2010) positions itself in favour of the latter interpretation, by which it could be understood that the precept we comment on is applicable to mobile devices as well as to any other personal communication medium. A contrary opinion (SÁNCHEZ, 2007) states that, in the expression we analyze, the legislator wished to allude to messages sent to the IP addresses, in which participation between initiator and addressee is not simultaneous.

Given that the electronic communications sector is characterized by a high level of technological innovation and highly dynamic markets, it would be recommendable to adapt the legislation at EC level as soon as possible, and in a coordinated and harmonious way. Hence, it should be noted that on 25th of May 2016, the General Regulation of Data Protection (RGPD) entered into force, and it will replace the current regulations and begin to be applied since 25th of May 2018 in Spain. This period of two years aims to allow the states of the European Union, the institutions, and also companies and organizations that analyze data to be prepared and adapted for the time that the regulation can be applied. In our opinion, it seems that the Spanish law (LOPD) will still have the potential to be applied in what is outside the law of the European Union, because, among other aspects, the Community Regulation refers many times to the national legislation of the member states.

Commercial communications sent via *bluetooth*

Without prejudice to commercial electronic communications sent via *bluetooth* being subject to the legal framework we have just analyzed, there are certain special features (KOSTA, VALCKE & STEVENS, 2009) that we shall now refer to, and which should each be studied in detail.

Before considering the regulation of this intriguing question, in terms of Spanish legislation, it is important to analyze briefly what for some could be objections to the application of the European Directive on privacy – which we

have previously analyzed – to the commercial communications sent via *bluetooth.* According to this position, the Directive on privacy, despite the express mention in Consideration 40 of the validity of the principle of technological neutrality, can only be applied to the electronic communication services on public networks. In this sense, the sceptics understand that there could be considerable doubt as to whether *bluetooth* can be described as belonging to the public network given that, according to such a hypothesis, its characteristics make it private in nature. This makes it is necessary to differentiate the concepts of public communication network and private communication network (a modality which, since the end of the previous century, has gained considerable importance) which, *a priori*, does not seem to be a simple task either on EC or national level for each of the Member States. In this sense, in order for a network to be considered public, and although there are various assumptions that need to be evaluated, a decisive factor is that they are placed at the disposition of the public as potential user (JAY, 2003).

According to our understanding, it is correct that the European Directive on privacy is applied to the electronic communication services available to the public on public networks (GADZHEVA, 2008). However, in practice, notions of public communication networks and electronic communication services are rarely ever clear. Services are increasingly a combination of private and public elements and, sometimes, it can be difficult to establish whether the European Directive on privacy is applicable to a particular situation, such as *bluetooth,* for example.

We consider that, although it would be convenient to modify this European Directive in order to allude expressly to *bluetooth,* it could be that what emerges is an extensive interpretation, having assessed the special features of this new technique, in the guaranteeing of users' privacy. Nevertheless, some institutions understand that what we have here is real legal loophole.

In any case, according to article 21 of the LSSI-CE, to which we referred in the previous section, it is prohibited to send advertising or promotional communications by email or by any other equivalent electronic communication medium that have not previously been requested or expressly authorized by the addressee. Considering this precept, and that both the activation of the wireless technology – and, in this case, its visibility for all to see – and the acceptance of the promotional message – in text, audio and/or video – are activities that are completely voluntary, it is clear that the users have the power at all times to accept or reject the commercial communications sent via *bluetooth.*

We understand that there should be a clear difference between the simple request for consent for sending a file, via *bluetooth*, and the downloading of the commercial message on the mobile device, for which prior acceptance of the request would be obligatory. Only this second action, were it not requested – that is, the download took place without requiring the consent of the affected party –, could be considered a case of *spam* –a supposition that has given rise to the name

bluespam –, but not, we insist, the simple request for consent from the owner of the device in order to initiate the reception of the message on the terminal.

The operation to obtain the consent of the interested party for the consented transmission of the file could be an irritant *per se* both when a request is sought once only and, obviously, on the assumption that it is requested on many occasions, which will be met with rejections from the owner or by owner inaction after which the request for consent disappears from the terminal. In any case, we should note that this extreme can be avoided by putting certain appropriate actions into practice.

There exists an option to disconnect *bluetooth* technology, as well as to activate it as hidden or invisible to third parties. The alternatives available that do not inconvenience the user are many although, to give an example, it could be established that the sender of the messages via *bluetooth* might only connect in order to send a request for consent to those devices that necessarily had a particular name previously established with the company responsible for the commercial campaign and it would be convenient if that name or names were not in common use but, to continue with the supposition proposed, was an alphanumerical designation or even one with special characters. The specific name that owners should assign to the devices with *bluetooth* technology (if, according to the formula we have been discussing, they really want to receive the messages) would be previously indicated in a place that was visible to the company wishing to send the messages. In this way, unnecessary irritation of those not wishing to download the message would be avoided. To visualize the message, the user must first accept the download, which supposes that the user is going to observe it – an aspect that is not achieved by advertising sent indiscriminately.

We must focus on a question that we have just touched on, namely the constant control that the owner of the device has with respect to *bluetooth* technology. In effect, if the user does not want to receive messages containing advertising via *Bluetooth*, the user can act to ensure that this does not occur. Firstly, the user can completely deactivate this service, or can activate *bluetooth* in a mode that is invisible or hidden to third parties which, among other things, would mean that the user of the device can interact with other devices that are set in visible mode, although these cannot do likewise since that user's device would be completely invisible.

In the case where the user wishes to receive commercial communications from third parties on an occasional basis, the *bluetooth* device should be visible beforehand to the sender, which in itself could be interpreted as consent to receive messages of this kind. Likewise, in order to guarantee respect for the user's privacy, in all cases, before the terminal begins to download the message that the company using the *bluetooth* technology wants to send, authorization from the

owner will be requested regarding whether the user wishes to accept or reject the request. In order to further protect user privacy, another security mechanism could be implemented by which the sender of the advertising must enter a code in order to be able to interact with the potential recipient of the commercial communication. It is important to note that in practice there could arise, as a consequence of resorting to reprehensible techniques, certain problems in relation to this question. We refer to cases in which *bluetooth* devices are identifiable by the series name – generally related to the model – and the fact that the database *bluetooth* uses in order to send the commercial messages has established passwords in series, in which case, they can impinge on the security mechanisms set up by the device's owner.

Assuming that the owner of the mobile device rejects the reception of a particular message via *bluetooth*, the server that executes the transmission of the messages should register this rejection in order not to send any more communications – this is, without being an exact comparison, a question of activating an option similar to the *opt-out* system.

In terms of the question we are tackling here, it is said that users of *bluetooth* devices do not connect to the network until they have given their consent to the downloading of the file. This appreciation might not be entirely correct given that, in our judgement, devices endowed with this technology – sender and receiver – might have *bluetooth* activated with the prior restrictions on interconnection, in order not to, among other things, receive unwanted commercial communications, which assumes that they are connected to the network, although the recipient's consent will be compulsory for the reciprocal communication to be established. We consider that this would be to confuse connection to the network with the need of users of certain networks to be subscribers to a supplier of telecommunication services. This does not occur in the case of *bluetooth* since it is not necessary to contract a service supplier, it merely being sufficient for the device to possess *bluetooth* technology whose use, as we have seen, is free of charge for both parties – sender and receiver.

Although we disagree with this opinion, let's not forget a feature that distinguishes *bluetooth* from other public communication networks, such as mobile phone, fax or Internet. We refer to the fact that in these cases commercial messages, whether wanted or unwanted – in which case they will be illegal –, are received in their entirety, which obviously assumes they have been fully downloaded directly to the in-tray of the various devices. This does not occur in the same way with *bluetooth* given that, in this case, in order to initiate the download, it is necessary to have prior consent from the device's owner except when the owner has voluntarily modified the configuration of the *bluetooth* service precisely in order to modify the need to require prior consent. This

difference highlights the less invasive nature in privacy terms of *bluetooth* technology.

Continuing with the legal requirements in article 21 of the LSSI-CE, the message sent has necessarily to be identified as advertising and the sender must also be identified. One viable option for complying with this premise could be that both aspects are visibly present in the file name and the sender's details. As an example, the title of the file could be "advert_" followed by the name of the product and/or service that the message aims to promote. In this way, before deciding to receive the message the user would be aware of both, namely the commercial content of the message and who the sender is.

That said, certain problems could arise in the case where, without taking the appropriate precautions, the message that is only apt to be seen by persons over the age of 18, might be sent to the terminal of a minor. Given that, as previously mentioned, the only data that the *bluetooth* access point possesses are the MAC, which is not linked to any type of personal data, or the name given to the device –which, as we have seen, could be the one assigned to it by default by the terminal manufacturer or, a user-modified name-, the advertiser would not normally know the age of the addresses of the message. It is precisely to comply with the current legislation on this matter that there are two possible alternatives that must always be considered complementary, never discriminatory.

We believe that warning must be given that the content sent is not appropriate for all ages but only for those over a certain age. This could be made clear in the name section of the sender of the message, in the title of the communication sent – "advert_over 18s" –, and include a pop-up window whose visualization and recognition of age of majority would be obligatory for the message to be downloaded –as the choice of alternative between age of majority and age of minority.

It must be taken into account that the content of certain messages intended to be sent by *bluetooth* have been conceived to go beyond visibility and reading by the potential user since, in some cases, it will be able to make modifications to the diary and/or contacts of the mobile terminal. In the diary or calendar, it will automatically be able to create an entry in the terminal that announces the opening and closing times and trading days of the establishment from which the message comes. In any case, the other content most likely to be sent out are text, images, videos, discount coupons, games, Java apps, maps and *Web* sites.

Monitoring behaviour in the current technological age: the temporary infringement of privacy in mobile devices with *bluetooth* technology

Currently, we move from one place to another –accompanied by our mobile devices- or using the network of networks, accessing different *Web* sites, or in colloquial terms, trailing our "electronic fingerprints" which, to a certain

extent, assumes knowledge – unknown and in many cases unconsented – of numerous personal data that belong to the user. These actions undoubtedly compromise the privacy of the device's owner as they enable the user's behaviour to be monitored.

As with Internet, so with mobile devices with *bluetooth* technology, there are actions that have been put into practice – unknown and unconsented – which aim to monitor the behaviour of their users. One of the most important initiatives in this respect is the *Cityware* project in which several universities – the University of Bath (United Kingdom) and the University of San Diego (USA) – and companies – Hewlett-Packard, Nokia and Vodafone – participated.

The project is based on the installation across various cities in the EC – Bath and Berlin – and in non-EC cities – San Diego, Hong Kong, Sydney, Singapore and Toronto –, of *bluetooth* signal scanners. It combines various social network tools, like Facebook, with *bluetooth* tracking devices connected in order to obtain more information on behaviour and human interactions in general (KOSTAKOS; NICOLAI & YONEKI, 2009).

A particular device can be tracked by means of the *bluetooth* signal that the mobile instruments has. Let us not forget that in certain cases the users identify the signal of their devices either by their own name (or with their initials) or by other names that are more or less particular to the owner which, with the service activated and in visible mode, and by means of these practices, enables someone to know a lot of personal data about the user, such as places visited, how often, for how long, on which days, and the supposed nature of the visit (personal or professional). Definitively, a huge amount of personal data can be known which could compromise the privacy of the owners, so in this case, they could be defined as illegal acts.

If the action were to take place in Spain, it would be subject to the LOPD. In effect, considering that the location data always refer to one identified or identifiable natural person –they therefore constitute personal data- they would be subject to the various dispositions on personal data protection contained in the LOPD and to the application of its regulations. As article 6.1 of the LOPD foresees, the treatment of personal data requires the unequivocal consent of the affected party, unless the law decrees otherwise, which, in the case we are examining, does not apply in any case.

In terms of the principles that regulate the treatment of personal data, it should not be forgotten that article 4.1 of the LOPD enshrines the principle of proportionality, thereby establishing that personal data can only be gathered for treatment, and for treatment only, when those data are adequate, pertinent and not excessive in relation to the scope and the specific, explicit and legitimate purposes for which they have been obtained. Applying the assumption that we analyze here, firstly it should have the unequivocal consent of the owner of the data gathered

for the use of the *bluetooth* device and, secondly, in terms of this specific case, it should assess the concurrence or otherwise of the principle previously mentioned.

When faced with this type of acts, and the risks that these acts might entail, as well as representing a constraint on the laws, the most convenient action would be to promote the phenomenon of self-regulation. As we shall now discuss, self-regulation is a complementary aspect of current legal norms.

Self-regulation as an ideal complement of the law

The phenomenon of self-regulation has its origins in society which, far from being dissolved into the State, has demonstrated a particular virtuality that has become dynamic, to a greater extent, thanks to the new communication platforms offered by the emergence of new technologies. In this way, self-discipline can be enacted in almost all facets of company activity.

Etymologically, "self-regulation" alludes to the capacity some subject shows to obey certain rules. Contracts, agreements, statutes and all the other internal regulations governing subjects and organizations are the result of self-regulation.

Self-regulation, as defined in the Dictionary of the Royal Academy of the Spanish Language, is the action and effect of self-regulation, which is the regulation of oneself by oneself. In other words, this option refers to the ordination of a specific area – in our case, electronic commercial communications transmitted by *Bluetooth* – by the agents that interact in this field (CHEVALLIER, 2001).

The formula that regulates the social relations that take place in a specific sector, which is self-discipline, has always existed, since any organization self-regulates in one form or another. The phenomenon of self-regulation assumes the observance of certain rules of conduct – principles and ethical norms – compliance with which has been established as an objective. Simultaneously, it also constitutes the expression of the commitment to social responsibility in a specific sector of industry.

For the codes of conduct to be worth the paper they are written on, it is fundamental that verification of compliance be placed in the hands of an authority that guarantees their observance by imposing sanctions when infringements take place (PIPAÓN, 2010). If this were not the case, we would simply be left with expressions of good intentions or instruments of propaganda that would serve no purpose.

Although the terms "self-regulation" – related by and large to private voluntary action and autonomy – and "sanction" – associated *a priori* to a public act for its coercive intent – would seem to be hard to reconcile, in fact they are not. In effect, it must come down to disciplinary penalties that are private in origin

– in our case in the business setting – traditionally defined as a natural complement of the capacity for legal self-regulation that each organization displays.

This is a modality of self-regulation that is entirely voluntary, and which does not have repercussions beyond the legal scope of its participants, whose rules have been negotiated and agree on consensually. In addition, it must be noted that its development will in no way be subject to the demands that public Law applies to the action of the State, rather it will be directed by private autonomy. This appreciation should not be invalidated by the fact that public law considers that the promotion of this phenomenon is positive and necessary in certain scenarios and, consequently, that the law incorporates measures aimed at encouraging self-regulation.

In any case, self-regulation has ceased to be a strictly private phenomenon – and hence remote from public Law – and has become a reality with considerable influence on the actions of public authorities. As a result, private self-regulation and public regulation are now no longer two radically opposed realities but rather two circles whose points of contact are more numerous and clear to see.

In the following section, we discuss the need to encourage the phenomenon of self-regulation in the setting of electronic commercial communications in general sent out by electronic mail, SMS/MMS and instant messaging, among other media and, in particular, those transmitted by *bluetooth* technology. We will emphasise the convenience of self-imposed standards of conduct that have been agree on by all the agents concerned (individuals, public and private business organizations) that interact on this stage.

The question we examine here is of great importance in practice. In fact, violations that occur in this space that we analyze are liable to affect a fundamental right of protection of one's personal data. Therefore, given its relevance, for the document that articulates self-regulation (such as a code of conduct) in the area of commercial communications sent via *bluetooth* to be widely known and complied with, it is advisable to get all the agents who could potentially be affected genuinely involved in the process. In effect, it is vital to get the prior agreement of all the agents who could be affected by the self-regulation document – associations representing consumers and/or users, advertisers, agencies and media, manufacturers of devices with *bluetooth* technology and the public authorities. By doing this, the code of conduct will be endowed with greater efficacy given that it will have been agreed on by all parties. In other words, there will be a greater willingness to ensure its full compliance since it constitutes a document that is self-imposed, and which has been drawn up by all the agents that interact within this sector.

For the code of conduct to be applied as broadly as possible in practice requires a high number of entities that operate in the sector to sign up to it. And

when one of its rules is infringed, the controlling body must impose the corresponding penalty, thus re-establishing the balance within the self-regulatory system.

The range of sanctions that the service provider could face would be broad. For example, the offender could be worthy of no more than a simple warning, a fine, temporary suspension of rights or even, in more serious cases, expulsion from the self-regulatory system. The exact amount of the fine imposed would depend on the seriousness of the infraction committed by the service provider. This assumes that a set of criteria is established to set the amount of the fine to be imposed in accordance with the nature of the infraction.

We understand that the penalties imposed on the service providers for having failed to comply with the code of conduct to which they adhere should be made public. In this sense, it is important not to make inopportune assessments that could damage the good name of the self-regulatory system, since the factor that most ennobles the system is making public all the significant actions that involve the members, both those which potentially benefit the system and those that do not.

The actual content of the code of conduct, as relates to the commercial communications transmitted by *bluetooth*, can be as broad and deep as the interested parties require. The document would be drafted in accordance with the principle of free will which, naturally, needs to respect the current legislation, both obligatory and semi-obligatory, which applies to the private individual. With this in mind, we consider that the code of conduct must include the best practices that the industry and the recipients of commercial communications need. This requires attending to privacy and security, two closely related concepts in the field that we analyze here.

In terms of personal data protection, the code of conduct should provide guideless to safeguard users' private information. As such, we understand that advertisers must request the user's consent before sending out their commercial messages and initiating the message download. Furthermore, in order that the mere request for consent is not seen as a nuisance, various technical formulas could be used by which the advertiser would have effective knowledge that the user wishes to receive specific commercial communications. In this sense, there are two complementary measures that can be taken which maintain a high level of respect for privacy.

One could be that in order for the sender to be able to seek the consent of the user, the user needs to assign a name to his/her device beforehand. In this way, two assumptions would be established at source for the reception of the message. The first, which is essential for the simple request for consent to be transmitted, is that the user has executed – according to the advertiser's indications – a name

change on his/her device – if this were not the case, the advertiser would not refer to the device – and second, that it is essential in order for the downloading of the message to begin, and for which authorization was originally sought.

The other measure relates to the manufacturers of mobile devices with *bluetooth* technology, who should by default configure their devices with a higher level of user protection. In other words, these devices should not be configured in series with a reduced level of protection for user privacy that leaves them exposed, wholly or partially, to the reception of messages sent by a wireless network. This happens when the device configuration enables files to be received without the sender needing to request prior consent from the user. This measure would help guarantee the highest level of protection of privacy both for seniors and minors. For the latter group, measures for the identification of mobile devices belonging to minors could also be demanded of manufacturers in order to guarantee the protection of young people's privacy. For example, manufacturers could fit all terminals with an option in the configuration of the device that allows advertisers to know when they are dealing with a device owned by a minor. The meaning of these indications should enable advertisers to interpret who is the owner of the device they wish to send messages to. Naturally, there are differences worldwide regarding the age at which minors become adults, which needs to be evaluated – in the European Union, it is 18. Until such techniques are put into practice, advertisers could attach a warning that the content of a message is not appropriate for all ages and is only meant for those over a certain age. This warning could be indicated in the name section of the sender of the message, in the title of the communication that is sent – "advert_over 18s" –, or via a pop-up message indicating that acknowledgement of age of majority would be obligatory in order to download and view the message, as the choice of the alternative between age majority of age minority.

Likewise, companies that operate in proximity mobile marketing must implement reasonable technical, administrative and physical procedures precisely to protect the personal data gathered from users, as opposed to the non-authorized use, alteration, disclosure, distribution or inappropriate access.

When dealing with technology based on transmission via radiofrequency, one of the main concerns is security since, *a priori*, it is easier to capture transmitted information this way than by cable technology. This makes it necessary to develop sophisticated security systems that guarantee the privacy of communications and which should be put into practice by advertisers. *Bluetooth* defines various modes of security in the access profile. In this way, unsecured transmission can be achieved with security at service level, or at link level (which would be stronger). On the other hand, as we analyze, there are two types of devices, defined as reliable and non-reliable, and in this way access to the devices

that are not reliable can be restricted. These premises will have to be taken into account by the entities which carry out activities that can be conceptualized as proximity mobile marketing, and on two levels: on the one hand, in order to guarantee at all times the implementation of the highest levels of security in line with the current state of technology, and on the other, with total respect for the security measures installed, either by the user or, in series, by the manufacturer, on the terminal. This assumes ethically unsound or illegal actions meant to ensure the transmission of commercial messages will not be carried out. These might include cases in which *bluetooth* devices are identifiable by the name assigned to them at origin – generally relating to the model type – and in which the database used by *bluetooth* to send commercial messages contains the passwords assigned in series, in which case they could damage the security mechanisms set up by the device's owner.

Although implementation and observance of some of the measures, such as the ones described here, seems plausible and necessary, it must go hand-in-hand with the development of policies to educate the potential user, both adult and minor. To that effect, it is advisable for all users to understand the risks to their privacy that certain actions in the area we describe can pose. So, it would be appropriate to inform users about activating preventive security measures, and opportune to recommend they periodically change the name on their device – preferably without including personal data (full name, phone number, email address) – as well as in the case of the passwords required to receive files.

In this way, for example, monitoring of behaviour during prolonged periods of time could be avoided.

Bearing in mind the risks that it might sometimes pose, it would also be convenient to urge the user to only activate *bluetooth* when absolutely necessary – so, in all other cases, it should best remain deactivated –, as well as pointing out the advantages of setting up security measures for the reception of files, such as when the sender must enter an access code in order to connect with a specific device. In line with the evaluations formulated, it is important to state that the problem with *bluetooth* is that the law only contemplates security at the level of the link, not for applications, in other words, there exists no mechanism that can prevent attacks as a result users' misuse or incorrect use of an app. If the user, consciously or unconsciously, leaves *bluetooth* activated and detectable, there are tools that can be illegally applied to access all the information on the device. This is not due to an error in the *bluetooth* specification but to the user's misuse of the equipment. This makes it clear that user educational policies are just as necessary as codes of conduct.

Conclusion

This article has analyzed the subject of electronic messages sent to mobile devices for commercial purposes. In particular, it has focused on those messages sent via radiofrequency on one of the wireless networks most widely used today for this end (*bluetooth*). We have analyzed novel questions related directly or indirectly to the privacy of the addressee who is the target of this type of communications.

When electronic commercial communications are sent out without the consent of the recipient, they are classified as unsolicited, in other words, *spam.* There are numerous actions in this area that can impact negatively on the privacy of the owners of these devices.

To mitigate as far as possible the pernicious effects of certain commercial practices that use radiofrequency, it is advisable that the industry adopts self-regulation in order to complement Spanish and European Community law on the subject.

References

APARICIO VAQUERO, J. P. Régimen jurídico de las comunicaciones comerciales realizadas a través del correo electrónico. **La Ley**, n. 4, p. 1476-1489, 2005.

BERCOVITZ RODRÍGUEZ-CANO, A. ***Apuntes de Derecho Mercantil***. 8ª ed., Navarra: Thomson Aranzadi, 2007.

BERNARD MONFERRER, M. E. La evolución de la figura de la publicidad denigratoria según la doctrina emanada de las resoluciones del Jurado de la Publicidad. **Revista Autocontrol de la Publicidad**, n. 68, p. 1-19, 2002.

BRONDMO, H. P. ***Las reglas del marketing directo en Internet. Cómo usar el e-mail para interesar y dialogar con el cliente***. Bilbao: Deusto D.L., 2001.

CHEVALLIER, J. La régulation juridique en question. **Droit et société**, n. 49, p. 834-835, 2001.

ESTRELLA RAMÓN, M.A. **Comunicación integrada de marketing**. Madrid: Esic, 2016.

GADZHEVA, M. Legal Issues in Wireless Building Automation: An EU perspective. **International Journal of Law and Information Technology**, n. 16, p. 159-170, 2008.

GARRIGA DOMÍNGUEZ, A. **Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua**. Madrid: Dykinson, 2016.

GUILLÉN CATALÁN, R. ***Spam y comunicaciones comerciales no solicitadas***. Navarra: Thomson Aranzadi, 2005.

JAUME BENNASAR, A. *La validez del documento electrónico y su eficacia en sede procesal*. Valladolid: Lex Nova, 2010.

JAY, R. ***Data Protection – Law and Practice***. 2ª ed., Londres: Sweet & Maxwell, 2003.

KOSTA, E.; VALCKE, P.; STEVENS, D. Spam, spam, spam, spam . . . Lovely spam!' Why is Bluespam different?. **International Review of Law, Computers & Technology**, v. 23, n. 1, p. 89-97, 2009.

KOSTAKOS, V.; NICOLAI, T.; YONEKI, E. Understanding and measuring the urban pervasive infrastructure. **Personal and Ubiquitous Computing**, v. 13, n. 5, p. 355-364, 2009.

LARA GONZÁLEZ, R. ***La denigración en el derecho de la competencia desleal***. Navarra: Thomson Civitas, 2007.

LESMES SERRANO, C. ***La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia***. Valencia: Tirant lo Blanch, 2008.

LÓPEZ JIMÉNEZ, D. Privacidad y seguridad en el comercio electrónico: nuevos retos y desafíos. **Cuadernos de Derecho y Comercio**, n. 52, p. 139-197, 2009.

MASSAGUER FUENTES, J. La publicidad comparativa. **Revista Autocontrol de la Publicidad**, n. 110, p. 1-16, 2006.

MESSÍA DE LA CERDA BALLESTEROS, J. A. ***La protección de datos de carácter personal en las telecomunicaciones***. Madrid: Dykinson, 2004.

PÉREZ BES, F. **La publicidad comportamental online.** Barcelona: UOC, 2012.

PÉREZ DE LA CRUZ BLANCO, A. ***Derecho de la Propiedad Industrial, Intelectual y de la Competencia***. Madrid-Barcelona: Marcial Pons, 2008.

PIPAÓN PULIDO, J.G. ***Derechos de los consumidores y usuarios***. Valladolid: Lex Nova, 2010.

RIVERA CAMINO, J. **Conducta del consumidor**. Madrid: Esic, 2013.

SÁNCHEZ DEL CASTILLO, V. ***La publicidad en Internet. Régimen Jurídico de las comunicaciones electrónicas***. Madrid: La Ley, 2007.

SCHRYEN, G. Anti-spam legislation: An analysis of laws and their effectiveness. **Information & Communications Technology Law**, v. 16, n. 1, p. 17-32, 2007.

STAZI, A. ***La pubblicità commerciale on line***. Milán: Giuffrè, 2004.

VAN DER HOF, S.; CUIJPERS, C.; VAN EECHOUD, M.; GIJRATH, S. SCHELLEKENS, M.; DE VRIES, M. ***Openbaarheid in het internettijdperk***. La Haya: Sdu Uitgevers, 2006.

VEGA VEGA, J. A. ***Contratos Electrónicos y Protección de los Consumidores***. Madrid: Reus, 2005.

JIMÉNEZ, D. L.; DITTMAR, E. C. *Consumer protection from abuses in commercial communications sent via radiofrequency*. **The Law, State and Telecommunications Review**, Brasilia, v. 10, n. 1, p. 37-60, May 2018. [DOI: https://doi.org/10.26512/lstr.v10i1.21499]