AMPARO SALOM LUCAS
Senior Judge
University Jaume I, Castellón, Spain
a.salom@poderjudicial.es
ORCID 0000-0002-1849-2643

Communication and Human Rights. The right to secrecy of communications and the judicial ability to investigate and prosecute crime effectively

ABSTRACT

The right to secrecy of communications, enshrined in the Constitutions of European countries and in International Conventions, is subject to multiple analyses by the judges when issuing an order for intercepting telephone communications or personal communications in vehicles, and when assessing the right of arrested people and inmates to communicate with their families and lawyers.

During investigations it is necessary for the judge to do a thorough weighting between the need for the interception of communication, the purpose for it, its suitability to the investigation and the fundamental right of the defendant. The same balance is needed when the judge order the search of information contained in electronic devices and computers.

Through this article we intend to give a general view of the interaction of this right with the judicial investigation and the different problems that may arise. In the same way, an analysis is made of the most recent European jurisprudence on the subject. Furthermore, we make a proposal regarding new mechanisms to extend this investigation measure beyond the borders of each country in the European Union, through the novel instrument of criminal cooperation, the European Investigation Order, which has definitively banished the traditional system of letters rogatory.

KEYWORDS: *secrecy of communication, interception of communication, right to privacy, private life, data, European investigation order.*

Introduction

The fundamental right to secrecy of communications is enshrined in the Spanish legal system in article 18.3 of the Constitution, hereinafter SC[1], Article 7 of the Charter of Fundamental Rights of the European Union, hereinafter CFREU[2], and 8 of the European Convention on Human Rights[3].

This right can be defined as a subjective public right, because it is enforceable before the public authorities. It is an autonomous right that has its own entity, since it is not part of another fundamental right, despite the undoubtable connections with other rights, such as freedom, dignity of the person and free development of one's personality. It is a right of a formal nature, because it protects what is communicated independently of its content and whether it belongs to the personal, intimate or reserved domain. Finally, it is a relative right, as it can be limited by a judicial decision[4], which would allow to invade the secret of communication, in the cases and with the requirements we will see next.

General doctrine

a) Access to the content of communications

In the Spanish legal system any interference of this right which is not provided by law and necessary for the prevention of crime or protection of the rights and freedoms of others[5] is prohibited.

---

[1] Art. 18 SC: *3. The secrecy of communications and, in particular, of postcards, telegraphs and telephones is guaranteed, except for judicial decisions.*

[2] Art. 7 CFREU: *Everyone has the right to respect for their private and family life, their home and their communications.*

[3] Art. 8 Convention: *1. Everyone has the right to respect for their private and family life, their home and their correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

[4] NISTAL BURÓN, JAVIER, 2015. The intervention of the verbal communications of the detainees in police dependencies. Aranzadi Doctrinal Magazine no. 1/2015 part Studies. Editorial Aranzadi SAU.

[5] Art. 8.2 of the European Convention for the Protection of Human Rights and Fundamental Freedoms of November 14, 1950

But this protection does not mean that the right to the inviolability of communications has no limits because otherwise that would mean leaving certain crimes unpunished. Therefore, the Constitution itself sets limits to this fundamental right, and this limit comes with a judicial decision.

Article 588.bis of the Spanish Criminal Procedure Law, hereinafter LECRIM, requires that any interference that affects the right to confidentiality of communications must meet four requirements: the principles of specialty, suitability, exceptionality, and necessity and proportionality.

The specialty principle requires that the specific object of the investigation be known before granting the order. That is, prospective and future investigations are banned, specifically the investigations "*aimed at preventing or discovering crimes or dispelling suspicions without an objective basis",* article 588 bis a.2 LECRIM.

The principle of suitability – art. 588 bis.a.2- requires that this method of investigation be adequate to obtain relevant information to any of the purposes that the legislator describes in the following section (discovery or verification of the fact under investigation, identification of the perpetrators, investigation of their whereabouts or location of the effects of the crime)

The principles of exceptionality and necessity of the measure – art. 588 bis.a.3 – are based on the idea that there is no other measure less restrictive of fundamental rights that gives us access to relevant information to the investigation. That is to say, the investigation would be seriously hampered without it.

As regards the principle of proportionality – art. 588 bis.a.4-, it requires a balance between the interest of the person affected by the measure and the public interest. The judge must make a ponderation attending jointly to the different criteria that are set in the LECRIM, consequently the interception can only be granted when investigating crimes classified as serious offences by the Penal Code and those that are especially serious due to the social significance of the facts, or the rights involved. Not only being investigating a serious offence is enough to comply with the proportionality criterion, as defended, among others, by the Spanish Constitutional Court

Judgment nº 82/2002. It is necessary to assess the seriousness of the crime against the relevance of the result sought by the restriction of the right.

From the point of view of the crime under investigation, art. 588 ter.a allows the interception of telephonic or telematic communications when related to intentional crimes punishable by a penalty with a maximum limit of at least three years of imprisonment, as well as specific categories of crimes: terrorism, organized crime, and crimes committed with computer tools or any other technology of communication.

Spanish Supreme Court has indicated in the recent Judgment 397/2018 of September 11, in relation to the evidence that must concur to issue a measure of interception of the communications:

In order to issue a telephone intervention, it is sufficient for the judicial authority to have evidence of relevant information (interception of the package) when there is no reason to doubt its certainty (a police invention?). It is not necessary to demand documentary accreditation (email) that endorses the veracity of the official manifestation of the police. If it is said that surveillance has been carried out, it is not necessary to prove it with graphic documents; if it is alleged that a person is convicted, it is not necessary for them to present the judgment; if it refers to having a police record, it is not necessary to endorse it with the reports. The explanations of the head of the Task Force of the National Police in the trial on the reality of these communications from Argentina are sufficient to rule out *the bizarre hypothesis that everything was a malicious invention designed with spurious -criminal!- intent to falsely accuse some people or to deceive the judicial authority so that it issued the interception of communications.*

b) Access to communications data

The Organic Law 1/2015 of October 5, amendment of the LECRIM to strenghten the procedural guarantees and the regulation of the technological investigating measures, gave the legal framework for this access in Spanish law. As a consecuence, nowadays there is specific regulation[6] on the

[6] Independent and different from the provisions for interceptions of communications

interception of the data generated by the use of telephone terminals[7], as for example, the association between the number of IMEI[8] of a terminal, and the phone number of the SIM card[9] that is inserted, as well as its owner.

We must not confuse this data with the data related to communications already completed, which must be kept by legal mandate[10] by telecommunications operators in the event that it is useful in the context of a police or judicial investigation. In the same way, we should not confuse them with the conserved data, also of completed communications, which must also be kept by the operators or by third parties, for commercial or other reasons.[11]

The art. 588 ter j.1 of the LECRIM subjects access to traffic data generated by a telephone terminal to the principle of jurisdictional exclusivity. Access to this information is subjected, on the one hand to the necessity test (when knowledge of this information is indispensable for the purposes of the investigation), and secondly to the criterion of proportionality (proportion between the measure of access to the data and the seriousness of the crime investigated, which is equivalent to the offences referred to in article 588 ter.a[12]) The Preamble of the Organic Law 13/2015, of October 5,

---

[7] According to Constitutional Court Decision 123/2000 of May 20, the traffic data generated by telephone terminals is part of the external field of communications, subject, as such, to the same protective discipline of Article 18.3 of the Spanish Constitution, but in the least intensity.

[8] IMEI stands for International Mobile Equipment Identity, and is a unique worldwide identifier that each mobile phone has. Thus, when a device connects to a network it automatically sends this identifier that operates as an "identity card" of the mobile.

[9] SIM stands for *subscriber identity module.* It is detachable card used in mobile phones and other devices that are connected thereto by means of a slot reader.

[10] Law 25/2007 of October 18, on the preservation of data relating to electronic communications and public communications networks, in relation to its First Additional Provision, paragraph 4.

[11] Article 588.ter.j of the Spanish Criminal Procedure Law.

[12] Article 588.ter.a LECRIM refers in turn to article 579.1 of this law. In short, the crimes for which traffic data may be requested are: 1. Intentional crimes punishable by a maximum of at least three years in prison, 2. Organized crime, 3. Terrorism and 4. Crimes committed using computer tools or any other technology of information or communication.

indicated that the transfer of such traffic data, its incorporation into the process "*... is only authorized in the case of the investigation of an offence that, for reasons related to the principle of proportionality, justifies the sacrifice of the inviolability* of communications . «

However, not even belonging to this list of crimes would guarantee the compliance with the proportionality criterion imposed by art. 588 bis.a.4, because we must also pay attention to the relevance of the result we are seeking with the interference in the right to secrecy of communications. Thus there is no possibility of obtaining research data for minor offences, although technological means were employed for its commission.

Finally, we must make a brief reference to the specialty principle, which must also be met to issue the order. This principle requires that the investigation is focused on specific facts rejecting completely the prospective investigations. Article 588.bis.a.5 expressly refers to the principle of proportionality when it states: "*the intensity of existing evidence*".

c) The registry of computer equipment

Articles 588.sexies.a.2 and 588.sexies.b LECrim regulate the access to information storaged in electronic devices. According to such articles a specific judicial decision is necessary to access to said information. It is not possible to extend the already issued order, for example, for a domiciliary search, to the device located in this domicile.

The Spanish legislator has granted express protection to the information contained in computers, Flash memory and other storage devices following the thesis maintained by the Constitutional Court Judgment 117/2011, of 4 July. This judgment established that access to the information stored in a device must be granted by a judicial authority because it is possible to make a detailed profile of the personality of the user of this device with all the information obtained.

The general principles already developed throughout this article apply to this measure, that is, the specialty principle by which we must be investigating a specific crime; principle of suitability so it is expected that through this search we can obtain relevant information to the investigation; principle

of exceptionality, for which there is no other less invasive measure to obtain such information; and the proportionality by which it is necessary to balance the seriousness of the crime, its social transcendence or the technological means used, the intensity of the existing evidence and the relevance of the desired result[13].

Article 588.sexies.c of the LECRIM, limits the object of the judicial authorization to the folders, files or data that can be extracted from the memory of the device that could have a direct relationship with the facts, that is to say that it will not be able to extract irrelevant information to the investigation from these devices. However, if the analysis of its content reveals evidence of another crime being committed (i.e. when a massive scam is being investigated but pedophile material is found in a computer) under the doctrine of the "casual finding", the police officer who discovered it, should immediately inform the judicial authority so that a different investigation could start with all the guarantees.

It is worth mentioning the ECHR ruling in the case of Trabajo Rueda v. Spain of May 30, 2017, which judged a case of a Spanish citizen who took his computer to repair to a specialized store and the technician, after opening the folder «My documents» found that there were files with pedophile content in it, which he reported to the police. The agents proceeded not only to examine the files contained in that folder, but also accessed the «Incoming « folder of the E-Mule file exchange program. Subsequently the agents communicated the investigation to the judge. Mr. Trabajo Rueda was sentenced to four years in prison for the crime of corruption of minors, possession and distribution of images of children for pornographic purposes, which he failed to serve because he fled and the penalties became time-barred. His appeal to the Constitutional Court[14] was dismissed because the Court considered that he made the whole content of the computer available to a computer technician without any restriction. The ECHR on the contrary understood that the registration of the files by the police was not proportionated to the

[13] Article 588.bis.a of the LECRIM

[14] Judgment of the Spanish Constitutional Court of November 7, 2011

legitimate purpose of ending the commission of an offence, since there was no urgency or risk of disappearance of files that would allow elude prior judicial authorization. In the literal words of the Court:

42. In the opinion of the ECHR, it is difficult to assess, in this case, the urgency that would have forced the police to intervene in the archives of the complainant's personal computer and access its content, without previously obtaining the judicial authorization normally required. In fact, there was no risk of disappearance of files since it was a computer intervened and retained by the police and not connected to the Internet. The ECHR fails to detect the reasons why waiting for a prior judicial authorization, which could be obtained relatively quickly, would have hampered the investigation carried out by the police on the facts denounced.

43. Consequently, the ECHR considers that the intervention and examination by the police of the computer files, as they have been done in this case, were not proportionate to the legitimate purposes intended and therefore "necessary in a democratic society" in accordance with article 8 § 2 of the Convention.

44. Consequently, there has been a violation of Article 8 of the Convention.

Investigation methods. special reference to the european investigation order

We can define European Investigation Order as a ruling issued or validated by an authority of a Member State, to carry out one or several specific investigative measures in another Member State, in order to obtain evidence in the context of an investigation[15]. Article 186.3 of the Mutual Recognition Law, and Article 3 of Directive 2014/41/EC of the European Parliament and of the Council of 3 April 2014, provides for the possibility that the order covers all the measures of investigation, obviously including the intervention of communications, to which both legal texts expressly refer[16]. The previous

[15] Directive 2014/41/EC and articles 186.1 and 2 of the Mutual Recognition Law 23/2014 of November 20

[16] Article 202 of the Mutual Recognition Law, and articles 30 to 31 of the Directive 2014/41/EC Chapter V.

system of letters rogatory made the process slow and difficult, and apart from really serious cases, it was avoided. Through this new regulation, the process has become more agile and dynamic, since the judicial authorities have a homogenous template for the entire Union where the necessary information is included so that the executing State can comply with the order, and also, as the template is uniform in all countries, locating the necessary information to execute the order is easier.

When issuing a transnational interception of communications, the requesting State may agree with the executing State that communications be transmitted directly, or conversely, that the executing State intercept and record communication to then send it to the issuing State[17]. It is even possible to intercept communications without technical assistance from the State where the person being investigated is, it will be enough to notify the State of the existence of the criminal procedure and inform it that its technical assistance is not necessary[18].

Finally it is possible to refuse executing an investigation order issued by another Member State to intervene communications in Spain, for the reasons set out in Articles 21.1 and 207 of the Mutual Recognition Law and also in those cases where such intervention would not have been authorized if the case took place in Spain. Such refusal must be communicated to the issuing State as soon as possible, and in any case within 96 hours of receiving the request, Article 222 of the Mutual Recognition Law.

Right to the secret of communications in specific cases

a) The undercover virtual agent

The art. 282bis.c of the LECRIM allows officials of the Judicial Police to act under fake identity in communications maintained in closed channels of communications, after a judicial order being granted, in order to clarify any of the crimes referred to in Section 4 of the same precept or any of the offences provided for in art. 588.ter.a LECRIM. This new method of investigation tries

[17] Article 221 of the Mutual Recognition Law

[18] Annex XV of the Mutual Recognition Law

to adapt the figure of the undercover agent to new technologies. Let's imagine for example a pedophile organization that captures minors through social networks, the judge can authorize an undercover virtual agent to create profiles in said social network to contact the leaders of the criminal group, know how to act, where etc. The main difference between both forms of investigation is that the real identity of the agent is preserved by a virtual identity; so the precautions for the preservation of the identity of the agent contained in sections 1 and 2 disappear with the mere creation of a fictitious virtual identity.

While the undercover virtual agent uses closed communication channels, these are still protected by article 18.3 of the SC. Therefore, judicial authorization is necessary not only to communicate with the supposed identity but also to exchange or send illegal files and analyze the results of the algorithms applied for the identification of said illicit files.

Using this investigation technique makes declaring the secret nature of the investigation necessary (because notifying it to the suspect would frustrate it completely) For that reason the principles of art. 588.bis.a of the LECRIM are applicable again[19].

b) The interception of correspondence and postal parcels

The Spanish Supreme Court, in its Judgment 397/2018 of September 11, makes us notice the obvious difference, in terms of human rights, between correspondence and postal parcel service. This difference in treatment was established by Spanish jurisprudence and finally with the amendment of Organic Law 1/2015 it was transferred to the text of the Law[20]. Consequen-

[19] That is, specialty, suitability, exceptionality, necessity and proportionality that we have already analyzed

[20] Article 579.4 LECRIM: *4. No judicial authorization shall be required in the following cases: a) Postal services that, due to their own external characteristics, are not usually used to contain individual correspondence but to serve the transport and traffic of goods or in whose exterior is recorded its content. b) Those other forms of sending correspondence under the legal format of open communication, in which an external declaration of content is mandatory or that include the express indication that inspection is authorized. c) When the inspection is carried out in accordance with customs regulations or proceeds in accordance with the postal regulations that regulate a certain type of shipment.*

tly, since there is no communication process in the delivery of parcels but the shipment of objects and merchandise, article 18.3 of the Constitution does not come into play. International standards of the Universal Postal Union[21] include two different regulations, the Regulation on mailings and the Regulation on postal parcels. This difference is also recognized by European Union Law, through Directive 97/67/EC, on common rules for the development of the internal market of Community postal services and the improvement of quality of service. That Directive[22], distinguishes between postal item (article 2.6) and item of correspondence (article 2.7). At a national level the regulation is also separated according to the type of delivery, Law 24/1998 of July 13, universal postal service and liberalization of postal services (Article 15.2.B, a and b) and the Royal Decree 1829/1999 of December 3, which approves the Regulation about postal services, in development of Law 24/1998 of July 13 (Article 13.2)

The right to secrecy of communications extends its protection against any kind of interception in the communication process, being indifferent the procedure used to access. In this way, this right is violated even when the information is not obtained by opening the package or the letter itself which remain closed. The existence of the communication, the identity of the correspondents, the moment it takes place, the places of remission and destination, are all data that, once the communication process is initiated, are secret for anyone outside the two people involved, it is therefore sensitive information. The people who provide the postal service may use the information of the shipping process described above for the sole purpose of providing the service[23].

The Supreme Court, in the aforementioned judgment, maintains that such a doctrine must be nuanced in the case of postal communication, because what is protected is human communication, consequently only the access to

[21] Proceedings of the Beijing Congress of 1999. Ratification by Spain published in the Official Gazette of the State no. 62, of March 14, 2005

[22] Approved on December 15, 1997

[23] Constitutional Court Decision 123/2002 of May 20. Grounds Fifth and Sixth

the content of the message will affect that right. Therefore it will not affect it procedures designed to know the content of the parcel or envelop but ineffective to discover the message, for example, trained dogs or the use of scanners.

c) The interception of the communications of persons deprived of liberty. Special mention to lawyer-client communication.

In the Spanish case, there are legal provisions that expressly regulate the communications of prisoners, Article 51 of the General Penitentiary Law, and 46 and 47 of the Prison Regulations. We cannot ignore that prison does not imply the loss of more rights than those inherent in the deprivation of liberty or the accessory penalty[24], so inmates retain their right to secrecy of communications.

Although in the criminal field the investigation of the crime justifies the adoption of this measure, in the penitentiary domain, its purpose is to guarantee security, the interest of the treatment and the good order of the Penitentiary Establishment[25]. Therefore, given that these are preventive interventions, the inmate is notified, unlike what happens with the ones adopted in the framework of a criminal investigation, at the risk of frustrating its success.

Under these precepts and the previous version of article 579 of the LECRIM, judicial decisions were issued granting interception of the inmate's communications. However, the Constitutional Court Judgment 145/2014 of September 22 considered such measures as a violation of the fundamental right to secrecy of communications. In the case analyzed by this judgement, the conversations were recorded in the jails of a police

[24] Article 25.2 of the Spanish Constitution*: 2. Prison sentences and security measures shall be aimed at reeducation and social reinsertion and may not consist of forced labor. The inmate will enjoy the fundamental rights of this Chapter, except for those that are expressly limited by the content of the conviction, the meaning of the sentence and the penitentiary law. In any case, the inmate will be entitled to paid work and the corresponding Social Security benefits, as well as access to culture and the integral development of their personality.*

[25] NISTAL BURÓN, JAVIER. 2015. The intervention of the verbal communications of the detainees in police dependencies. Aranzadi Doctrinal Magazine no. 1/2015 part Studies. Editorial Aranzadi SAU.

station and not in a prison. This recording was ground for conviction of the crimes of aggravated murder, illegal detention, robbery with violence and intimidation and illegal possession of weapons. The Constitutional Court considered that the recordings made under the article 579 of the LECRIM, and of the penitentiary legislation, were contrary to Article 18.3 of the Constitution. The Court reasoned that, in the first place, article 579 only contemplated telephone conversations, and in the second place, prison regulations serve a purpose other than the investigation of a crime. In the end the Constitutional Court concluded that a legal gap like the one we are analyzing (conversations between detainees in the cells) cannot be filled through the analog application of another similar rule. This is so because the reservation of law is the only effective way to guarantee the legal security requirements of citizens in the area of their fundamental rights and public freedoms.[26]

Moving on to the intervention of communications between a lawyer and his or her client deprived of freedom, we must bear in mind that the criminal process of the Rule of Law is structured on the accusatory principle and the presumption of innocence. The right of defence, as right to any accused, is essential in the process so that the judicial power, can only operate given certain conditions guaranteeing the rights of the parties, and especially the accused. In the words of the Supreme Court[27]:*Justice obtained at any price ends up not being Justice.*

The Spanish Constitutional Court has indicated (among others in its judgment 1560/2003) that *"the trust of the client on the professional and human conditions of his or her Lawyer occupies an outstanding place in the exercise of the right of legal assistance when it comes to the defence of an accused in criminal proceedings"*. On the other hand, the confidentiality of relations between the accused and his or her counsel is an essential element[28]. At the

[26] Article 53.1 of the Spanish Constitution

[27] Supreme Court Judgment 79/2012 of February 9

[28] ECHR Castravet v. Moldova March 13, 2007 and Foxley v. the United Kingdom on June 20, 2000.

Judgment of the ECHR on October 5, 2006, Marcello Viola v. Italy (61), it was said that "... an accused's right to communicate with his advocate out of hearing of a third person is part of the basic requirements of a fair trial in a democratic society and follows from Article 6 § 3 (c) of the Convention. If a lawyer were unable to confer with his client and receive confidential instructions from him without such surveillance, his assistance would lose much of its usefulness (see *S. v. Switzerland, 28 November 1991, § 48, Series A no. 220). The importance to the rights of the defence of ensuring confidentiality in meetings between the accused and his lawyers has been affirmed in various international instruments, including European instruments (see Brennan v. the United Kingdom, no. 39846/98 §§ 38-40, ECHR 2001-X)*".

In this regard, the Court of Justice of the European Union in the judgment of the Grand Chamber of September 14, 2010, (40) stated that "*confidentiality of written communications between lawyers and clients should be protected at Community level.*", when: "*... first, that the exchange with the lawyer must be connected to 'the client's rights of defence' and, second, that the exchange must emanate from 'independent lawyers', that is to say 'lawyers who are not bound to the client by a relationship of employment*"

In this type of communication where the accused expresses himself or herself freely about what happened, it is evident that, if the investigators know or can know the content of these conversations, the defence loses most of its effectiveness. In the Judgment of the ECHR Castravet v. Moldova, (50) the Court affirmed that "*if a lawyer were unable to confer with his client and receive confidential instructions from him without surveillance, his assistance would lose much of its usefulness, whereas the Convention is intended to guarantee rights that are practical and effective (see, inter alia, the Artico v. Italy* judgment of 13 May 1980, Series A no. 37, p. 16, § 33)". It is not necessary, therefore, to take advantage of this information improperly obtained to cause a breach on the right of defence. The mere possibility of knowing is already an advantage, (and with greater reason the effective knowledge) Knowing if the accused has participated or not in the facts, knowing his or her line of defense, if the investigation is on the right track etc is a more subtle use of the information, but not for that reason non-

existent. The ECHR has indicated in this regard that the interference exists from the interception of communications, regardless of the subsequent use of the recordings[29]. In addition to the right to defence, other rights may be affected, such as the right not to declare, the right of the lawyer to professional secrecy and the right to privacy.

Finally we note that we are not facing an absolute right. The ECHR, in the Marcello Viola v. Italy judgment cited above, stated that "*However, restrictions may be imposed on an accused's access to his lawyer if good cause exists. The question, in each case, is whether the restriction, in the light of the entirety of the proceedings, has deprived the accused of a fair hearing (see Öcalan v. Turkey* [GC], no. 46221/99, § 133, ECHR 2005*IV)*". Both the Constitutional Court and the ECHR require that in order to have access to such communications there must be a legal provision, a sufficient justification in the specific case, that takes into account the available evidence in the case, the need for the measure and respect for the principle of proportionality[30], and in the Spanish case, a judicial authorization.

Finally we must point out that there is an express exception to the secrecy of communications between lawyer and client in prison, contained in article 51.2[31] of the General Penitentiary Organic Law, reserved for terrorism cases. In this way, it is possible to intercept such conversations by means of a judicial decision.

d) Communications between two individuals, recorded by one of the interlocutors

The jurisprudence of the Supreme Court[32] has stated that it does not affect the right to secrecy of communications and the right to privacy when a person

---

[29] Judgment of the ECHR Kopp v. Switzerland of March 25, 1998

[30] Judgment of the ECHR of November 2, 1991 case S. v. Switzerland and STEDH of January 31, 2002 Lanz v. Austria

[31] Art. 51.2 LGP: *The communications of the inmates with the defence attorney in relation to criminal matters and with the attorneys who represent him, shall be held in appropriate departments and may not be suspended or intervened except by order of the judicial authority and in the terrorism cases.*

[32] Judgment case Gürtel- Fitur No 214/2018 of 8 May

records their own conversations with third parties, regardless of whether it is ethically questionable. This rule has exceptions: when the conversation is inciting to crime, when it is used as a means of inquiry by the police, or when these recordings affect the right of privacy. We must also add the cases in which, when the content of the recorded is disclosed, causes damage to privacy or private life. The Constitutional Court itself[33] said that: "*there is no secret for the one to whom the communication is addressed, nor does it imply a contravention of the provisions of article 18.3 of the Constitution the retention of the content of the message. This retention (the recording in the present case) may be, in many cases, the factual basis for communication to third parties, but even considering the problem from this point of view the behavior of the interlocutor cannot be seen preparatory to the constitutional ilict, which is the breach of the secrecy of communications. Who delivers the letter to another or who uses during his or her telephone conversation a voice amplification device that allows capturing that conversation to other people present is not violating the secret of communications, without prejudice to these same behaviors could constitute attacks on the right guaranteed in Article 18.1 of the Constitution in the event that what is transmitted to others enter the 'intimate' sphere of the interlocutor*, [...] *Who records a conversation of others is violating, independently of any other consideration, the right enshrined in Article 18.3 of the Constitution; on the other hand, whoever records a conversation with another does not incur, by this single fact, in conduct contrary to the aforementioned constitutional precep*".

In spite of above, the Supreme Court judgment 178/1996 of 1 March rejects the validity of the recording, as having being admitted as a piece of evidence would breach the right of the accused not to testify against themselves and not to plead guilty. The conversation did not arise spontaneously and had the interlocutors known that they were being recorded it would have had a different content or at least the interlocutors would have accommodated their questions and answers to the situation created by the existence of a recording instrument. The content of a conversation obtained by these methods

[33] In judgments 114/1984 of November 29 and 56/2003 of March 24

cannot be incorporated into an ongoing criminal process when it is used as a piece evidence of a confession since it has occurred without any of the guarantees established by the constitutional principles and it is null and void.

REFERENCES:

Directive 2014/41 / EC of the European Parliament and of the Council of 3 April 2014

European Charter of Human Rights

European Convention for the Protection of Human Rights and Fundamental Freedoms of November 14, 1950

General Penitentiary Law and Penitentiary Regulation

Judgments of the European Court of Human Rights Trabajo Rueda v. Spain of May 30, 2017; Marcello Viola v. Italy; S. v. Switzerland of November 2, 1991, Brenan v. the United Kingdom, no. 39846/1998; Castravet v. Moldova; Kopp v. Switzerland of March 25, 1998; Lanz v. Austria of January 31, 2002

Judgments of the Spanish Constitutional Court 123/2000; 1560/2003

Judgments of the Spanish Supreme Court 397/2018 of September 11; case Gürtel- Fitur No 214/2018 of 8 May

Mutual Recognition Law 23/2014 of November 20

NISTAL BURÓN, JAVIER. The intervention of the verbal communications of the detainees in police dependencies. Aranzadi Doctrinal Magazine no. 1/2015 part Studies. Editorial Aranzadi SAU. 2015

Spanish Constitution, 1978, December 8

Spanish Criminal Procedure 1889