The Criminal Prosecution of Market Abuse: More Efficiency and Fewer Rights

Yolanda Doig Díaz
Castilla-Lamancha University

After Directive 2014/65/EU and Regulation (EU) No. 596/2014 of the European Parliament and of the Council of April 16 came into force, access to telephone records, data traffic, recordings of telephone conversations and electronic communications registered and stored by investment entities constitute measures aimed at guaranteeing market integrity, as repeatedly stated by European regulations and the Spanish transposition regulation. The truth, however, is that they have a more specific objective, which is to facilitate the prosecution and punishment of market abuse infringements. As will be shown in this paper, such recordings have a direct impact on the fundamental rights of the entities' employees, such as the personal and family privacy laid down in art. 18.1 SC, data protection 18.4 SC or the secrecy of communications art. 18.2, and therefore, the limitations imposed require compliance with certain assumptions.

Keywords: communication recording, email, monitoring, financial system, investment services entities, market abuse

PRESENTATION

In December 2014, Professors JOHN VERVAELE and MICHIEL LUCHTMAN described the problems faced by the competent authorities of European Union countries in prosecuting insider trading and market manipulation: first, the absence of infringing behavior and, therefore, of the corresponding sanctioning power; second, meager financial penalties and, third, limited authority to effectively enforce market abuse regulations, since they lacked the power to arrange for access to premises, to telecommunications data or to seize such data. Such a situation gave rise -in their view- to a questionable margin of regulatory discretion and weakened cross-border cooperation of law enforcement authorities.

With this diagnosis, the aforementioned authors considered as positive the legislative initiatives proposed by the European Commission in the field of market abuse, which introduced the obligation of Member States to establish criminal sanctions for serious violations of market abuse regulations and endorsed the decision to give national authorities the power to access documents and other data, to demand information from persons, carry out on-site inspections, enter the premises of natural and legal persons, require telephone recordings, electronic communications and registers of data traffic held by investment firms[1].

On these proposals, the authors warned that the powers assumed by the authorities could involve serious interference with the right to privacy and property and recommended that they be exercised in cooperation with the relevant judicial authority, because of their intrusive nature. They also criticized the

fact that the European legislator focuses on the application of rules of this nature in the national context without ensuring the existence of adequate guarantees and their correspondence with the requirements of jurisdiction or proportionality[2].

Despite this expectation, the Directives went through the legislative process and were adopted for one essential purpose: to correct the existing supervisory and control models for investment firms, which proved to be incapable of preventing and managing the 2008 crisis[3].

And in the need to strengthen surveillance, they structured an ambit of control over the employees of the entities that provide investment services to prevent and, where appropriate, effectively punish the commission of conduct related to market abuse, and for the first time made it mandatory -since until then it was a state-level and optional decision[4]- for investment entities to record the communications they have with clients regarding purchase orders.

The interest aroused for this work by the system implemented in the financial field to ensure compliance with the directive known as MIFID II, focuses on the essential, on making clear how those warnings of VERVAELE~~A~~ and LUCHTMAN have materialized in a new scenario in which financial institutions and their own internal surveillance systems are capable of preconstituting evidence for a future administrative or criminal process. The European regulatory framework, its transposition in Spain and only one of the many areas in which this reform generates some concern will be presented, such as the expectation of privacy of investment firm employees and the possibility that, such evidence, might be questioned in the eventual process for violation of fundamental rights.

THE REFORM OF THE FINANCIAL INSTRUMENTS MARKET

On May 15, 2015, the European Parliament and the Council of the European Union approved Directive 2014/65/EU on financial instruments markets, amending Directive 2002/92/EC and Directive 2011/61/EU. The coverage of regulation is very broad, since it encompasses investment services firms, market governing bodies, data supply service providers and non-EU firms. It outlines its regulatory framework by defining the conditions and requirements for operation, enshrining the operational conditions under which investment services firms must ensure investor protection, the powers of Member States' supervisory authorities, their framework for action and the system of sanctions. However, for the purposes of this paper, we are particularly interested in the imposition of a new constraint on the organization of investment firms, namely that they must record telephone conversations or electronic communications of all transactions carried out on their own and on clients' behalf (art. 16) and, as a corollary to this constraint, the authorities of each State will have supervisory powers, including the power to require recordings of such conversations and records of data traffic (art. 69)[5].

The new legal framework of the Union, as far as investment service companies are concerned, is accompanied by Regulation (EU) No. 596/2014 of the European Parliament and of the Council of 16 April, which sets out the regulatory framework in the field of insider trading, illegal disclosure of inside information and market manipulation, as well as measures to prevent market abuse. All the descriptive effort that this Regulation displays, and which should become part of the national law of the EU States, will not be sufficient, as stated in the Directive and the Regulation, if the authorities are not provided with effective powers, instruments and resources to detect and verify the infringement so that it can be punished. To this end, both documents stress the powers to be exercised by the authorities of each State, and the need to have a minimum set of duties in the area of supervision and investigation which, in certain cases, will involve the use of powers which, as stated in art. 23.2 of Regulation 596/2014, will be exercised "in accordance with national law" and, where necessary, after they have been reviewed by the competent judicial authority[6].

In its art. 69, Directive 2014/65/EU details the functions and faculties to be exercised by supervisory authorities, with authority you investigate and correct, which must at least consist of: a) having access to any document and data regardless of format; b) requiring recordings of telephone conversations or electronic communications or records of data traffic maintained by investment firms, credit institutions or financial institutions; c) demanding, where permitted by national law, existing records of data traffic

maintained by telecommunications firms[7]. Regulation 596/2014 adds to these powers that of access to the premises of natural and legal persons for the purpose of seizing documents and data in any form where there is reasonable suspicion of the existence of documents or data relating to the matter (art. 23.2.e).

As a correlate of the control that the authority can exercise over entities providing investment services, Directive 2014/65/EU requires them to implement a record of all services, activities or transactions they perform, including recordings of telephone conversations or electronic communications relating to transactions on their own and customers' behalf. According to the Directive, the firm's clients, both new and old, will be notified about the recording of telephone communications or conversations and if no such notification has been previously made, the investment firm (art.16) will not provide services or carry out investment activities with that client by telephone.

Such entities will be bound to take measures to record telephone conversations and electronic communications made, either sent or received via the communication device provided by the firm to the employee, unless the use of another means of communication has been accepted or authorized by the firm. The records shall be available to customers and kept for a period of five years, except when the competent authority requests that they be kept for a period of up to seven years, and the persons concerned shall have the right to request a copy of the recording[8].

This register of electronic communications and traffic data, which is required to be implemented by entities providing investment services in 2014, is further outlined in the Delegated Regulation (EU) 2017/565 of the Commission of 25 April, which complements Directive 2014/65/EU with regard to the organizational requirements and operating conditions of such companies.

This Delegated Regulation establishes the requirements that investment services firms must comply with when implementing and maintaining the system for recording conversations and electronic communications. As explained in art. 76.1, this system must respond to an effective recording policy established in writing and appropriate to the size of the organization, nature, magnitude and complexity of its activity. Such efficiency implies the need of a system that allows them to identify telephone conversations and electronic communications, including internal electronic conversations and communications, on the one hand, and their content, on the other hand, provided that they are transactions carried out when trading on own account and providing services related to the reception, transmission and execution of client orders, even if those conversations or communications are unfruitful (art. 76.1.a). Said policy must specify the procedures and measures that guarantee that the firm has a system in place when, due to exceptional circumstances, the conversation or communication cannot be recorded on the devices created that are accepted or permitted by the firm (art. 76.1.b).

As for the system implemented by each entity, the Delegated Regulation (EU) 2017/565 requires that the recordings be kept in a durable medium that allows their reproduction or copying and that they be kept in a format that prevents the modification or deletion of the original recording, they are to be stored in a medium that allows them to be accessible and available to clients who request them (art. 76.10). Employees of investment firms will be trained in the procedures in place at their entity, in order to comply with the requirements of the recording system.

Depending on the recording and storage system that the Directives require of firms, and which has been outlined, all conversations and all electronic correspondence between the client and the firm, aimed at closing a transaction or service, must be stored in such a way that it can be reconstructed from its beginning to its conclusion in a short period of time.

The magnitude of the information that each bank has available and that will be at the disposal of the administrative authority or the judicial authority, does not only derive from the recording of telephone conversations, but it will be obtained from very different sources, such as videoconference, fax, email, mail, SMS, Bloomberg or Reuters chat, instant messaging and mobile applications[9].

To the variety of sources, the content of the information is added, which can be of a very different nature, since it will involve recording, registering and storing all communication related to purchase and sale orders of any financial product, such as swaps, bonds, derivatives or shares, among all those persons who in one way or another have contributed to the closing of that operation. This entails recording not only communications between the client and the employee responsible for marketing the product, but also

the entire chain of employees involved in a transaction, from the first call or email -even if it is unsuccessful- until the transaction is closed[10]. Thus, it will begin when the client contacts the bank's agent, then the agent will go to the treasury sales desk, and explain the requested operation, specifying conditions such as expiration, reference interest rate, frequency of payments, strike level if it is an option, and after that, it will be the sales desk that will ask for a solid quote from the trading desk. All communications aimed at closing a transaction and all its content are recorded, but the system does not discriminate, so that it may happen that a recorded conversation includes not only financial matters but also personal or family matters of the customer or the firm's employees. Moreover, the recording system cannot a priori identify the conversation that will revolve around a transaction of which it does not, by default, record all communication between the customer and the areas of the bank involved in the purchase orders.

However, the recording of transactions and orders, including telephone and electronic communications, will not only serve to identify the transaction and those who intervened in the event that a violation of the market abuse rules is detected, but will also be subject to checks by the investment service firm to ensure that recording requirements and other regulatory obligations under Directive 2014/65/EU[11] are met. Such monitoring involves regular inspection of transaction and order records, including discussions, and, insofar as it involves follow-up, must be proportionate and risk-based (art. 76.6). In the absence of criteria specifying the proportionality referred to in the Regulation, the European Security and Market Authority has determined certain parameters, namely that the frequency and purpose of such monitoring may be linked to the volume and frequency of own-account transactions; to the volume, frequency and characteristics of client orders; to the characteristics of the clients; to the financial instruments and services offered and to the conditions of the market accounts.

This monitoring means that all conversations recorded one day will be the object of surveillance from the following day, according to the alert policy that each entity designs, which consists of outlining and specifying those behaviors that could constitute an infraction and which will have to serve to monitor the conversations. For instance, such conduct may consist of acts of pressure on clients, exaggeration of profits, risks or volumes traded, requests to increase or decrease an index, disclosure of the volume of orders or the position of other parties. According to this configuration, communications will be catalogued according to their content and alerts will be triggered when, for example, communication does not follow normal behavior by using words in unusual contexts, infrequent patterns related to the number of transactions in specific time frames, disorderly trading or unusual language.

Directive 2014/65 considered recordings to be an effective tool for detecting market abuse offences, a crucial and, in some cases, the only evidence of insider trading and market manipulation. However, it is not the only instrument used to prosecute such crimes, as it includes two other means of investigation: access to the premises of natural and legal persons, and logs of data traffic maintained by a telecommunications company.

The objective of this system is none other than to detect with rapidity the operations that involve market abuse, to initiate the pertinent investigation and to obtain evidence that allows the sanctioning of the employee, the client or the corresponding entity. The transposition to Spain, as will be noted, does not provide further elements of judgment on the value that such recording may acquire in a criminal or administrative sanctioning process.

TRANSPOSITION IN SPAIN

Royal Decree 1464/2018 of December 21, published in the Official Gazette on December 28, 2018, aims to finalize the regulatory development of the legal regime of Royal Decree 21/2017 and the revised text of the Securities Market Law, approved by Royal Decree 4/2015, as amended by Royal Decree 14/2018. The fourth final provision incorporates the amendments to Royal Decree 217/2008 on the legal regime for investment services companies and other entities providing such services. Among the precepts modified, art. 32 is reformed, which under the label "Registers" develops art. 194 of the revised text of the Securities Market Law which, until 2018, required entities to keep a register of services, activities and

operations. The new provision, in addition to enabling the Spanish National Securities Market Commission (Comisión Nacional del Mercado de Valores or CNMV) to perform its supervisory functions and implement the executive measures provided for in Regulation (EU) No. 600/2014 of May 15, Directive 2014/57/EU and Regulation (EU) No. 596/2014, will be able to determine whether the investment services firm has fulfilled all its obligations, including those relating to its clients or potential clients and to market integrity.

This new art. 32 is a transcription of art. 16.7, Directive 2014/65/EU, which does not add or specify anything about important issues such as the need to ask for the client's consent, since art. 32.5 only refers to the notification of the recording; neither is the purpose of the recording clearly defined, since although it is part of a Directive aimed at combating market abuse practices and verifying whether they comply with the requirements aimed at protecting investors, it is not specified whether such recordings may be used to measure effectiveness at work, absences from work or conversations with colleagues.

Fortunately, art. 32 does not -and could not- give the CNMV the power to request existing registers on data traffic from telecommunications operators[12], as long as there is a reasonable suspicion of an infringement and the investigation is related to the violation of Directive 2014/65/EU or Regulation 600/2014. As is known, data traffic will be facilitated by the operators or providers of communication services as long as it corresponds to the investigation of a crime, there is sufficient evidence, and there is an enabling judicial decision[13], as provided for in art. 588 (j) LECrim.

Another investigative measure that has not been transposed in the terms of European legislation is provided for in Regulation (EU) No. 596/2014 of the European Parliament and of the Council of April 16, 2014 on market abuse, which establishes access to the premises of natural and legal persons for the purpose of seizing documents and other data relating to the subject matter of an investigation that may be relevant to prove a case of insider trading or market manipulation. It happens that a financial institution is the holder of the right to inviolability of the domicile, it is true that it is not in the same intensity as a natural person, but the necessary and indispensable physical space for the development of the activities of the entity is protected, so that, only a Judge may provide access to the facilities of the investment services firm to seize documents[14].

In conclusion, it can be seen that the Explanatory Memorandum to Royal Decree 1464/2018 of December 21 refers to recordings as a measure to protect investors and enhance the supervision of the CNMV. And a generic reference to the principle of legal certainty is included, which is reinforced, according to this Royal Decree, due to the regulatory development of those issues that due to their level of detail or technical character must be regulated in rules of legislative rank, including the secrecy of telephone and electronic communications to which the CNMV can have access without the need to request judicial authorization. And although the Royal Decree makes no reference to its use as evidence in administrative sanctioning proceedings, in criminal proceedings or in labor proceedings, there is concern about the degree of effect it may have on the employee's expectation of privacy and its consideration as a legitimate action, as an assumption of validity before the courts to defend the employer's power of direction, as will be discussed in the following section.

THE LOW EXPECTATION OF WORKER PRIVACY

According to the European regulatory framework explained above, the recordings are presented as a kind of pre-constituted evidence, by virtue of which, an action carried out in the business sphere, without judicial intervention and with an impact on the fundamental rights of clients and workers, acquires evidential value. This paper will not address the discussion of the alleged nature of pre-constituted evidence or the interference in fundamental rights that it entails. On this occasion, the aim is to analyze its evidential value under the control exercised by the employer.

It should be recalled that recordings in the field of investment services firms are a necessary tool for monitoring the market, increasing security in negotiations and managing it effectively[15], and they modulate rights such as secrecy of communications, data or privacy. It is well known that these rights are not absolute[16], and it must therefore be assumed that the parties concerned, clients and employees, tolerate

this scope for interference. This requires that in both collectives there is full knowledge of the recording of their telephone conversations, their registration, storage and monitoring. In the case of clients, knowledge would not be sufficient, but consent would have to operate, and in the case of investment firms' employees, the scope of control exercised by the employer and its purpose would have to be communicated to them.

As an argument to defend the legitimacy of the measure under study, it could be argued that both clients and employees are aware of this measure and have renounced the secrecy of their communications (art. 18.3 Spanish Constitution (SC)), privacy (art. 18.1 SC) and informational self-determination (art. 18.5 SC).

In the case of the entity's worker, one could defend that, in order to avoid any infringement f his rights, the recordings of his communications are not made in a domestic or private environment and that, therefore, one cannot speak of an affectation to privacy. However, the ECHR has considered it excessively restrictive to limit the notion of private life protected by art. 8.1 ECHR to an «intimate circle» in which the individual can conduct his personal life in his own way and fully exclude the outside world not included in this circle. The Court understands that in other areas, and in particular in relation to work or profession, interpersonal relationships, links or actions are developed which may constitute manifestations of private life[17] and communications from the workplace, as well as those from the home, may be included in the notions of private life. The Constitutional Court (CC) has also ruled on the right to privacy in the area of labor relations in a number of judgments[18].

It is thus clear that employees of investment services institutions, and in particular those involved in client orders, will see their reasonable expectations of privacy diminished significantly, since their telephone communications, those made through messaging management programs and those maintained through emails will be recorded.

From the company's perspective, these recordings may form part of the business right of vigilance and control to verify compliance by the worker of his employment rights and duties, as provided for in art. 38 SC and art. 20.3 Workers' Statute (WS), but with an important projection, since in this case it is not only a matter of access to the computer and technological means of the workers, whose information will be registered, stored and monitored periodically, but such examination will also be made of the content of their telephone conversations.

With regard to the monitoring of email, it should be remembered that this control has been endorsed by rulings of the Social Chamber of the Supreme Court which consider that the use of the company's computers, including the personal computer assigned to each worker, is within the scope of the employer's power of supervision and is covered by art. 20 of the Workers' Statute[19]. The employer's power of direction is essential for the proper functioning of the productive organization -a reflection of the rights proclaimed in arts. 33 and 38 SC- and empowers the employer to adopt the measures he deems most appropriate to verify compliance with labor obligations and duties, always from the standpoint of dignity[20]. It is distinguished from the surveillance provided for in art. 18 of the Statute, which corresponds to the function of "private police", an exceptional regime referring to the worker's private sphere, such as the locker or personal effects[21]

Within this framework, in the case of monitoring of emails, the courts have emphasized the need for a clear and express prohibition of the use of computers for personal purposes, so that, once such a warning has been given, monitoring does not impose concern for privacy or the secrecy of communications, since, in the absence of a situation of tolerance of personal use, there is no longer any reasonable expectation of privacy either[22].

It should be remembered that, in the case of emails, control is exercised over a closed communication process, as distinguished by the Supreme Court[23], where the rights that may be affected are intimacy, privacy or, as the case may be, informational self-determination and, as the Court has repeated, not every measure that affects the right to privacy always requires judicial authorization as a precondition[24].

Access to emails must therefore comply with the principle of proportionality in order to verify whether the measure adopted achieves the proposed objective, whether it is necessary and whether there is no other more moderate measure for achieving the purpose with equal effectiveness and, finally,

whether it is adequately weighted, since it derives more benefits or advantages for the general interest than harm to other goods, values or conflicts[25].

On this basis, it is understood that the daily monitoring of the emails of the employees of investment services firms that are directly involved in own account or client transactions, means that the employee is warned, knows and understands that his or her business-owned email account is intended for professional use and will be subject to continuous checks to rule out market abuse operations. Briefly, from that employee's perspective, the control system must consist of a known[26] and contractually assumed[27] limitation. It is true that this checking of electronic mail is not carried out in a generic and indiscriminate way, but it is carried out on mail relating to specific commercial operations and is carried out on the server housed in the premises of the financial entity and with computer search parameters designed to limit the invasion of privacy, but the plaintiff's particular device or apparatus is not accessed[28].

Yet when it is not a question of access to email, but of telephone communications within a company, in this case an investment entity, it is worth asking whether greater caution is required since the right concerned is "ongoing communication", as the SC distinguishes, and in that case, the secrecy of communications. And on this point, case law has maintained certain fluctuations[29] that respond to the necessary weighting of the specific case. In the CC ruling (STC) 98/2000 of April 10, the evidential value of the recordings of the conversations of workers in a casino is questioned. In order to assess the appeal, the Court analyzed whether the installation of microphones to record the conversations of workers and customers in certain areas of the casino meets the essential requirements of respect for the right to privacy. And while it considered that such a measure could be useful or convenient, it verified the existence of other less intrusive mechanisms and the absence of failures in the previously established security and control systems that would justify the measure, so that, since it is not an indispensable system, the continuous and indiscriminate listening to all types of conversations, both of the casino's employees and customers, was considered an action that goes far beyond the powers granted to the employer by art. 20.3 of the WS and, ultimately, constitutes an unlawful interference with the right to privacy enshrined in art. 18.1 SC. Following this line of jurisprudence, the CC, in its ruling 29/2013, upholds the protection of the worker who has been sanctioned with disciplinary measures and in whose procedure the recordings have been used to detect breaches of working hours. In this case, the right invoked was that of data protection under art. 18.4 SC, since the images recorded on a physical medium allow the person to be identified and can be used to draw up his or her profile. Also in said ruling, reproducing the sentence of the plenary session 292/2000, the CC recalls that the fundamental right of art. 18.4 SC empowers the subject to know at all times who has the personal data and to what use it is being submitted, so that, as the STC 29/2013 specifies, an element characterizing its essential core is the right to be informed of who has the personal data and for what purpose. This right also operates when there is legal entitlement to collect the data without the need for consent, given that the need for authorization is independent of the duty to inform the holder of the purpose of the handling, in such a way that private interests are prevented from justifying the use of the data against the worker without prior information on the workplace supervision carried out. And in the case of the recordings in the casino, the CC warned that it was not enough that there were signs announcing the installation of cameras and the capture of images, nor that the Spanish Data Protection Agency had been notified of the creation of the file, it was also necessary to provide workers with precise, express, clear and unequivocal information about the purpose of the monitoring of the work activity to which that capture could be directed. Three years after this ruling on the appeal, in STC 39/2016, the CC adjusted its doctrine in a similar case, in which the recording was used to dismiss the applicant for protection by means of an installed camera, of which the workers were not informed due to a suspicion of illegal appropriation. In this case, the CC understood that the duty to inform was fulfilled by the company, since the camera was located in the place where the work was performed, focusing directly on the cash register and in the shop window, the logo of the processing of personal data for surveillance purposes through camera or video camera systems was visible, and in those circumstances, the CC concluded that the worker was aware of the installation of the video surveillance system without having to specify, beyond mere surveillance, the exact purpose assigned to that control.

Following this decision, the ECHR in the López Ribalda and others v. Spain ruling of January 9, 2018, consecrates a different doctrine to the one maintained by the CC and considers, in general, that the fundamental right to private life is affected, in the use of hidden or concealed video surveillance systems aimed at recording the cashiers of a Spanish supermarket without justified suspicion. In this case, the employees were aware of the existence of cameras focusing on the supermarket exit but not of those focusing on the checkouts[30]. However, the Grand Chamber of the ECHR rectifies the doctrine in this case, and in its ruling of October 17, 2019, it concludes that the video surveillance recordings were proportional, in view of the business interest in identifying those responsible for the economic losses detected and the impossibility of communicating this, since it would have compromised the purpose of the video surveillance, and furthermore, the recordings were limited to a space, a group of workers and for a certain period of time.

With this reasoning, the doctrine of the Grand Chamber of the ECHR coincides with the STC 39/2016 and with the legal framework implemented in Spain in 2018, which is the Organic Law 3/2018, of December 5, on the Protection of Personal Data and the guarantee of digital rights that recognizes video and audio surveillance in its art. 89. Concretely, this precept enshrines two situations that NAVARRO NIETO distinguishes, firstly, a video surveillance of labor control, which requires informing workers or their representatives, of the measure beforehand, in an express, clear and concise manner and, secondly, a video surveillance of illegal acts, in which the duty of prior information will be understood to be fulfilled in accordance with art. 22.4 Organic Law on Data Protection (OLDP), that is, with the placement of an informational device in sufficiently visible places identifying the existence of the video surveillance system.

As expressed by this author, this precept seems to take as a reference the doctrine of STC 39/2016, but it goes further, since it admits the recording of sounds in the workplace when the risks to the safety of the installations, goods and persons derived from the activity carried out in the workplace prove to be relevant (art. 89.3 OLDP) and always respecting the principle of proportionality, that of minimum intervention and the guarantees of information.

The legitimacy of corporate monitoring and control, and the limits that the jurisprudence of the CC, the ECHR and the provisions of the OLDP impose on its exercise, in view of the impact on fundamental rights that it entails, make clear the extent of the area affected by the recording of telephone conversations or electronic communications linked to client orders in investment firms. In this scenario, such recording does not respond to a number of findings[31], but rather fulfils a preventive purpose, aimed at stopping infringements from occurring, and raises the standard by not requiring any evidence to justify the measure, as if there were a presumption of the commission of the crime. All of this requires entities to arbitrate systems that respect fundamental rights, aimed at ensuring that professional data or the effects of professional communication of each purchase order are subject to corporate control, but that they do not invade or exceed this specific area.

As this control and surveillance system is set up, it consists of a collection of evidence of conduct involving market abuse, both administrative and criminal offences, but with scope for use in other cases in view of the silence of the regulations on the subject.

Thus, not only must workers be warned of the scope of the recordings, their preventive nature and the possibility that they may constitute evidence, but also of the purpose and use to which the stored conversations will be put.

CONCLUSION

The regime for recording telephone and electronic communications imposed on institutions providing investment services in the European Union, enshrined in Directive 2014/65/EU, Regulation (EU) No. 596/2014, Regulation (EU) 2017/565 and, in Spain, in Royal Decree 1464/2018, has a direct impact on the right to secrecy of communications, privacy and data of customers and employees involved in orders, and responds to the need to strengthen investor protection, enhance market surveillance and increase legal

certainty for the benefit of firms and their customers. This objective, in the estimated balance achieved by the Community legislator, appears to take a predominant place over the rights concerned.

Despite the importance of this objective in its justification, it cannot be explained that the specific regulations governing such measures are not clear nor precise on the nature of the infringements, nor on how to combat the risks of abuse or illegal use of the stored data[32]. Nor does it explain how to avoid situations of arbitrariness in the random control that is carried out, let alone delimit the criteria for the extent of the work of the register or establish safeguards to prevent manipulation[33].

In order to guarantee the expectation of privacy of employees, entities will have to inform them of the following aspects: first, of the entity's policy on recordings of telephone and electronic communications; second, of the extent of such recordings, which affect any telephone communication addressed to the employee or made by the employee operating under orders, since the recording system does not distinguish between contents and records by default; third, that such telephone recordings including those made by email and chat will be monitored periodically; fourth, that such information is only intended to discover conduct that violates the rules against market abuse, and to use it as evidence in an eventual criminal and administrative proceeding, but it does not serve to discover conversations of the employee, nor to verify his dedication or efficiency in the performance of his activity; fifth, such recordings may also not be used by the compliance bodies except when they have initiated investigations for market abuse.

ACKNOWLEDGEMENT

This work was financially supported by the Research Project R+D+I called "Investigation and evidence of money laundering. The 4th Guideline" (Reference DER2016-80685-P).

ENDNOTES

1. LUCHTMAN, M and VERVAELE, J., "Application of the market abuse regime (insider trading and market manipulation): towards an integrative model of criminal and administrative law enforcement in the EU?", Cuadernos de Derecho Penal, ISSN: 2027-1743, July-December 2014, p.27
2. LUCHTMAN, M and VERVAELE, J., "Application of the market abuse regime ...", p.44-45
3. Communication from the Commission, European Financial Supervision, 27 May 2009, Brussels
4. It should be noted that Commission Directive 2006/73/EC of 10 August 2006 implementing Directive 2004/39/EC of the European Parliament and of the Council as regards organizational requirements and operating conditions for investment firms, enshrined in its art. 51 the right of Member States to impose on investment firms the obligation to record telephone or electronic conversations.
5. Art. 69(d) and (r) Directive 2014/65/EU of May 15, 2014
6. Recital 137 Directive 2014/65/EU and Recital 62 Regulation (EU) No 596/2014
7. Art. 69 Directive 2014/65/EU of May 15, 2014
8. Delegated Regulation (EU) 2017/565 of the Commission of April 25, 2016
9. European Securities and Market Authority, Questions and Answers, On MIFID II and MIFIR investor protection and intermediaries' topics, pg. 46. Accessible on https://www.esma.europa.eu/sites/default/files/library/esma35-43-349_mifid_ii_qas_on_investor_protection_topics.pdf (June 19, 2019)
10. European Securities and Market Authority, Questions and Answers, On MIFID II and MIFIR investor protection and intermediaries' topics, pg.43. Accessible on https://www.esma.europa.eu/sites/default/files/library/esma35-43-349_mifid_ii_qas_on_investor_protection_topics.pdf
11. European Securities and Market Authority, Questions and Answers, On MIFID II and MIFIR investor protection and intermediaries' topics, pg.44. Accessible on https://www.esma.europa.eu/sites/default/files/library/esma35-43-349_mifid_ii_qas_on_investor_protection_topics.pdf
12. Recital 144 Directive 2014/65/EU.

13. MARCHENA GOMEZ, M., La Reforma de la Ley de Enjuiciamiento Criminal en 2015, Castillo de Luna Ediciones Jurídicas, Madrid, 2015, p. 288.
14. Judgements 137/1985, 69/1999 and 54/2015 recognize the inviolability of the home for legal persons. Vid RODRÍGUEZ BAHAMONDE, R., "Estatuto jurídico procesal de la persona jurídica como parte pasiva del proceso penal", In Proceso penal y responsabilidad de las personas jurídicas (Pérez-Cruz Martín, A., Dir.), Edit. Aranzadi, 2017, p.115
15. STC 233/2005, of September 26
16. STC 57/1994 and STC 142/1994
17. SECHR 2014, Fernández Martínez v. Spain; 2013 Oleksandr Volkov v. Ukraine; of December 16, 1992, Niemietz v. Germany; May 4, 2000, Rotaru v. Rumania; July 27, 2004, Sidabras y Džiautas v. Lithuania.
18. STC 12/2012, STC 98/2000, STC 186/2000.
19. Sentence of the Supreme Court (SSC) (S 4ª) February 8, 2018
20. STC 98/2000 of April 10, STC 186/2000 of July 10, STC 241/2012 of December 17.
21. SSC (S 4ª) February 8, 2018, SSC September 26, 2007, SSC March 8, 2011
22. SSC (4ª) October 6, 2011
23. SSC (2ª) 528/2014, June 16.
24. SSC (2ª) 777/2013, October 7.
25. SSC (4ª) 119/2018 February 8.
26. The Compliance Officer may be responsible for ensuring that the employees of the entities are aware of this, as reported by SAURA ALBERDI in the case of the liability of legal entities. SAURA ALBERDI, B., "Daño e implementación del plan de prevención de delitos en la empresa", In Proceso Penal y Responsabilidad de las Personas Jurídicas, Thomson Aranzadi, Navarra, 2018, p. 299
27. SSC (2ª) 489/2018, October 23.
28. SSC (4ª) 119/2018, February 8.
29. As stated in the private vote of SSC 239/2014 of April 1, p.13 and in the Pamplona Social Court ruling, February 18, 2019, p.5
30. NAVARRO NIETO, F., "La videovigilancia laboral. Un comentario a la STEDH 17-10-2109. Asunto López Ribalda," In Diario La Ley, No. 9519, November 15, 2019, Wolters Kluwer, p. 4.
31. If they were to do so, they would then have to claim judicial intervention to guarantee the validity of the evidentiary material obtained in the investigation. GÓMEZ COLOMER, I., "Cesión de datos obtenidos a través de sistemas de compliance y procesos penales", In Cesión de datos Personales y Evidencias entre procesos penales y Procedimientos Administrativos Sancionadores Tributarios, (Colomer Hernández Dir.), Thomson Reuters Aranzadi, 2017, p. 378.
32. LUCHTMAN, M and VERVAELE, J., "Application of the market abuse regime (insider trading and market manipulation): towards an integrative model of criminal and administrative law enforcement in the EU?", Cuadernos de Derecho Penal, ISSN: 2027-1743, July-December 2014, p.33
33. RODRÍGUEZ LAINZ, JL, "Sobre la influencia de la jurisprudencia del Tribunal Europeo de Derechos Humanos en la actual regulación legal del llamado "derecho al entorno virtual", In Cesión de datos Personales y Evidencias entre procesos penales y Procedimientos Administrativos Sancionadores Tributarios, (Colomer Hernández Dir.), Thomson Reuters Aranzadi, 2017, p.306.