Privacy as Data Protection: Some Critical Legal Problems

Yolanda Doig, Olga Fuentes, Alfonso Ortega e Isabel Turégano

Members in the Project AICO 2017/161 *La era digital,nuevos problemas para el derecho" (PI Olga Fuentes)

Universidad Miguel Hernández and Universidad de Castilla-la Mancha (Spain)

Introduction

This paper is presented as a collective contribution of members of the multidisciplinary project *Digital Age: New Problems for the Law*, funded by the Generalitat Valenciana, which aims at analysing and discussing some crucial impacts that communication and information technologies are having on our legal systems. Our present proposal revolves around the content and reach of a conception of privacy interpreted in an informational sense. The controversial separation of the public and private spheres is particularly troubling nowadays given the current capacity of governments and enterprises to collect and use personal information. Starting with a conceptual approach to the meaning and value of privacy where the cluster of moral pretensions and reasons implied can be a guide to legislative and judicial decisions, the paper goes on to deal with three problems that have been considered worthy of particular attention. First, the recording of communications of customers that financial institutions will accomplish in accordance with the European regulation on market abuse raises particular concern about their impact on privacy. Secondly, the use of video surveillance evidence has been considered by our constitutional jurisprudence specially protected by informational self-determination. But this interpretation can generate an interesting debate about different standards of evidence in social and criminal jurisdictions. Finally, the intrinsic vocation to internationalisation of information flows requires an international legal perspective from which to consider the new European legal regime as well as to reflect on disputes resolution and applicable law.

1. Privacy in Information Technology: Concept and Foundations for Regulation.

A free society favours the diffusion of information as a solid basis for a free and committed citizenship and the control of governmental and market institutions. However, information irresponsibly wielded can become a hazardous instrument that undermines foundational values of a society. In the Internet era, the growth and possibilities of processing data imply a particularly severe risk for privacy. At first sight, it is so because it becomes more difficult to preserve a reserved sphere where to build and develop our personality outside the eyes of others. Yet it is not simply a negative matter of personal privacy or intimacy. It is also an issue of an increased informational power of private and public institutions at the expense of individuals. Defining privacy in a broad sense as a guarantee of non-domination requires, first, stating the relation of the concept with intimacy and, then, exposing its broader implications with other values in the context of information technologies. Here privacy appeals to values beyond intimacy since "the emergence of Big Data creates clear winners and losers"[1].

Intimacy and privacy are interrelated concepts. However, and against linguistic common uses[2], it is necessary to draw a conceptual distinction between the intimate and the private, according to Garzón Valdés[3] or Castilla el Pino's[4] proposals. Some important normative issues underlying the debate about the risks of information technologies are better enlightened if we separate the inner sphere where the most profound individual

[1] Strahilevitz, Lior Jacob (2010). "Toward a positive theory of privacy law", *Harvard Law Review*, vol. 126, pp. 2010-2042, at 2021.
[2] Toscano, Manuel (2017), "Sobre el concepto de privacidad: la relación entre privacidad e intimidad", *Isegoría. Revista de Filosofía Moral y Política*, nº 57, pp. 533-552, at 544.
[3] Garzón Valdés, Ernesto (2003), "Lo íntimo, lo privado y lo público", *Claves de Razón Práctica*, nº 137, pp. 14-24.
[4] Castilla del Pino, Carlos (1989), "Público, privado, íntimo", en Castilla del Pino (ed.), *De la intimidad*. Barcelona: Crítica, pp. 25-31.

identity and autonomy are formed from the shared experiences of privacy, not always founded in our desire to partake this inner life in a caring context.

The origin of the idea of intimacy lies in the liberal defence of autonomy and the need for a realm reserved for the full realization of individuals[5]. As Garzón Valdés stated, the intimate is "the sphere of each person's thoughts, of the formation of decisions, of doubts that escape a clear formulation, of what is repressed, of what has not yet been expressed and perhaps never will be, not only because the individual does not want to express it but because it cannot be expressed"[6]. The sphere of intimacy is the last redoubt of the individual's personality, in which the individual fully exercises her sovereignty and decides her social, private and public, behaviour. Therefore, any intervention in a person's intimacy affects her autonomy and her dignity as a human being. Our inner lives should be developed under the protection of public exposition that would inhibit the free operation of personal feeling, fantasy, imagination, and thought[7]. Individuality is realized through experimental self-discovery, which requires space free from evaluation and risk[8]. The more our inner lives are being exposed, the more we are tempted to act in compliance with collective norms and we are subjected to approval of others[9].

Intimacy is irradiated in those private areas that are reserved for a kind of interpersonal relationships where the individual's desires and preferences prevail and do not allow for general accessibility. Privacy is the domain of personal freedom, in which individuals try to assert their wishes and preferences. The veil that protects individuals from public gaze is partially lifted at the discretion of each individual to admit certain others. This sphere also plays an important part in the articulation of an inner life in as much as "it permits one to explore unpublic feelings in something other than solitude, and to learn about the comparable feelings of one's intimates, including to a degree their feelings toward oneself"[10]. Privacy in this sense can be understood as shared intimacy. And it is privacy, and not intimacy, that has legal relevance: it is only when intimacy impinges on relationships with others that it becomes a legal issue[11].

Having control over what we expose privately or publicly is what allows us to adapt ourselves to a world of social relationships in which we expose our desires or materialize our preferences according to how they fit our social environment. An individual is much more than what could be integrated into social spaces. The value of privacy lies in the possibility it affords to share our inner experience only with those we choose and, in the degree, that it is appropriate for us to share in a particular relationship[12]. Intimate details can be disclosed for specific purposes in relationships that are far from being thought as intimate, such as medical, financial or legal. What constitutes intimate relationships is not the sharing of personal information, but the context of caring which makes the sharing of personal information relevant. It is in the context of a reciprocal desire to share present and future intense and important experiences that the revealing of personal information takes on special significance[13]. So, what is properly called private is not some kind of event or setting but the kind of relationship in which acts or sharing of information occur. In this sense, a certain place is not private or public in itself. The scope of privacy depends on the different type of interpersonal relationship or context that can generate a reasonable expectation of privacy. And that means the expectation of non-intrusion or, at least, of

[5] Béjar, Helena (1988), *El ámbito íntimo. Privacidad, individualismo y modernidad*. Madrid: Alianza.
[6] Garzón Valdés, E., "Lo íntimo, lo privado y lo público", *cit.*, p. 16.
[7] Nagel, Thomas (1998), "Concealment and Exposure", *Philosophy & Public Affairs*", vol. 27 nº 1, pp 3-30, at 4-5.
[8] Magi, Trina J. (2011). "Fourteen Reasons Privacy Matters: A Multidisciplinary Review of Scholarly Literature", *The Library Quarterly*, vol. 81, nº 2, pp. 187-209, at 195.
[9] Nagel, T., "Concealment and Exposure", *cit.*, p. 20; Reiman, Jeffrey (1995), "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future", Santa Clara Computer & High Technology Law Journal, vol. 11, pp. 27-44, at 41.
[10] Nagel, T., "Concealment and Exposure", *cit.*, p. 20.
[11] Pérez Luño, Antonio (2012), *Los derechos humanos en la sociedad tecnológica*, Madrid: Editorial Universitas, p. 92.
[12] Rachels, James (1975). "Why Privacy is Important?", *Philosophy & Public Affairs*, vol. 4, nº 4, pp. 323-333, at 328.
[13] Reiman, Jeffrey (1976), "Privacy, Intimacy, and Personhood", *Philosophy & Public Affairs*, vol. 6, nº 1, pp. 26-44, at 33-34

notification and request of consent to obtain information and its restriction for specific purposes, as we see below in the case of the use of video surveillance for the control of work activity.

From this point of view, intimacy and privacy are part of a continuum. Firstly, it is in the intimate domain where individuals develop their desires, opinions and thoughts that will be translated into diverse relationships with others in the private sphere. The right to intimacy refers to the power that every individual has to control the access and reach of others to that intimate domain. The right to privacy refers to legitimated restrictions on the accessibility and dissemination of what has been expressed in the context of particular relationships. Secondly, if intimacy is necessary for our autonomy and free development of our personality, privacy provides the space to develop a variety of acts and relationships and to exchange personal information that allows us to explore new facets of our own. Privacy is especially closer to intimacy when private relationships are oriented to express emotions or feelings of love, liking or care[14]. The protection of privacy is then justified in the same reasons that justify the protection of intimacy.

But the province of privacy is broader than that of intimate relationships. In a contextual sense, the concept refers broadly to a plurality of areas or contexts preserved from the public gaze and in which different norms governing roles, expectations, actions and practices operate[15]. The same meaning of control over accessibility to the information disseminated in particular contexts is central to the right of privacy in this broader sense. But its underlying rationale is not just intimacy. The right to data protection is based on the value of privacy as distinct from intimacy. The difference is relevant in cases such as those related to video recordings at work discussed later. While the right to intimacy has a more negative content of exclusion, the right to data protection is conceived in the sense of informational self-determination; that is, as a positive freedom to exercise control over the data and information related to a person that have already left the sphere of intimacy to become information shared in particular relationships. Both rights can be considered independent for various reasons:

1. The right to data protection refers specifically to personal information that can be collected, analysed, processed and disseminated or made accessible to third parties.

2. The rationale under the protection of personal data is not always their intimate nature. There can be other important reasons for such a protection, being especially relevant those that appeal to security, equality and justice[16]. Data protection tries to avoid information-based harms. The fact that personal information is used to inflict harm does not make it primarily a privacy issue but one of security. Protection is also oriented to eliminate information inequality: people value the opportunities, facilities, discounts, and knowledge provided by information technologies in exchange for the use of their personal data. But this willingness to share personal data in exchange for benefits does not take place in a fair and transparent context, in which everyone knows the conditions and results of their decisions and there is an equal opportunity for all. Therefore, data protection should be put in place to guarantee fair and equitable market conditions, appealing to transparency, participation and notification in order to constitute fair contracts. And, finally, uncontrolled use of data generates information injustice. Protection should aim at avoiding transfers of information beyond the context and the purposes for which it was collected. What is to be controlled is the dominant position that possession and uses of data can secure in spheres and for purposes different from the ones they were collected for, particularly in case of secondary uses that may not have even been conceived when it was collected[17].

[14] Innes, Julie (1992), *Privacy, Intimacy and Isolation*. New York: Oxford University Press.
[15] Nissenbaum, Helen (2004). "Privacy as Contextual Integrity", *Washington Law Review*, 79 (1), pp. 101-139
[16] Hoven, Jeroen van den (2004). "Privacy and the Varieties of Informational Wrongdoing", en Richard A. Spinello & Herman T. Tavani (eds.), *Readings in Cyber Ethics*, Jones & Bartlett Publishers, 2ª edn., pp. 489-500, at 491 ff.
[17] Mayer-Schönberger, Viktor and Cukier, Kenneth (2013), *Big Data. A Revolution that Will Transform How we Live, Work, and Think*. New York: Houghton Mifflin Harcourt, p. 153.

3. The ability to capture and keep a huge amount of diverse information has altered the nature of the problem. Big data worries not just because it contains personal information, but also because of the consequences of analysing and correlating data through new technologies. The incomparable increase in the ability to disseminate and provide access to information; the advances in storage, aggregation, analysis, and mining of information; or the enhanced modes of gathering or capturing information from automated devices, service providers and metadata require public intervention. The risks I have referred to so far -insecurity, inequality, secondary uses, decontextualization, scale and aggregation- produce an entirely new menace: they increase the power that a few can have over individuals. The compilation of individual's data is being used to make important decisions about her[18]. An immense power is held by those who have the control over the collection and processing of data. This is so especially when it is exercised in a non-transparent manner, there is no real competition between the agents that have the capacity to execute those activities, and the subjects are unaware or do not participate in the determination of purposes. Control over financial information discussed later is an interesting case where some of these problems emerge. Using the metaphor of the panopticon, Reiman highlighted that privacy is affected "from the way our publicly observable activities are dispersed over space and time" and the way its collection is gathering up "the pieces of our public lives and making them visible from a single point"[19].

The human being becomes a mere object of information instead of a subject of rights[20]. Particularly, when people are classified into categories on the basis of their estimated value or worth and their susceptibility to various appeals[21]. This categorization leads to important injustices. In the first place, it produces losses of opportunities. An individual can be deprived of access to certain goods or services that do not fit the profile that has been attributed to him. Secondly, it generates inequalities. As Lyon states, "the software codes that classify us are designed to distinguish between one group and another to enable people to be treated differently depending on the category into which they fall". Classification and profiling processes favour "the formation of social stereotypes" determining the "attribution of privileges and rights and social exclusion"[22]. Thirdly, it is based on oversimplification, that is, categorization reduces individual diversity to collective models of behaviour. And, finally, it involves loss of autonomy. "Obedience to standards", wrote Bauman, "tends to be achieved nowadays through enticement and seduction rather than by coercion - and it appears in the disguise of the exercise of free will, rather than revealing itself as an external force"[23].

Therefore, the problem of privacy in information technologies is a wider problem than the violation of intimacy. Flow and overuse of personal information is a social reality that individuals cannot restrict by themselves and that affects shared moral values, such as security, equality or inclusion. As such, it is insufficient to consider that the role of legislation is to give individuals the means (notice, access, consent, correction) by which they can act to protect their privacy and to set responsibilities to organizations in collecting and using personal information. This approach aims at providing people with control over their personal data, allowing them to decide how to weigh the costs and benefits of collecting and using their information. Underlying some of the difficulties of this "privacy self-management" framework[24] is the lack of consideration of privacy as a common good that should be enhanced collectively[25]. Being an indispensable condition for a just order, public regulation of privacy should help to move people away from irrationality or indifference when providing personal information and protect the most vulnerable. Government's constraint

[18] Solove, Daniel (2004). *The Digital Person: Technology and Privacy in the Information Age*, New York: New York University Press.
[19] Reiman, J., "Driving to the Panopticon", *cit.*, p. 29.
[20] Garriga, Ana (2018), "La elaboración de perfiles y su impacto en los derechos fundamentales. Una primera aproximación a su regulación en el Reglamento General de Protección de Datos de la Unión Europea", *Derechos y libertades*, nº 38, pp. 107-139, at 138.
[21] Gandy, Oscar (1993). *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview.
[22] Lyon, David (2007), *Surveillance Studies. An Overview*, Cambridge: Polity Press, p. 184-185.
[23] Bauman, Zygmunt (2000), *Liquid Modernity*, Cambridge: Polity Press, p. 86.
[24] Solove, (2013). "Privacy Self-Management and the Consent Dilemma", *Harvard Law Review*, 126, pp. 1880-1903.
[25] Regan, Priscilla (2002). "Privacy as a Common Good in the Digital World", *Information, Communication & Society*, vol. 5, nº 3, pp.382-405, at 395.

of individual choice is legitimate to prevent or preserve foundational goods as privacy[26]. And, as we shall see below, this justified intervention must be nowadays necessarily supranational or global.

Certainly, impeding information flows can have significant economic and social costs. Like any other value, privacy must be weighed with other values when it is regulated. This is the case, for instance, of the problems that arise from the control of financial information, which highlights the conflict between privacy and prevention of market abuse; or the conflict between worker's privacy and employer's interests. When conflict occurs, intimacy provides an ultimate reason as a requirement of human dignity and autonomy strong enough to defeat other moral claims. This explains that those data that affect the "most intimate redoubt of personality" (beliefs, ideology, ethnic or racial origin, sexuality, health, death, family relationships, genetic data) usually require special guarantees in our legal systems. It is a controversial issue which personal data meet a sufficient degree of intimacy or sensitivity to require more guarantees. Data is usually categorized as sensitive according to material social standards that consider their special incidence in matters that individuals may wish reasonably to withhold. But we can doubt if certain personal matters are intrinsically sensitive or it depends on the claim by the individual (norm-dependent or norm-invoking)[27]. In any case, it is not usually interpreted in a subjective sense. It may refer both to the quality of the information or to the reasonable expectations of the individual, in the objective sense that most people in a given society choose not to reveal. In other cases, a protective criterion is used according to which those data whose dissemination entails a greater risk of domination, discriminatory practices or depiction of the individual in an unfavourable light are sensitive.

2. Privacy and Financial Information within the Scope of the Criminal Process[28]

2.1. Introduction

Although the use of video recordings as a source of evidence has been subject to questioning in the fields of labour and criminal law, due to the especially invasive nature of the recording of the subject's personal activity, in an area that is as different in scope as is the financial field, we are now witnessing the creation of a new kind of financial reporting – involving telephone communications, electronic communications and video conferencing – of all the transactions that take place daily in institutions, with the purpose of combating market manipulation through the use of insider information. Regulation (EU) No. 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse is intended to preserve the integrity of the internal market by prosecuting the carrying out of transactions using insider information, illegal communication of such information and market manipulation. As a complement to, and effective guarantee of its enforcement, Directive 2014/57/EU of 16 April 2014 provides for criminal sanctions to punish market abuse behaviours, in the face of the evident inadequacy of administrative sanctions.

The basic premise of Regulation (EU) No. 596/2014 is that market abuse is the main obstacle to economic growth and market wealth. From there, the above-mentioned regulation defines those behaviours that are condemned, not only by specifying the situations that constitute infringements and those that do not, but also illustrating with examples the behaviours that the State intends to prosecute and punish.

The above descriptive effort is not sufficient to ensure the integrity of the market; it is necessary to provide the authorities of each State with effective powers, instruments and resources to enable detection and demonstrate the infringement in order to punish it. With this goal in mind, measures are articulated, such as access to the premises of natural and legal persons for the purpose of seizing documents, whenever there is reasonable suspicion of the existence of documents and data related to an investigation into insider dealing or

[26] Allen, Anita (2011). *Unpopular privacy: What must we hide?*. Nueva York: Oxford University Press.
[27] Wacks, Raymond (2010). "Should the Concept of Privacy be Abandoned?", *Law, Morality, and the Private Domain*. Hong Kong: Hong Kong University Press, pp. 235-248.
[28] This paper is part of the research project "The Digital Era: New Problems for the Law" (AICO/2107/161) funded by the Generalitat Valenciana's Conselleria d'Educació, Cultura i Esport.

market manipulation. Depending on the laws of each State, such access may require the prior authorization of the judicial authority of the Member State concerned. In addition to entry into the premises, there is another instrument that will serve in the investigation: access to the data traffic and recordings of telephone conversations held to make purchases, and to discover and corroborate the existence of transactions involving insider dealing.

As recognized by Regulation (EU) No 596/2014 itself, data traffic and telephone conversations constitute decisive evidence and, in some cases, the only evidence that can prove insider dealing and market manipulation, and that is why these must be recorded and stored by the institutions for some years. Although this evidence may be key to detecting an infringement, it will mean accessing information of quite different types, since it will entail recording, managing and storing all communication related to the purchase and sale of any financial product, whether they be swaps, bonds, derivatives or shares, between all those people who in some way or another have contributed to closing the transaction. This means that not only will communications between the client and the employee who is responsible for marketing the product be recorded, but any and all previous and internal communications directed towards concluding the transaction – even if it ultimately fails to materialise – will also be stored[29]. For illustrative purposes, these include all those the trader holds with the sales distribution desk, either to close or negotiate the final selling price, determine details of the transaction or set the due date, the interest rate or the price of the transaction. All communications aimed at closing a transaction and all their contents are subject to being recorded, without discrimination, so it may be that a recorded conversation includes not only financial information, but also personal or family issues related to the client or the institution's employees.

According to this system of recording and storage – which must be durable and safe – all conversations and all electronic correspondence between the client and the institution – aimed at closing a transaction or service – shall be stored in such a way that it allows the transaction to be reconstructed from its beginning to its conclusion in a short period of time.

The objective of this system is to quickly detect transactions involving market abuse, initiate the relevant investigation and locate evidence to enable the punishment of the employee, the client or the corresponding institution.

2.2. Recording of telephone communications and access to documentation. Regulatory Framework

As already stated, in order to detect and punish the carrying out of transactions involving insider dealing, illegal communication of such information and market manipulation, the records made by the investment services company, credit institution or financial institution of the data traffic and telephone conversations between its employees and its clients constitute an essential piece of evidence.

Thanks to this information, the competent authority will be able to identify the person responsible for disseminating false or misleading information, the contact maintained for a period of time or the relationship between them.

The scale of the information available to each banking institution and which will be made available to the administrative authority, is explained in Recital 65 of Regulation (EU) No. 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse, and in particular is found in art. 23, which details the functions and the powers exercised by the competent authorities, in accordance with national legislation, in the field of oversight and investigation. These powers include accessing any document and data regardless of its format and requesting existing recordings of telephone conversations, electronic communications and data

[29] European Securities and Markets Authority, Questions and Answers, On the MiFID II and MiFIR investor protection and intermediaries topics, p. 38. Accessible at https://www.esma.europa.eu/system/files_force/library/esma3543349_mifid_ii_qas_on_investor_protection_topics.pdf June 2018 (8).

traffic records kept by the investment services companies, credit institutions or financial institutions. They may also require, to the extent permitted by national legislation, existing records on data traffic held by a telecommunications company when it is reasonably suspected that an offence has been committed, and these records may be relevant to the investigation of transactions or recommendations using insider information. In the case of Spain, currently the data traffic will be provided by communications operators or service providers as long as it is related to the investigation of an offence, there is sufficient evidence, and a judicial resolution has been taken in this regard[30], as provided for in art. 588 ter j) of the Criminal Procedure Act.

For its part, Directive 2014/65/EU of the European Parliament and of the Council, which establishes a framework for a regulatory regime for financial markets in the European Union, recognizes the power of the competent authority to require investment services companies to hand over their records of phone conversations, electronic communications or data traffic held by an investment services company or a credit institution, with the aim of detecting and punishing the practices of market abuse or the failure to comply with the requirements laid down in the Directive, provided there is a reasonable suspicion that such records, relating to the subject matter of the inspection or investigation, may be relevant to demonstrate market abuse behaviours.

The same Directive, when it lists the requirements that must be fulfilled by investment services companies, requires a record of all the services, activities or transactions that are performed, which includes the recordings of telephone conversations or electronic communications relating to transactions on their own account and at the order of clients. The communication which will be recorded, stored, monitored and possibly used in a criminal process, shall be both telephone and electronic, and this category includes video conferencing, fax, email, Bloomberg mail, SMS, chat, instant messaging and mobile applications[31].

As a preliminary step to this measure, clients of the company, both new and old, will have to be notified that communications and telephone conversations will be recorded, and if such a notification has not been previously given, the investment services company (art. 17) shall not provide services by telephone, nor carry out investment activities with that client.

Obviously, the client can communicate their orders using another channel other than electronic communication or telephone, but in that case, it should be recorded in a long-lasting medium and, in the case of transactions negotiated in conversations, the record will consist of minutes and notes. In this case, information will be logged about the date and time of the meetings, the place, the identity of attendees, promoters of the meeting and information about the order.

And among the precautions to be taken, it must be shown that the company took "reasonable steps" to prevent their employees from carrying out, sending or receiving phone calls or electronic communications through private devices that the company cannot record or copy.

The records shall be made available to clients and shall be kept for a period of five years, except where the competent authority requests that they be kept for a period of up to seven years. According to Delegated Regulation (EU) 2017/565, they have the right to request a copy of the recording during the term of 5 years.

This record of electronic communications and data traffic that financial entities have implemented is described with detail in Commission Delegated Regulation (EU) 2017/565 of 25 April 2016, which in art. 76 outlines the

[30] MARCHENA GÓMEZ, M., La Reforma de la Ley de Enjuiciamiento Criminal en 2015 (The Reform of the Criminal Procedure Act in 2015), Castillo de Luna Ediciones Jurídicas, Madrid, 2015, p. 288.

[31] European Securities and Markets Authority, Questions and Answers, On the MiFID II and MiFIR investor protection and intermediaries topics, p. 41. Accessible at https://www.esma.europa.eu/system/files_force/library/esma3543349_mifid_ii_qas_on_investor_protection_topics.pdf (8 June 2018).

"recording of telephone conversations and electronic communications policy" that investment services companies have to comply with.

According to this article, the recording policy should be available in writing and its scope shall correspond to the institution, nature, scale and complexity of the institution's activity. In all cases, and irrespective of their number, such recordings will make it possible to identify the telephone conversations and electronic communications, on the one hand, and their content, on the other, provided that these are transactions carried out when trading on their own account and when providing services related to the reception, transmission and execution of client orders, even if those conversations or communications do not give rise to the conduct of such transactions or services (art. 16.7 Directive 65).

With regard to its requirements, the recording policy must specify the procedures that guarantee that the company has implemented a system for those cases in which the recording is performed on devices provided by the company to an employee or hired person, and also, will determine the actions to be taken when performing communications or calls from personal devices which do not fall within the scope of recording (art. 16.7 3rd and 8th paragraph, Directive 65). To this end, a record of people who have devices that are the property of the company or their own private property, whose use has been approved by the company, shall be maintained and regularly updated.

However, that record of transactions and orders, including the communications, will not only serve to identify the transaction and those involved in case a violation of the market abuse rules is detected, it will also be continuously monitored by the investment service company with the aim of ensuring compliance with the recording requirements and the rest of the regulatory obligations provided for in Directive 2014/65/EU[32]. The criteria that will determine the frequency and purpose of monitoring, as an example but without limitation, may be the volume and frequency of transactions on their own account; the volume, frequency and characteristics of the orders from clients; the characteristics of clients; financial instruments and services offered and the conditions of the market accounts.

2.3. Extension of the measure

The recording of telephone and electronic communications, in the process of being implemented in financial institutions, is not only aimed at ensuring the integrity and transparency of the system, but also at ensuring, in the event of disciplinary procedures being opened for market abuse, that it has the virtue of constituting evidence, and this, however, raises questions about its procedural legitimacy. Firstly, due to the regulatory framework in which it is scheduled, it is not a framework decision that is binding on the target, but a Directive that sets out the objectives but whose effectiveness rests on the Member States of the EU and requires a law of transposition.

Secondly, since it constitutes a measure with the power to impact on fundamental rights, such as the right to privacy (art. 18.1 EC), the right to the inviolability of communications (art. 18.3 EC) and the right to the protection of data (art. 18.4 EC), it requires clear and precise regulations on how to combat the risks of abuse or misuse of the data to be stored.

Thirdly, it could be argued that the communication which will be subject to recording does not require the same degree of protection or safeguarding, due to its proprietary nature; however, although this is true, it is nevertheless a large database of personal and private data, subject to automated processing and with a high risk of irregular access. There are doubts as to whether this intervention, approached in such general terms

[32] European Securities and Markets Authority, Questions and Answers, On the MiFID II and MiFIR investor protection and intermediaries topics, p. 39. Accessible at https://www.esma.europa.eu/system/files_force/library/esma3543349_mifid_ii_qas_on_investor_protection_topics.pdf (8 June 2018).

because it records the entire conversation indiscriminately, is strictly necessary to achieve the intended purpose or if provision should be made for some sort of differentiation, limitation or exception.

3. The Probative Value of Video Surveillance: Between the Right to Privacy and the Right to Data Protection. Its Different Treatment in Social and Criminal Jurisdiction[33]

The use of video recordings as a source of evidence has been questioned on multiple occasions and, of course, rejected or disallowed, due to the obtaining of the recording being considering illegitimate when it was in violation of fundamental rights; to such an extent that, due to the particularly invasive nature of the capturing of the personal activity of the recorded subject, it is often frequently condemned. That is, precisely, the focus of the role played by art. 11.1 of Spain's Judiciary Act (LOPJ) when stipulating that evidence obtained in a way that directly or indirectly violates fundamental rights is not admissible.

At the present time, one of the areas in which the use of these video recordings has played its largest role is in the field of employment law, with its use protected under the power to monitor granted to employers by art. 20.3 ET (Workers' Statute). In this particular context, the TC (Constitutional Court) has been delineating an interesting legal principle whereby the recording of the work activity of workers within the company is not seen as affecting, in general terms, their right to privacy, especially if the recording takes place in communal areas of the company exclusively intended for the carrying out of the worker's contractual obligations (compare cash registers at a supermarket as opposed to the greater controversies that arise with any recording in an office which, while being the property of the company is intended for private use[34] or, of course the ban on its use in spaces such as toilets or changing rooms[35]). The TC also recognizes that, more than the right to privacy, these recordings affect the right to informational *self-determination* (or the right to data protection) expressed in art. 18.4 CE (Spanish Constitution) (Sentence of the Constitutional Court STC 29/2013, 11 February). By extension, then – and as long as the recording of the image is the personal data of the worker (art. 3, Spanish Data Protection law, or LOPD; STC 173/2013, of 7 October) – the right of the worker to know (in other words to be informed) of the place and manner in which their data is collected, and the intended purpose to which the data will or may be put, is enshrined in the legislation (art. 5 LOPD)[36].

[33] This paper is part of the research project "The Digital Era: New Problems for the Law" (AICO/2107/161) funded by the Generalitat Valenciana's Conselleria d'Educació, Cultura i Esport.

[34] SSC 239/2014, of 1 April uses terminology imported from that used by the European Court of Human Rights (ECHR) to pronounce on the difference between recording in open spaces, such as those where cash registers are found, and recording in an office, based on the "reasonable expectation of privacy" stating that: "the recording cameras were installed in at least two different places. In one area was the cash register, where the money was taken. The substance of the judgement is that all workers or, at least, most of them, had access to this location (…). It cannot be claimed that there is a reasonable expectation of privacy in a place of common access for the performance of the functions that each worker is assigned by the company within the employment relationship. In that case, the company's power to manage and its related powers, does not impinge on the right to privacy of the workers when placing recording cameras in public areas with widespread access in which the general working activity of the company is performed. This is not the case with the cameras that were installed in the office of the defendant. (…) In principle, a single office is a room allocated to a particular person, and consent is required before facilitating the visual or personal access of third parties to the same. Therefore, in general terms, it can be said that the holder of the same has a reasonable expectation of privacy within his or her office, which may be violated if recording cameras are installed without their knowledge."

[35] STS (Sentence of the Supreme Court) 620/1997, of 5 May.

[36] See STC of 3 March 2016, as well as the more restrictive interpretation, on the need to inform the worker, which is contained in the individual opinions. With regard to developments in doctrine and jurisprudence that have led to the view of recordings as attacking the right to the protection of personal data and not, strictly speaking, against the right to privacy; as well as on employment and administrative demands to ensure that the recording of the work activity for the purpose of monitoring by the employer is not considered an attack on the fundamental rights of the worker, see ARRABAL PLATERO, P., "La videovigilancia laboral como prueba en el proceso" (Labour Video Surveillance as Evidence in the Judicial Process) Revista General de Derecho Procesal, Iustel, September-October 2015, www.iustel.com.

On the basis of these previous positions, the TS (Supreme Court) and TC have laid down the fundamental criteria for permissible recordings arising from the installation of video cameras by the employer provided that: 1) it is either a case of ordinary monitoring or there is a prior suspicion of unlawful behaviour[37]; 2) the measure passes the test of proportionality (suitability, necessity, and proportionality in the narrow sense) and 3) the workers are unequivocally informed and the express purpose of the recording for monitoring is stated[38].

It is interesting to note that the suspicion of illegality of the activity or alleged failure to comply with employment terms is not always necessary as a prerequisite for the validity of the recordings. Ordinary measures exist to monitor the work activity that the employer can deploy without having had any suspicion of non-compliance on the part of the worker (and which would enable the employer to install recording cameras provided that workers are expressly warned of this); and, together with these, there is also the possibility of extraordinary monitoring measures that, on suspicion of the commission of an illegal activity, would authorize the employer to install cameras and legitimise the use of the recordings, even without the corresponding arning to the worker[39]. From this perspective, one might understand that in the case of recordings made as part of ordinary monitoring activity, the capture of illegal activities performed by the worker that fall outside the purpose of the recording may not be used as a source of evidence substantiating any disciplinary action in the workplace. However, in my opinion, it will be necessary to introduce some nuance to this possible interpretation of the regulations in order to sustain a consistent application in the different areas of law.

A direct consequence of the jurisprudential construction presented is the paradoxical situation in which the same recording could be admitted as evidence in employment proceedings, since there has been no breach of fundamental rights to obtain it, but nevertheless it will be inadmissible in criminal proceedings according to art. 11.1 LOPJ, since it does violate fundamental rights (or vice versa)[40].

This is the conclusion that could be drawn from an extrapolation of the arguments contained in the STC 29/2013, of 11 February that overrides the disciplinary sanction imposed on a worker at the University of Seville who was in breach of his work schedule according to what could be verified from recordings obtained by a camera that he had not been warned had been installed and which had a different purpose (security) that was outside the area of the corporate monitoring of work activity. The question that can be raised in this case is what would have happened if, instead of the worker not complying with his work schedule, the recording

[37] Regarding the suspicion of the employer in regard to the unlawful activity of the worker, two interesting rulings of the ECHR should be noted: the case of Köpke against Germany (ruling of inadmissibility) of 5 October 2010 and the judgement in López Ribalda and others v. Spain, from 9 January 2018. While in the ruling of inadmissibility in the Köpke case, suspicions were focused on only two workers and the recording lasted two weeks, in the conviction against Spain in the case of López Ribalda, suspicions were directed against all the staff and the recordings were kept for months.

[38] The ECHR has ruled on the extensive and exact information that must be provided to workers in the judgement Barbulescu v. Romania (Great Hall), of 5 September 2017 and, especially, against Spain in the Lopez Ribalda and others judgement, of 9 January 2018. In this judgement Spain was found guilty of the infringement of art. 8 of the ECHR after having accepted the dismissal of 5 supermarket workers for a number of thefts recorded by a video surveillance system, with some visible cameras and some hidden, but in relation to which they had only been informed of the visible cameras.

[39] In this sense, see FABREGAT MONFORT, G., "El control empresarial de los trabajadores a través de las nuevas tecnologías: algunas ideas clave" (Corporate Monitoring of Workers Using New Technologies: Some Key Ideas", Trabajo y Derecho, No. 5, May 2015. For the author "not having a clear idea of the aforementioned leads to confusion, because only from that perspective, from the purpose of the means used to monitor and the reason for its existence, and the differentiation between the measures taken as ordinary or extraordinary (i.e., to monitor someone), it is understood that neither the evidence obtained in the case prosecuted under the aforementioned STC 29/2013, of 11 February (LAW 11227/2013), of the University of Seville, nor that of the case which is the subject of the also mentioned STS of 13 May 2014, Rec. 1685/2013 (LAW 76886/2014) complies with the law, since in both cases the video camera, in theory, had been placed without the previous existence of indications or suspicions of a prior non-compliance". Op cit., p. 7.

[40] I had the opportunity to examine the different treatment that certain technological evidence is receiving in criminal and social cases in "The Probative Value of Emails", in *Justicia penal y nuevas formas de delincuencia* (C*riminal Justice and New Forms of Crime)* (ASENCIO MELLADO and FERNÁNDEZ LÓPEZ, Coords.), Tirant lo Blanch, Valencia, 2017, pp. 199-200.

had shown the commissioning of a criminal act (e.g., drug trafficking or theft of computer equipment)? Its foreseeable admission as evidence in criminal proceedings collides head-on – and is very difficult to justify – with its impossibility of use in employment proceedings. And giving a further turn to this argument, we would find that the recording that did not serve to impose a disciplinary action on the worker, would in fact serve to convict him for theft, and once convicted for theft from the company, his disciplinary dismissal would then be justified. This obliges the defendant to undertake long and costly procedural paths to reach, in the end, the initial starting point: the adoption of disciplinary measures from the evidence of the commissioning of a crime evidenced by a recording.

A similar extrapolation could be made in the course of the facts referred to in the STS of 13 May 2014[41] that did not take video evidence into account to justify the dismissal of the cashier at a supermarket, recording the theft committed by not scanning the products that her boyfriend passed her, based on the reasoning that the camera had been installed for reasons of security against possible theft by third parties and not to monitor ordinary compliance with work activity. The possibility that this specific recording would not be taken into account for the purposes of a plausible criminal conviction in a prosecution for theft cannot, however, seem to be reasonably upheld.

The enshrining of this different evidentiary treatment under criminal and employment law has become evident in several different and increasingly numerous judgements, as in the case of those of 26 September 2007; 8 March 2011; 6 October 2011; or 16 June 2014, all of the TS; and the STC of 17 December 2012; of 7 October 2013.

It is therefore urgent to clarify the scope of the protection of fundamental rights and the role that art. 11.1 LOPJ and the theory of prohibited evidence are called upon to play in proceedings. Or, put another way, whether the prohibition on the use in proceedings of evidence obtained through the violation of fundamental rights is intended to safeguard the essential purposes of the same (including the aim that the solution reached has not been achieved through the violation of fundamental rights), or to determine the extent and scope of indemnity for each specific fundamental right.

The first of the options, in my view desirable, finds the reasoning for the exclusionary rule in the need to ensure behaviour in accordance with the law on the part of the agents of the state – the police – responsible for the criminal investigation[42]. In this way, the purpose of the exclusionary rule acquires a prophylactic or deterrent effect: it is absurd to obtain certain evidentiary information in violation of fundamental rights, since this cannot be used in legal proceedings.

This origin connected to the need to ensure correct state action in criminal investigation, does not preclude the application of art. 11.1 LOPJ to evidence obtained illegally by individuals, although it is true that it influences its application by requiring, for it to be declared null and void, that the individual had obtained the evidence with the intention of providing it in the proceedings[43].

[41] Rec. 1685/2013.

[42] This reasoning for the exclusionary rule has been expressly and constantly defended by the US Supreme Court since 1976 (Case *Stone v. Powell*).

[43] See STC 114/1984, of 29 November; 56/2003, of 29 March; or ATC (Decision of the TC) 115/2008, of 28 April. Also, along the same lines, VELASCO NUNEZ goes deeper when he claims that "We disagree with the Barcelona SAP (Court of Appeals) 20 October 2012 that decreed that the evidence was inadmissible when the complainant provided DVDs with pictures of non-consensual sexual abuse of her sister-in-law, since they had been stolen from the car of the alleged perpetrator where they had been concealed, alleging that this violated his right to privacy, "contaminating" the derived evidence. What is essential between individuals is the good or bad faith of whoever provides the evidence since, rather than considering an illegal and prohibited object – such as an illegal film – as property, and since in cases such as this the motives of profit and *rem sibi habendi* are excluded, it should be considered that its contribution to a criminal proceedings – through the police or directly to the Judge – is more constitutive of an act of a citizen who is collaborating and reporting, especially if the offence is serious, than an arbitrary act at the hands of the justice system, because in the

It is my understanding that, if this interpretive approach were to be applied to the evidence provided by an employer who, within the margin of monitoring allowed by art. 20 ET, has proceeded to install cameras for video recording, there would be fewer areas of conflict between criminal and social jurisdiction and it would contribute to the formation of a coherent thesis around the limitability of fundamental rights.

In this way, any evidence found "by chance" (or "in good faith") by an employer who installed video surveillance cameras for the ordinary monitoring of compliance in workplace relations, in accordance with the requirements of the regulations in force, should be perfectly admissible and, consequently, should be able to uphold a conviction or sanctions according to the case.

This is based on the argument that, in the first place, it is evidence obtained by an individual – however much the employer/employee relationship is not ruled by the equality of position normally present in this type of relationship; and, secondly, it is evidence obtained "by chance" (or "in good faith"), in the sense that the purpose of the recording was not to obtain evidentiary sources for court proceedings. In this regard, it should be recalled that the obligation to inform workers about the recordings is the responsibility of the employer

This interpretation would allow us to evaluate the evidence referred to earlier – rejected by the TS – of the cashier in the supermarket who passed items without scanning them, handing them to her boyfriend (STS of 13 May 2014), and that of the theft carried out by a worker in an office that had likewise had a video surveillance camera installed (STS 239/2014, of 1 April)[44]. Acceptance of this theory could result in acceptance of the evaluation of evidence in both social and criminal proceedings, with the consequent unification of doctrine on the interpretation of prohibited evidence.

4. International Data Transfers: International Flow of Data *vs.* Protection of the Owner of the Data

4.1. Technological advances – in particular, the development of the Internet – greatly facilitate the processing and exchange of information, allowing us to share technological resources, centralise certain activities and processes, and lower costs involved in the delivery of services by companies, outside of the country in which they are based. These advances mean personal data, always of interest and useful for the development of any large scale activity, can today circulate internationally very quickly and be stored indefinitely.

International transfers of personal data, in areas such as human resources, financial services, education, e-commerce and research in the area of health, have become an integral and integrating part of the globalised economy. Indeed, the international flow of personal data is not only an auxiliary industry with regard to companies, institutions and people engaged in performing or using bank transfers, reservations of airline tickets or international legal assistance, but is a growing economic sector in itself.

It is undeniable that the qualitative and quantitative transformation in the international flows of personal data has increased the efficiency of companies and has contributed to the development of the Information Society and the globalisation of economic activity. But such contributions have not come without costs, since the privacy of the owner of such data has been put in jeopardy. It is also clear that, without too much technical difficulty, information can be the subject of unlawful processing; in other words, an international transfer of personal data without the consent of the person concerned, concluding in a violation of their fundamental, constitutionally protected rights.

The purpose of data protection is to provide the owner of the data with adequate and effective defence mechanisms against the unlawful acquisition or processing of personal information. This is achieved

end the purpose of the photos is that they serve as evidence." VELASCO NÚÑEZ, E., "Derecho a la imagen: tratamiento procesal penal" (Rights to the Image: Criminal Procedural Treatment), Diario La Ley, Nº 8595, 1 September de 2015, Ref. D-311.

[44] In this respect, the individual opinions issued by the Judge Antonio del Moral García in response to STS 569/2013, of 26 June and 239/2014, of 1 April are particularly eloquent.

through a balancing act involving the allocation of rights to the owner of the data and the imposition of obligations on those that capture or process the data, and/or exercise control over its processing. Finding solutions that satisfy the legitimate interests of all parties involved in international data transfers is not easy, particularly due to the clear differences existing between the different levels of protection of the rights and freedoms of individuals and their privacy.

The differences found in the protection provided by the relevant provisions of the various regulations are susceptible to both hindering the free transfer of data and to circumventing its correct handling: if the processing regime is more burdensome in one country than in another, this may encourage the development of business strategies or a change in location in an attempt to avoid the application of high standards of protection.

The undeniable international nature of the relationships involved in a transfer of personal data creates a fertile ground for the emergence of problems that are the subject of study on the part of private international law. On the one hand, the vast majority of personal data processing operations are *presupposed to have cross-border implications*. For example, those relating to the provision of processing services that businesses agree between each other – already involving the assignment or communication of data between those responsible, or access to them by a manager or delegated person – where there is a presence of one or more foreign elements, can become *international*. This would be the case where the professionals involved are located in different states, either because the data itself moves from one state to another, or from a protected territory to a third state. On the other hand, beyond the undeniable multidisciplinary nature of the issue, international transfers of data are susceptible to causing multiple *private* legal relationships, both contractual and extra-contractual.

The potential plurality of legal systems involved in the safeguarding of the correct international movement of personal data and the existence of international transfers of such data, a result of the increasing international nature of personal and commercial relationship, requires the intervention of private international law – but not just any intervention. Rather it is necessary to explore the virtues of the system when dealing with a specific legal problem in order to achieve proper, balanced and effective safeguards for anyone harmed by the unlawful processing of personal data, derived from an international transfer.

And all this must be done within a new normative context: Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 relating to the protection of individuals with regard to the processing of personal data and on the free movement of such data, which repeals Directive 95/46/EC (General Rules of Data Protection).

4.2. The proliferation of state courts with jurisdiction in cases involving a multitude of countries hinders the much-needed legal security in international private traffic and means that the harmful effects of a wrongful act may emerge in every country in the world from where it is possible to access the injurious information (the personal data of the affected party). The plurality of judicial forums that are provided by different regimes of international jurisdiction favours so-called *forum shopping* on the part of the subject affected, who may choose to file a lawsuit before those courts whose rules of conflict apply a law that provides for a regime of non-contractual liability that is more favourable to their own interests.

The current rules of international jurisdiction are not only clearly inadequate to protect the victim of the unlawful international processing of their data, but they can even lead to counterproductive results. Firstly, the judicial remedy of free will is dangerous in a situation involving imbalance between the parties, as evidenced by the existence of forums for protection under the various systems of private international law. The possibility of an implied jurisdiction is difficult to verify in practice: firstly, because the victim will have a logical tendency to sue in the courts of their place of residence; secondly, because it seems clear

that the causer of the damage, rather than submit to such courts, would challenge their jurisdiction, to avoid being tried by the courts of the counterparty.

As to the determination of applicable law, insofar as Article 1.2.g of the current "Rome II" Regulation establishes that "this Regulation will exclude from the scope of application, the area of: [...] *g)* non-contractual obligations arising out of the breach of privacy or rights related to the personality; in particular, defamation", the solution will involve resorting to article 10.9 of Spain's Civil Code, which takes *locus delicti commissi* as its point of connection*;* that is to say, the application of "the law of the place where the delict [tort] was committed" *(lex loci delicti commissi)*, which could mean a choice between the law of the place where the personal data was collected or that of the state where such personal information was processed, must be presided over by *favor laesi,* in order to guarantee that the injured party receives adequate, balanced and effective protection.

Reference

1. Strahilevitz, Lior Jacob (2010). "Toward a positive theory of privacy law", *Harvard Law Review*, vol. 126, pp. 2010-2042, at 2021.

2. Toscano, Manuel (2017), "Sobre el concepto de privacidad: la relación entre privacidad e intimidad", *Isegoría. Revista de Filosofía Moral y Política*, nº 57, pp. 533-552, at 544.

3. Garzón Valdés, Ernesto (2003), "Lo íntimo, lo privado y lo público", *Claves de Razón Práctica*, nº 137, pp. 14-24

4. Castilla del Pino, Carlos (1989), "Público, privado, íntimo", en Castilla del Pino (ed.), *De la intimidad*. Barcelona: Crítica, pp. 25-31.

5. Béjar, Helena (1988), *El ámbito íntimo. Privacidad, individualismo y modernidad*. Madrid: Alianza.

6. Garzón Valdés, E., "Lo íntimo, lo privado y lo público", *cit.*, p. 16.

7. Nagel, Thomas (1998), "Concealment and Exposure", *Philosophy & Public Affairs*", vol. 27 nº 1, pp 3-30, at 4-5.

8. Magi, Trina J. (2011). "Fourteen Reasons Privacy Matters: A Multidisciplinary Review of Scholarly Literature", *The Library Quarterly*, vol. 81, nº 2, pp. 187-209, at 195.

9. Nagel, T., "Concealment and Exposure", *cit.*, p. 20; Reiman, Jeffrey (1995), "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future", Santa Clara Computer & High Technology Law Journal, vol. 11, pp. 27-44, at 41. Nagel, T., "Concealment and Exposure", *cit.*, p. 20.

10. Pérez Luño, Antonio (2012), *Los derechos humanos en la sociedad tecnológica*, Madrid: Editorial Universitas, p. 92.

11. Rachels, James (1975). "Why Privacy is Important?", *Philosophy & Public Affairs*, vol. 4, nº 4, pp. 323-333, at 328.

12. Reiman, Jeffrey (1976), "Privacy, Intimacy, and Personhood", *Philosophy & Public Affairs*, vol. 6, nº 1, pp. 26-44, at 33-34

13. Innes, Julie (1992), *Privacy, Intimacy and Isolation*. New York: Oxford University Press.

14. Nissenbaum, Helen (2004). "Privacy as Contextual Integrity", *Washington Law Review*, 79 (1), pp. 101-139

15. Hoven, Jeroen van den (2004). "Privacy and the Varieties of Informational Wrongdoing", en Richard A. Spinello & Herman T. Tavani (eds.), *Readings in Cyber Ethics*, Jones & Bartlett Publishers, 2ª edn., pp. 489-500, at 491 ff.

16. Mayer-Schönberger, Viktor and Cukier, Kenneth (2013), *Big Data. A Revolution that Will Transform How we Live, Work, and Think*. New York: Houghton Mifflin Harcourt, p. 153.

17. Solove, Daniel (2004). *The Digital Person: Technology and Privacy in the Information Age*, New York: New York University Press.

18. Reiman, J., "Driving to the Panopticon", *cit.*, p. 29.

19. Garriga, Ana (2018), "La elaboración de perfiles y su impacto en los derechos fundamentales. Una primera aproximación a su regulación en el Reglamento General de Protección de Datos de la Unión Europea", *Derechos y libertades*, nº 38, pp. 107-139, at 138.

20. Gandy, Oscar (1993). *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview.

21. Lyon, David (2007), *Surveillance Studies. An Overview*, Cambridge: Polity Press, p. 184-185.

22. Bauman, Zygmunt (2000), *Liquid Modernity*, Cambridge: Polity Press, p. 86.

23. Solove, (2013). "Privacy Self-Management and the Consent Dilemma", *Harvard Law Review*, 126, pp. 1880-1903.

24. Regan, Priscilla (2002). "Privacy as a Common Good in the Digital World", *Information, Communication & Society*, vol. 5, nº 3, pp.382-405, at 395.

25. Allen, Anita (2011). *Unpopular privacy: What must we hide?*. Nueva York: Oxford University Press.

26. Wacks, Raymond (2010). "Should the Concept of Privacy be Abandoned?", *Law, Morality, and the Private Domain*. Hong Kong: Hong Kong University Press, pp. 235-248.

27. This paper is part of the research project "The Digital Era: New Problems for the Law" (AICO/2107/161) funded by the Generalitat Valenciana's Conselleria d'Educació, Cultura i Esport.

28. European Securities and Markets Authority, Questions and Answers, On the MiFID II and MiFIR investor protection and intermediaries topics, p. 38. Accessible at https://www.esma.europa.eu/system/files_force/library/esma3543349_mifid_ii_qas_on_investor_protection_topics.pdf June 2018 (8).

29. MARCHENA GÓMEZ, M., La Reforma de la Ley de Enjuiciamiento Criminal en 2015 (The Reform of the Criminal Procedure Act in 2015), Castillo de Luna Ediciones Jurídicas, Madrid, 2015, p. 288.

30. European Securities and Markets Authority, Questions and Answers, On the MiFID II and MiFIR investor protection and intermediaries topics, p. 41. Accessible at https://www.esma.europa.eu/system/files_force/library/esma3543349_mifid_ii_qas_on_investor_protection_topics.pdf (8 June 2018).

31. European Securities and Markets Authority, Questions and Answers, On the MiFID II and MiFIR investor protection and intermediaries topics, p. 39. Accessible at https://www.esma.europa.eu/system/files_force/library/esma3543349_mifid_ii_qas_on_investor_protection_topics.pdf (8 June 2018).

32. Strahilevitz, Lior Jacob (2010). "Toward a positive theory of privacy law", *Harvard Law Review*, vol. 126, pp. 2010-2042, at 2021.

33. Toscano, Manuel (2017), "Sobre el concepto de privacidad: la relación entre privacidad e intimidad", *Isegoría. Revista de Filosofía Moral y Política*, nº 57, pp. 533-552, at 544.

34. Garzón Valdés, Ernesto (2003), "Lo íntimo, lo privado y lo público", *Claves de Razón Práctica*, nº 137, pp. 14-24.

35. Castilla del Pino, Carlos (1989), "Público, privado, íntimo", en Castilla del Pino (ed.), *De la intimidad*. Barcelona: Crítica, pp. 25-31.

36. Béjar, Helena (1988), *El ámbito íntimo. Privacidad, individualismo y modernidad*. Madrid: Alianza.

37. Garzón Valdés, E., "Lo íntimo, lo privado y lo público", *cit.*, p. 16.

38. Nagel, Thomas (1998), "Concealment and Exposure", *Philosophy & Public Affairs*", vol. 27 nº 1, pp 3-30, at 4-5.

39. Magi, Trina J. (2011). "Fourteen Reasons Privacy Matters: A Multidisciplinary Review of Scholarly Literature", *The Library Quarterly*, vol. 81, nº 2, pp. 187-209, at 195.

40. Nagel, T., "Concealment and Exposure", *cit.*, p. 20; Reiman, Jeffrey (1995), "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future", Santa Clara Computer & High Technology Law Journal, vol. 11, pp. 27-44, at 41.

41. Nagel, T., "Concealment and Exposure", *cit.*, p. 20.

42. Pérez Luño, Antonio (2012), *Los derechos humanos en la sociedad tecnológica*, Madrid: Editorial Universitas, p. 92.

43. Rachels, James (1975). "Why Privacy is Important?", *Philosophy & Public Affairs*, vol. 4, nº 4, pp. 323-333, at 328.

44. Reiman, Jeffrey (1976), "Privacy, Intimacy, and Personhood", *Philosophy & Public Affairs*, vol. 6, nº 1, pp. 26-44, at 33-34

45. Innes, Julie (1992), *Privacy, Intimacy and Isolation*. New York: Oxford University Press.

46. Nissenbaum, Helen (2004). "Privacy as Contextual Integrity", *Washington Law Review*, 79 (1), pp. 101-139

47. Hoven, Jeroen van den (2004). "Privacy and the Varieties of Informational Wrongdoing", en Richard A. Spinello & Herman T. Tavani (eds.), *Readings in Cyber Ethics*, Jones & Bartlett Publishers, 2ª edn., pp. 489-500, at 491 ff.

48. Mayer-Schönberger, Viktor and Cukier, Kenneth (2013), *Big Data. A Revolution that Will Transform How we Live, Work, and Think*. New York: Houghton Mifflin Harcourt, p. 153.

49. Solove, Daniel (2004). *The Digital Person: Technology and Privacy in the Information Age*, New York: New York University Press.

50. Reiman, J., "Driving to the Panopticon", *cit.*, p. 29.

51. Garriga, Ana (2018), "La elaboración de perfiles y su impacto en los derechos fundamentales. Una primera aproximación a su regulación en el Reglamento General de Protección de Datos de la Unión Europea", *Derechos y libertades*, nº 38, pp. 107-139, at 138.

52. Gandy, Oscar (1993). *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview.

53. Lyon, David (2007), *Surveillance Studies. An Overview*, Cambridge: Polity Press, p. 184-185.

54. Bauman, Zygmunt (2000), *Liquid Modernity*, Cambridge: Polity Press, p. 86.

55. Solove, (2013). "Privacy Self-Management and the Consent Dilemma", *Harvard Law Review*, 126, pp. 1880-1903.

56. Regan, Priscilla (2002). "Privacy as a Common Good in the Digital World", *Information, Communication & Society*, vol. 5, nº 3, pp.382-405, at 395.

57. Allen, Anita (2011). *Unpopular privacy: What must we hide?*. Nueva York: Oxford University Press.

58. Wacks, Raymond (2010). "Should the Concept of Privacy be Abandoned?", *Law, Morality, and the Private Domain*. Hong Kong: Hong Kong University Press, pp. 235-248.

59. This paper is part of the research project "The Digital Era: New Problems for the Law" (AICO/2107/161) funded by the Generalitat Valenciana's Conselleria d'Educació, Cultura i Esport.

60. European Securities and Markets Authority, Questions and Answers, On the MiFID II and MiFIR investor protection and intermediaries topics, p. 38. Accessible at https://www.esma.europa.eu/system/files_force/library/esma3543349_mifid_ii_qas_on_investor_protection_topics.pdf June 2018 (8).

61. MARCHENA GÓMEZ, M., La Reforma de la Ley de Enjuiciamiento Criminal en 2015 (The Reform of the Criminal Procedure Act in 2015), Castillo de Luna Ediciones Jurídicas, Madrid, 2015, p. 288.

62. European Securities and Markets Authority, Questions and Answers, On the MiFID II and MiFIR investor protection and intermediaries topics, p. 41. Accessible at

https://www.esma.europa.eu/system/files_force/library/esma3543349_mifid_ii_qas_on_investor_protection_topics.pdf (8 June 2018).

63. European Securities and Markets Authority, Questions and Answers, On the MiFID II and MiFIR investor protection and intermediaries topics, p. 39. Accessible at https://www.esma.europa.eu/system/files_force/library/esma3543349_mifid_ii_qas_on_investor_protection_topics.pdf (8 June 2018).

64. This paper is part of the research project "The Digital Era: New Problems for the Law" (AICO/2107/161) funded by the Generalitat Valenciana's Conselleria d'Educació, Cultura i Esport.

65. SSC 239/2014, of 1 April uses terminology imported from that used by the European Court of Human Rights (ECHR) to pronounce on the difference between recording in open spaces, such as those where cash registers are found, and recording in an office, based on the "reasonable expectation of privacy" stating that: "the recording cameras were installed in at least two different places. In one area was the cash register, where the money was taken. The substance of the judgement is that all workers or, at least, most of them, had access to this location (...). It cannot be claimed that there is a reasonable expectation of privacy in a place of common access for the performance of the functions that each worker is assigned by the company within the employment relationship. In that case, the company's power to manage and its related powers, does not impinge on the right to privacy of the workers when placing recording cameras in public areas with widespread access in which the general working activity of the company is performed. This is not the case with the cameras that were installed in the office of the defendant. (...) In principle, a single office is a room allocated to a particular person, and consent is required before facilitating the visual or personal access of third parties to the same. Therefore, in general terms, it can be said that the holder of the same has a reasonable expectation of privacy within his or her office, which may be violated if recording cameras are installed without their knowledge."

66. STS (Sentence of the Supreme Court) 620/1997, of 5 May.

67. See STC of 3 March 2016, as well as the more restrictive interpretation, on the need to inform the worker, which is contained in the individual opinions. With regard to developments in doctrine and jurisprudence that have led to the view of recordings as attacking the right to the protection of personal data and not, strictly speaking, against the right to privacy; as well as on employment and administrative demands to ensure that the recording of the work activity for the purpose of monitoring by the employer is not considered an attack on the fundamental rights of the worker, see ARRABAL PLATERO, P., "La videovigilancia laboral como prueba en el proceso" (Labour Video Surveillance as Evidence in the Judicial Process) Revista General de Derecho Procesal, Iustel, September-October 2015, www.iustel.com.

68. Regarding the suspicion of the employer in regard to the unlawful activity of the worker, two interesting rulings of the ECHR should be noted: the case of Köpke against Germany (ruling of inadmissibility) of 5 October 2010 and the judgement in López Ribalda and others v. Spain, from 9 January 2018. While in the ruling of inadmissibility in the Köpke case, suspicions were focused on only two workers and the recording lasted two weeks, in the conviction against Spain in the case of López Ribalda, suspicions were directed against all the staff and the recordings were kept for months.

69. The ECHR has ruled on the extensive and exact information that must be provided to workers in the judgement Barbulescu v. Romania (Great Hall), of 5 September 2017 and, especially, against Spain in the Lopez Ribalda and others judgement, of 9 January 2018. In this judgement Spain was found guilty of the infringement of art. 8 of the ECHR after having accepted the dismissal of 5 supermarket workers

for a number of thefts recorded by a video surveillance system, with some visible cameras and some hidden, but in relation to which they had only been informed of the visible cameras.

70. In this sense, see FABREGAT MONFORT, G., "El control empresarial de los trabajadores a través de las nuevas tecnologías: algunas ideas clave" (Corporate Monitoring of Workers Using New Technologies: Some Key Ideas", Trabajo y Derecho, No. 5, May 2015. For the author "not having a clear idea of the aforementioned leads to confusion, because only from that perspective, from the purpose of the means used to monitor and the reason for its existence, and the differentiation between the measures taken as ordinary or extraordinary (i.e., to monitor someone), it is understood that neither the evidence obtained in the case prosecuted under the aforementioned STC 29/2013, of 11 February (LAW 11227/2013), of the University of Seville, nor that of the case which is the subject of the also mentioned STS of 13 May 2014, Rec. 1685/2013 (LAW 76886/2014) complies with the law, since in both cases the video camera, in theory, had been placed without the previous existence of indications or suspicions of a prior non-compliance". Op cit., p. 7.

71. I had the opportunity to examine the different treatment that certain technological evidence is receiving in criminal and social cases in "The Probative Value of Emails", in *Justicia penal y nuevas formas de delincuencia* (*Criminal Justice and New Forms of Crime)* (ASENCIO MELLADO and FERNÁNDEZ LÓPEZ, Coords.), Tirant lo Blanch, Valencia, 2017, pp. 199-200. Rec. 1685/2013.

72. This reasoning for the exclusionary rule has been expressly and constantly defended by the US Supreme Court since 1976 (Case *Stone v. Powell*).

73. See STC 114/1984, of 29 November; 56/2003, of 29 March; or ATC (Decision of the TC) 115/2008, of 28 April. Also, along the same lines, VELASCO NUNEZ goes deeper when he claims that "We disagree with the Barcelona SAP (Court of Appeals) 20 October 2012 that decreed that the evidence was inadmissible when the complainant provided DVDs with pictures of non-consensual sexual abuse of her sister-in-law, since they had been stolen from the car of the alleged perpetrator where they had been concealed, alleging that this violated his right to privacy, "contaminating" the derived evidence. What is essential between individuals is the good or bad faith of whoever provides the evidence since, rather than considering an illegal and prohibited object – such as an illegal film – as property, and since in cases such as this the motives of profit and *rem sibi habendi* are excluded, it should be considered that its contribution to a criminal proceedings – through the police or directly to the Judge – is more constitutive of an act of a citizen who is collaborating and reporting, especially if the offence is serious, than an arbitrary act at the hands of the justice system, because in the end the purpose of the photos is that they serve as evidence." VELASCO NÚÑEZ, E., "Derecho a la imagen: tratamiento procesal penal" (Rights to the Image: Criminal Procedural Treatment), Diario La Ley, Nº 8595, 1 September de 2015, Ref. D-311.

74. In this respect, the individual opinions issued by the Judge Antonio del Moral García in response to STS 569/2013, of 26 June and 239/2014, of 1 April are particularly eloquent.

75. the judgement is that all workers or, at least, most of them, had access to this location (...). It cannot be claimed that there is a reasonable expectation of privacy in a place of common access for the performance of the functions that each worker is assigned by the company within the employment relationship. In that case, the company's power to manage and its related powers, does not impinge on the right to privacy of the workers when placing recording cameras in public areas with widespread access in which the general working activity of the company is performed. This is not the case with the cameras that were installed in the office of the defendant. (...) In principle, a single office is a room allocated to a particular person, and consent is required before facilitating the visual or personal access of third parties to the same. Therefore, in general terms, it can be said that the holder of the same has

a reasonable expectation of privacy within his or her office, which may be violated if recording cameras are installed without their knowledge." STS (Sentence of the Supreme Court) 620/1997, of 5 May.

76. See STC of 3 March 2016, as well as the more restrictive interpretation, on the need to inform the worker, which is contained in the individual opinions. With regard to developments in doctrine and jurisprudence that have led to the view of recordings as attacking the right to the protection of personal data and not, strictly speaking, against the right to privacy; as well as on employment and administrative demands to ensure that the recording of the work activity for the purpose of monitoring by the employer is not considered an attack on the fundamental rights of the worker, see ARRABAL PLATERO, P., "La videovigilancia laboral como prueba en el proceso" (Labour Video Surveillance as Evidence in the Judicial Process) Revista General de Derecho Procesal, Iustel, September-October 2015, www.iustel.com.

77. Regarding the suspicion of the employer in regard to the unlawful activity of the worker, two interesting rulings of the ECHR should be noted: the case of Köpke against Germany (ruling of inadmissibility) of 5 October 2010 and the judgement in López Ribalda and others v. Spain, from 9 January 2018. While in the ruling of inadmissibility in the Köpke case, suspicions were focused on only two workers and the recording lasted two weeks, in the conviction against Spain in the case of López Ribalda, suspicions were directed against all the staff and the recordings were kept for months.

78. The ECHR has ruled on the extensive and exact information that must be provided to workers in the judgement Barbulescu v. Romania (Great Hall), of 5 September 2017 and, especially, against Spain in the Lopez Ribalda and others judgement, of 9 January 2018. In this judgement Spain was found guilty of the infringement of art. 8 of the ECHR after having accepted the dismissal of 5 supermarket workers for a number of thefts recorded by a video surveillance system, with some visible cameras and some hidden, but in relation to which they had only been informed of the visible cameras.

79. In this sense, see FABREGAT MONFORT, G., "El control empresarial de los trabajadores a través de las nuevas tecnologías: algunas ideas clave" (Corporate Monitoring of Workers Using New Technologies: Some Key Ideas", Trabajo y Derecho, No. 5, May 2015. For the author "not having a clear

80. Trabajo y Derecho, No. 5, May 2015. For the author "not having a clear idea of the aforementioned leads to confusion, because only from that perspective, from the purpose of the means used to monitor and the reason for its existence, and the differentiation between the measures taken as ordinary or extraordinary (i.e., to monitor someone), it is understood that neither the evidence obtained in the case prosecuted under the aforementioned STC 29/2013, of 11 February (LAW 11227/2013), of the University of Seville, nor that of the case which is the subject of the also mentioned STS of 13 May 2014, Rec. 1685/2013 (LAW 76886/2014) complies with the law, since in both cases the video camera, in theory, had been placed without the previous existence of indications or suspicions of a prior non-compliance". Op cit., p. 7.

81. I had the opportunity to examine the different treatment that certain technological evidence is receiving in criminal and social cases in "The Probative Value of Emails", in *Justicia penal y nuevas formas de delincuencia* (C*riminal Justice and New Forms of Crime)* (ASENCIO MELLADO and FERNÁNDEZ LÓPEZ, Coords.), Tirant lo Blanch, Valencia, 2017, pp. 199-200. Rec. 1685/2013

82. This reasoning for the exclusionary rule has been expressly and constantly defended by the US Supreme Court since 1976 (Case *Stone v. Powell*).

83. See STC 114/1984, of 29 November; 56/2003, of 29 March; or ATC (Decision of the TC) 115/2008, of 28 April. Also, along the same lines, VELASCO NUNEZ goes deeper when he claims that "We disagree with

the Barcelona SAP (Court of Appeals) 20 October 2012 that decreed that the evidence was inadmissible when the complainant provided DVDs with pictures of non-consensual sexual abuse of her sister-in-law, since they had been stolen from the car of the alleged perpetrator where they had been concealed, alleging that this violated his right to privacy, "contaminating" the derived evidence. What is essential between individuals is the good or bad faith of whoever provides the evidence since, rather than considering an illegal and prohibited object – such as an illegal film – as property, and since in cases such as this the motives of profit and *rem sibi habendi* are excluded, it should be considered that its contribution to a criminal proceedings – through the police or directly to the Judge – is more constitutive of an act of a citizen who is collaborating and reporting, especially if the offence is serious, than an arbitrary act at the hands of the justice system, because in the end the purpose of the photos is that they serve as evidence." VELASCO NÚÑEZ, E., "Derecho a la imagen: tratamiento procesal penal" (Rights to the Image: Criminal Procedural Treatment), Diario La Ley, Nº 8595, 1 September de 2015, Ref. D-311.

84. This reasoning for the exclusionary rule has been expressly and constantly defended by the US Supreme Court since 1976 (Case *Stone v. Powell*).

85. See STC 114/1984, of 29 November; 56/2003, of 29 March; or ATC (Decision of the TC) 115/2008, of 28 April. Also, along the same lines, VELASCO NUNEZ goes deeper when he claims that "We disagree with the Barcelona SAP (Court of Appeals) 20 October 2012 that decreed that the evidence was inadmissible when the complainant provided DVDs with pictures of non-consensual sexual abuse of her sister-in-law, since they had been stolen from the car of the alleged perpetrator where they had been concealed, alleging that this violated his right to privacy, "contaminating" the derived evidence. What is essential between individuals is the good or bad faith of whoever provides the evidence since, rather than considering an illegal and prohibited object – such as an illegal film – as property, and since in cases such as this the motives of profit and *rem sibi habendi* are excluded, it should be considered that its contribution to a criminal proceedings – through the police or directly to the Judge – is more constitutive of an act of a citizen who is collaborating and reporting, especially if the offence is serious, than an arbitrary act at the hands of the justice system, because in the end the purpose of the photos is that they serve as evidence." VELASCO NÚÑEZ, E., "Derecho a la imagen: tratamiento procesal penal" (Rights to the Image: Criminal Procedural Treatment), Diario La Ley, Nº 8595, 1 September de 2015, Ref. D-311.