SUMMARY 2022 | INTERNAL INVESTIGATIONS

MOLINS

Defensa Penal

TABLE OF CONTENTS

INTRODUCTION 4

1. **INTERNATIONAL COMUNITY** 6

International Organization for Standardization 6

- Draft ISO 37008 - Guidance for the conduct of internal investigations. 6

U.S. Securities and Exchange Commission 6

- Million-dollar penalties from the SEC for the systematic use of informal 6

communication channels for professional purposes (*Whatsapp*, e.g.). 6

2. **EUROPE** 7

Court of Justice of the European Union 7

European Commission: standard contractual clauses on the international transfer of personal data. 9

European Data Protection Board: the first certification system under the GDPR approved by the EDPS is born. 9

Member States with transposed Directive (EU) 2019/1937 10

3. **SPAIN** 13

Legislation 13

Jurisprudence 14

Constitutional Court Ruling No. 42/2022, OMNIUM CULTURAL case. 16

Subject matter: sanctions for international transmission of personal data. 16

Judgment of the **Supreme Court (Plenary of the Labor Chamber)** no. 692/2022, of July 22, p. García-Perrote Escartín. 17

Subject matter: evidentiary validity of a hidden camera installed by the employe. 17

Judgment of the **Supreme Court (Criminal Division)** no. 132/2022, of January 24, p. Hernández García. 18

Subject matter: evidentiary validity of the evidence obtained through the registration of corporate e-mail. 18

Ruling of the **Superior Court of Justice of Madrid** No. 671/2022, of September 23, p. Moreno González-Aller: 19

Subject matter: evidentiary validity of the recording of a telephone conversation between two workers obtained by the employer. 19

Judgment of the **Superior Court of Justice of Catalonia** no. 5693/2022, of October 28, p. Bono Romera: 19

Subject matter: validity of the evidence obtained by the employer from the employee's social networks..... 19

State Attorney General's Office..... 20

INTRODUCTION

Except in the USA, **the conduct of internal corporate investigations is not an established or recurrent practice in most of the world's legal systems**. Its relevance in the legal-economic scene is usually in the wake of the existence and degree of implementation of criminal liability regimes for legal persons in the corresponding countries. Since the criminal prosecution of companies and other organizations is a new political-criminal trend at the international level as well, it is not surprising that the proliferation of this type of investigation is still in its infancy.

Nevertheless, the year 2022 has borne some significant fruit in this maturation process. At the international level, the draft Guide for the Conduct of Internal Investigations developed by the *International Organization for Standardization* (ISO/DTS 37008 project) is noteworthy.

In Europe, the past year has been marked by the end of the deadline given to European Union Member States to implement Directive (EU) 2019/1937 of 23 October on the protection of persons who report breaches of Union law. States had until December 17, 2021 to adopt the transposing legislation. The European mandate consists of imposing the duty to establish internal whistleblowing channels and whistleblower protection systems against possible retaliation on public sector entities and private sector entities with more than 250 employees. Smaller entities with less than 250 employees, but with more than 50 employees, are also targeted, but for them the implementation deadline is extended to December 17, 2023.

As of today, the deadline has not been observed by a significant number of States, including Germany, Italy, Austria, Poland and Spain. Among those that can boast the most punctuality are France and Portugal.

From the old continent it is also worth mentioning the end of the deadline for adapting to the Commission Decision on standard clauses on international data transfer, a sensitive issue in any cross-border investigation, as well as the first certification system approved by the European Data Protection Committee with respect to the measures required by the GDPR. At the jurisdictional level, mention should be made of the Judgment of the Grand Chamber of the Court of Justice of the European Union on the scope of the duty of professional secrecy of lawyers, following the obligations of communication of information to the authorities on risky tax transactions imposed by the DAC 6 (Directive

aimed at preventing tax fraud). The preservation of the results of investigations from being requested or seized by the public authorities depends, among other things, on the scope conferred on the duty of professional secrecy, so that the position adopted by the Grand Chamber of the CJEU on this right/duty, albeit in other areas, is necessarily of interest.

As far as Spain is concerned, apart from the approval of the draft law on the protection of whistleblowers, several rulings of our Courts on the validity of sources of evidence obtained by means of image and/or voice recording systems, or by means of computer and/or telecommunication equipment records stand out. Among them is a ruling handed down by the Plenary of the Constitutional Court, which was divided into two opposing blocks as a result of the problem being judged: the scope of the duty to specifically inform workers of the existence of a video-surveillance system. The ruling has five dissenting votes out of the eleven issued. There is also a judgment of the Plenary of the Social Chamber of the Supreme Court, on the same issue. In this case, the ruling was unanimous. The fact that in a single year there were two plenary rulings and one with the dissenting vote of half but one of the members of the Court shows that the issue in question is both relevant and controversial.

With the expected approval of the national regulations on whistleblower protection in the member states that have not yet transposed Directive 2019/1937, including Spain, and with the probable publication of ISO 37008, on the conduct of internal investigations, it can be expected that in 2023 there will be firm and important steps forward in the progressive standardization of internal corporate investigations. We look forward to this.

In Barcelona, February 6th, 2023.

Internal Investigations Team
Molins Defensa Penal

1. INTERNATIONAL COMUNITY

From the past year 2022, at the international level, the draft guide on internal investigations of the *International Organization for Standardizaton* and the million-dollar sanction imposed by the SEC on 16 investment firms on the Wall Street stock exchange for the systematic use of informal messaging applications (*Whatsapp*, e.g.) for professional purposes stand out.

International Organization for Standardization

- Draft ISO 37008 - Guidance for the conduct of internal investigations.

The **ISO/DTS 37008** project, currently under development, consists of a guide on the conduct of internal investigations aimed at any type of organization, whether in the public, private or charitable sector (NGOs, foundations, associations, etc.)..

Its objective is to provide guidance to entities to better identify what has occurred, why it has occurred (root cause), as well as to decide who should conduct the investigation, how it should be conducted, what corrective actions to take, what and how to report, and how to prevent possible retaliation.

The draft guide is at an advanced stage in the processing process. It has passed the phases of proposal, preparation and study of the project in committee, as well as the consultation period. It is currently in the approval phase. Once validated, the next step will be its publication[1].

U.S. Securities and Exchange Commission

- Million-dollar penalties from the SEC for the systematic use of informal communication channels for professional purposes (*Whatsapp*, e.g.).

[1] Details of the procedure can be found at https://www.iso.org/stage-codes.html#50_00.

U.S. regulations governing the financial markets require investment entities authorized to trade on the Wall Street stock exchange to record and retain all communications made by their employees in the course of their business.

Following an investigation, the U.S. financial markets authority, the U.S. Securities and Exchange Commission (SEC), concluded that employees of sixteen of these companies, including senior executives, had been systematically using informal messaging applications (e.g. Whatsapp) for which the respective companies did not keep proper records of communications or perform the required oversight.

Sixteen entities accepted the alleged facts and reached an agreement with the regulator. Among them are Barclays Capital Inc, Merrill Lynch, Citigroup Global Markets Inc, Credit Suisse Securities (USA) LLC, Deutsche Bank Securities Inc, Goldman Sachs & Co LLC, Morgan Stanley & Co LLC and UBS Securities LLC. The fine imposed on each of these companies amounts to USD 125 million. The agreement reached includes the monitoring of the financial compliance process.

2. EUROPE

Court of Justice of the European Union

A few days before the end of the year 2022, the Judgment of the Full Court of the Court of Justice of the European Union was published in Case C-694/20, the subject matter of which was a preliminary ruling on the compatibility with the right to privacy (Art. 7 of the EU Charter of Fundamental Rights) of the obligations to disclose information to third parties imposed on lawyers by the CAD 6 Directive.

As part of the tax fraud prevention policies and measures adopted by the Union institutions, 2018 saw the adoption of Directive (EU) 2018/822, also known as DAC 6, which obliges Member States to establish certain reporting duties on lawyers who are in any way involved in the design, marketing, organization, making available for execution or management of the execution of a potentially aggressive cross-border tax planning scheme subject to reporting under the DAC regulations.

While the CAD regulations exempt intermediaries subject to the duty of professional secrecy from the obligation to inform the competent public authorities, Art. 8ab of the

CAD 6 obliges Member States to impose on such intermediaries, which include lawyers, the duty to inform other intermediaries involved in setting up or implementing the potentially aggressive tax planning scheme that, due to their duty of professional secrecy, they will not comply with the obligation of communication provided for in the CAD.

As the Court points out, this duty implies a double interference with the right to secrecy of communications between lawyer and client, contained in the right to privacy provided for in Art. 7 of the CDFUE. Firstly, the right is affected by the fact that the lawyer has to communicate to a third party the existence of the consultation or advice given to the client, his assessment that the same refers to a potentially aggressive tax planning mechanism, as well as his identity. The second, indirect, interference consists of the communication that the intermediary is obliged to make to the tax authorities about the identity of the lawyer who has informed of his dispensation, as well as the existence of the client's consultation.

Having established the existence of this double interference with the fundamental right, the Plenary of the CJEU examines whether the effect is justified. Applying the proportionality test, it concludes that, although the measure is suitable to maximize the prevention of tax fraud (a legitimate aim), it is unnecessary to ensure that the tax administrations are aware of the existence of a potentially aggressive cross-border tax planning mechanism. For both the other intermediaries and the client, when there are no intermediaries obliged to inform, have the duty to communicate the existence of the mechanism to the authorities. Therefore, the duty imposed on lawyers under CAD 6 is not essential for the tax administrations to be aware of the mechanism.

The Judgment resolves a question referred for a preliminary ruling by the Belgian Constitutional Court in relation to its legislation transposing the CAD 6. In Spain, the transposing legislation, consisting of Law 10/2020, of December 29, Royal Decree 243/2021, of April 6, and Order HAC/342/2021, of April 12, are being challenged before the Supreme Court and the Audiencia Nacional by the Spanish Association of Tax Advisors. As in Belgium, the aforementioned Spanish regulation imposed on lawyers the aforementioned duties of communication under threat of financial penalties, in faithful compliance with the European legislator. In the light of the CJEU Plenary Judgment, it is to be expected that this duty will be repealed.

The ruling is important in matters of internal investigations insofar as it is a reflection of the position of the full Court of Justice of the European Union in relation to the scope of

the duty of secrecy of communications between the lawyer and his client. This is a particularly sensitive issue in the area of internal investigations, where in light of U.S. praxis and the well-known 2018 German Constitutional Court Ruling flat the fear that the competent public authorities may require or seize the results of an internal investigation.

European Commission: *standard contractual clauses on the international transfer of personal data.*

On December 27, 2022, the transitional period for modifying the standard contractual clauses on the international transfer of personal data came to an end.

At present, the standard clauses provided for in **European Commission Decision 2021/914** must be used, at the risk of incurring penalties for non-compliance with the data protection regulations contained in or derived from the General Data Protection Regulation.

European Data Protection Board: the first certification system under the GDPR approved by the EDPS is born.

The competent authority for data protection in Luxembourg, the *Commission nationale pour la protection des données* (CNPD), has developed the first certification system under the General Data Protection Regulation (GDPR) approved by the European Data Protection Board (EDPB).

The ECDC is an independent European body that contributes to the consistent application of data protection rules throughout the European Union and promotes cooperation between national data protection authorities in the EU.

The certification system developed by the Luxembourg authority, called GDPR-CARPA, is based on an ISAE 3000 Type 2 report, which makes it possible to issue an

opinion on the correct implementation of the control mechanism with the assumption of formal responsibilities by the auditor.

Since it is a system developed and implemented by the Luxembourg data protection authority, only entities operating in Luxembourg are eligible for this certification.

However, it is a benchmark for the national authorities of the other European Union member states, which will surely follow in the footsteps of their Luxembourg counterpart.

Member States with transposed Directive (EU) 2019/1937

To date, sixteen (16) member states have already approved the national legislation transposing the *Whistleblowing Directive*, ten (10) have started the legislative process, without having approved the implementing legislation, and one (1) has not yet started the legislative process (Hungary)[2].

Unpunctual countries include Austria, Poland, Italy, Germany and Spain. The list of the most disciplined includes Denmark, Finland, Sweden, Belgium, Greece, Ireland, the Netherlands, France and Portugal.

The Directive obliges Member States to adopt the necessary national regulatory provisions to impose a duty on public sector entities and private sector entities with more than 50 employees to establish internal whistleblowing channels, as well as to adopt measures to protect whistleblowers against retaliation, in relation to certain breaches of EU law. This is without prejudice to the possibility for Member States to extend such duties to complaints about breaches of domestic, international or other law.

The European legislator requires that internal whistleblowing channels and protection measures are not only available to employees of the entities concerned, but also to former employees, persons close to the whistleblower or journalists.

A very important aspect of the Directive is that it obliges to provide protection to whistleblowers regardless of whether their first communication was not through the internal channel of the entity concerned. The European legislator requires that the whistleblower can choose between the internal whistleblowing system or the external whistleblowing system, consisting of the channels provided by the competent public authority. Public communication (through the media) must also be possible in the first instance, but in this case certain conditions must be met: either an attempt must have been made to exhaust the internal or institutional channels, or there must be a pressing public interest (art. 15).

[2] Véase la página web: https://www.whistleblowingmonitor.eu/.

Finally, Member States are ordered to impose effective, proportionate and dissuasive sanctions on natural or legal persons who: (i) make it difficult to lodge a complaint; (ii) retaliate against whistleblowers; (iii) fail to preserve the confidentiality of the whistleblower (Art. 23).

The following is a brief mention of the most noteworthy aspects of two of the Member States that have already complied with the transposition obligation. For reasons of geographical and commercial proximity, attention has been given to the regime adopted in France and Portugal.

- France:

Approved on March 21, 2022, Loi No. 2022-401, aimed at improving the protection of whistleblowers, also known as the "Waserman Act", came into force on September 1 for all entities, public or private, with more than 50 employees.

France already had a whistleblower protection regime in place prior to the adoption of Directive (EU) 2019/1937. These are the provisions contained in the "Sapin II Law" (Loi no. 2016-1691).

The new Law of 2022 has reformed in substantial aspects the regime provided for in the "Sapin II Law", in which the French legislator adopted a more balanced position between the interests of the whistleblower, those of the generality and those of the reported. In order to comply with the requirements of Directive (EU) 2019/1937, a model more focused on the interests of the whistleblower and those of the community is required. In this regard, Loi n.º 2022-401 has repealed the previous three-step protocol to be followed by the whistleblower: 1) first resort to the internal whistleblowing system of the entity; 2) Then, in the event that the internal whistleblowing was not properly handled, resort to the external institutional whistleblowing system; 3) as a last resort, proceed to the public dissemination of the fact. Now, after the reform, the whistleblower can freely choose between the internal or the external institutional whistleblower system. Public dissemination is also an option, but subject to further conditions. This is in accordance with the provisions of the Directive.

As regards the type of reportable offenses, the French legislator has extended the subject matter of complaints to: i) any crime or misdemeanor; ii) threats or damage to the general interest; violations or attempts to conceal violations of international commitments ratified or approved by France, or unilateral acts of an international

organization based on such commitments; iv) violations of European Union law or regulations.

Also of interest are the incentives provided in favor of whistleblowers. They are exempted from criminal liability for misappropriation, theft or concealment of documents related to the subject matter of the report to which they had legitimate access. They are also exempted from civil liability for any damage or harm that may have been caused by the report filed in good faith.

In terms of penalties, the French legislator has provided for a civil fine of €60,000 for dilatory or abusive actions by the entities concerned, aimed at hindering or concealing the report. Those who discriminate or retaliate against the whistleblower may be sentenced to 3 years' imprisonment and a fine of €45,000.

- Portugal:

In Portugal, the EU Directive regulating whistleblowing was transposed by Law No. 93/2021, on the general regime for the protection of whistleblowers. It came into force on June 18, 2022.

In Portugal there were already a good number of sectorial rules imposing on certain companies and entities the duty to have internal complaint channels and other measures provided for in the Directive. Law No. 92/2021 does not repeal such specific regimes, but acts as a general subsidiary rule.

As of June 2022 all public or private sector entities with more than 50 employees, as well as municipalities with more than 10,000 inhabitants, must have internal whistleblower channels.

Of note in the Portuguese regime is the prioritization of the whistleblower's available whistleblowing channels. The Portuguese legislator makes the protection measures conditional on the whistleblower having followed the following order: 1) first resort to the internal whistleblowing channel; 2) secondly resort to external institutional channels, if an adequate response has not been received internally; 3) as a last resort, public dissemination of the facts is allowed.

In terms of penalties, a distinction is made between very serious and serious offenses, as well as between offenses committed by legal entities and those attributable to individuals:

Very serious misconduct *Examples*: preventing the filing or follow-up of a complaint; retaliation; breach of the duty of confidentiality.	Individuals: 1.000 € a 25.000 € Legal entities: 10.000 € a 250.000 €
Serious misconduct *Examples*: failure to establish internal whistleblower channels; failure to comply with channel guarantees (independence, impartiality).	Individuals: 500 € a 12.500 € Legal entities: 1000 € a 25.000€

3. SPAIN

Legislation

On September 23, 2022, the **Draft Law on the Protection of Persons Reporting Regulatory Violations and the Fight against Corruption** was published, transposing Directive (EU) 2019/1937 on *Whistleblowing*.

The Spanish draft law extends the scope of application of the Directive. The infringements that may be reported through the reporting channels provided for in the draft law and that entitle the parties to the protective measures provided for therein are as follows:

- Infringements of European Union law provided for in Directive 2019/1937, infringements affecting the financial interests of the EU, as well as infringements having an impact on the internal market.
- Criminal offenses
- Serious or very serious administrative infractions.

In the subjective scope, internal reporting channels become mandatory for **private companies** with **more than 50 employees**. This includes political parties, trade unions and business organizations, as well as foundations created by them, provided they receive or manage public funds.
Likewise, the obligation is extended to all **public sector** entities, except for municipalities with less than 10,000 inhabitants or less than 50 employees.

The Bill requires companies to allow **anonymous communications** (art. 7.3). Complaints through external institutional channels may also be anonymous (art. 17.1).

The draft expressly states that **the internal channel** shall be the preferred channel (Art. 4.1). However, in the chapter regulating **external channels**, it is established that the informant may resort to it after exhausting the internal channel or directly. Unless the reference to the preferential nature of the internal channel is merely a declaration of intent without binding normative effects, we are faced with an obvious internal contradiction that should be resolved during the legislative processing of the draft, since it affects a fundamental aspect of the whistleblowing phenomenon. The Directive seems to require freedom of choice between the internal channel and the external institutional channel, as provided for in the French regulation, but it is true that countries such as Portugal establish a prioritization in favor of the internal system. We will see whether the compatibility of this second model with the Directive will be challenged before the CJEU in the near future.

A system of penalties is established which, in Article 63, classifies infringements as "very serious", "serious" or "minor". It should be noted that the **liable parties** may be both the entities (legal persons) and the individuals who are part of them, even after the employment or contractual relationship with the company concerned has ended (art. 62.3).
An example of a very serious infringement is the failure to comply with the obligation to have an internal information system, which may be subject to a fine of between 600,001 and **1,000,000** euros for legal entities and between 30,001 and 300,000 euros for individuals. In comparison with the sanctioning regimes in France and Portugal, the Spanish draft law is undoubtedly much more severe (see comment above).

Jurisprudence

Ruling of the **Constitutional Court** (Plenary) No. 119/2022, of September 29, p. Narváez Rodríguez.
Subject matter: evidentiary validity of images captured by video-surveillance system.

The Plenary Session of the Constitutional Court heard a petition for amparo filed by an employer who was denied as a valid source of evidence in a labor proceeding for disciplinary dismissal the recording obtained by his video-surveillance system of a certain action of the dismissed employee.

The images showed that the employee appropriated company property and subsequently sold it to third parties, keeping the money for himself. The inadmissibility

of the evidence led to the declaration of the dismissal as unfair, as the evidence was based on the video images.

The reason for the rejection by the High Court of Justice of the Basque Country was that the employer had not complied with its duty "to previously, expressly, clearly and concisely inform" the workers of the existence of the video-surveillance system and its use for the purpose of monitoring their work performance, a duty provided for by art. 89.1 of the Organic Law on Data Protection (hereinafter, LOPD).

The employer had complied with the general duty to inform of the existence of cameras by means of the visible sign approved by the Spanish Data Protection Agency (see art. 22.4 LOPD and Instruction no. 1/2006 of the AEPD). Therefore, the employer invoked the exception provided for in the second paragraph of art. 89.1 LOPD: "[i]n the event that the flagrant commission of an unlawful act by workers or public employees has been captured, the duty to inform shall be deemed to be fulfilled when there is at least the device referred to in article 22.4 of this organic law".

However, the Basque Country Supreme Court rejected its application because it was the second time that the plaintiff had used its video surveillance system to dismiss an employee. Five years earlier it had already resorted to it in a similar case. The Court understood the lack of regularization of the situation in relation to the duty to specifically inform the workers as "a unilateral interpretation of the exceptional power, attributing to itself means and powers that the legal system has only exceptionally provided for and that in no way serve to omit the duties that the company has with regard to fundamental rights".

The Plenary of the Constitutional Court upheld the employer's request for protection, annulling the Judgment of the Supreme Court of the Basque Country, on the grounds that the exception in the second paragraph of art. 89.1 LOPD was applicable, despite the employer's background. What is relevant, according to the majority of the Plenary, is that the employee has engaged in unlawful conduct and that the system has caught him

red-handed. The fact that the employer has had to resort to the video-surveillance system on previous occasions does not affect the only two relevant criteria: a) that the employee has committed an unlawful act, and b) that the cameras have caught him in the act (flagrante delicto).

This judgment has the dissenting vote of 5 of the 11 judges who were members of the Plenary at the time it was issued. Among them are the current President, Mr. Conde-Pumpido, the current Vice-President, Ms. Montalbán, as well as Mr. Sáez and Ms. Balaguer. In his opinion, the majority would be "*placing the general rule and the exception on the same level of value". If it depends on them: "[i]t will not be enough to verify that there is a situation of flagrancy in the capture of the image and the presence in the workplace of the posters announcing the existence of the system to legitimize, from the perspective of art. 18.4 EC, the use of that image for disciplinary purposes. It will also be necessary, in view of the essential and principal nature of the specific duty to inform the workers as a guarantee of the fundamental right, for the employer to give full reasons for non-compliance*".

Having substantially changed the composition of the Plenary, it cannot be ruled out that the minority position at the date of this resolution will be imposed in the future, in a judgment on a new similar case.

Constitutional Court Ruling No. 42/2022, OMNIUM CULTURAL case.
Subject matter: sanctions for international transmission of personal data.

In this decision, the Constitutional Court dismisses the appeal filed by ÒMNIUM CULTURAL against the judgment of the Contentious-Administrative Chamber of the Audiencia Nacional, which upheld the fine of **€90,000** imposed by the Spanish Data Protection Agency against the entity.

In July 2014, the ÒMNIUM CULTURAL association signed a contract with the BLUE STATE DIGITAL, Inc. (BSD), so that this company, in its capacity as file controller, would store a file of the entity with numerous personal data on its servers located in the USA. At the time the contract was signed, the international transfer of data was covered by Commission Decision 2000/520/EC, according to which the USA was considered a "safe harbor" for hosting personal data of European citizens.

However, in its Judgment of 6/10/2015, the Court of Justice of the European Union invalidated the aforementioned Commission Decision with regard to the consideration of the USA as a safe harbor for data protection purposes.

Although ÒMNIUM CULTURAL tried to terminate the contract with BSD during the months following the publication of the CJEU Judgment, making effective the termination of the contract and the deletion of the file in September 2016, the AEPD imposed a penalty of €90,000 for having breached the prohibition provided for in art. 33 LOPD (1999 version, in force at the time of the facts).

The Agency had received the complaint from two individuals in April 2016 and, after initiating sanctioning proceedings against ÒMNIUM, they detected that the entity had not marked the field relating to international data transfers in the General Data Protection Register, despite the fact that they had registered the file in question at the time. Likewise, the Agency reproached the entity for not informing it of the existence of a file in the USA after the publication of the CJEU Ruling, despite the fact that on 19/10/2015 the AEPD published on its website a communiqué informing of the effects of the ruling.

The sanction imposed on ÒMNIUM was the second sanction applied by the AEPD for a breach of international data transfer.

Judgment of the **Supreme Court (Plenary of the Labor Chamber)** no. 692/2022, of July 22, p. García-Perrote Escartín.
Subject matter: evidentiary validity of a hidden camera installed by the employe.

In this judgment, the Plenary of the Social Division of the Supreme Court upheld the appeal filed by a domestic worker whose employer, after the High Court of Justice of Asturias had rejected as valid evidence the images captured by the hidden camera installed in her home, with the consequent unfairness of the dismissal of her domestic worker.

The homeowner had been robbed of €30,000 in cash, a box with jewelry and other valuables located in her bedroom closet and other rooms in the house. After the incident, she installed a hidden camera in front of the closet where she kept the safe. Weeks later,

reviewing the captured images, he found that his housekeeper had tried to break into the safe.

The employer of the household, who had several people helping her because she was a quadriplegic, did not specifically inform her employees about the (possible) existence of cameras. Nor did she install the sign approved by the AEPD (see art. 22.4 LOPD and Instruction no. 1/2006 of the AEPD).

The Fourth Chamber found that, in this particular case, the measure was proportionate, and therefore did not consider that the employee's fundamental right to the protection of personal data (art. 18.4 EC) had been violated. Among the many arguments used to support its decision, one stands out. According to the Court, a distinction must be made between permanent and ad hoc video-surveillance systems. In the former, compliance with the generic duty to inform with the approved sign (art. 22.4 LOPD) is practically unavoidable. In the case of one-off installations, this duty admits greater relativization.

Judgment of the **Supreme Court (Criminal Division)** no. 132/2022, of January 24, p. Hernández García.
Subject matter: evidentiary validity of the evidence obtained through the registration of corporate e-mail.

In this decision, the Criminal Chamber of the Supreme Court strengthens the doctrine established in its Judgments No. 489/2018, of October 23, p. del Moral García and No. 328/2021, of April 22, p. Marchena Gómez, in which the conditions under which an employer can legitimately access an employee's email are examined.

Access to the employee's e-mail is only lawful with the employee's prior consent. Their consent may be express or tacit. In any case, **a prior notice** of the possibility of inspection of the computer and/or telematic equipment and systems made available to the employee is essential. The warning must clearly and precisely determine the conditions of the eventual search: "*who, how, when, why and to what extent*" access may occur.

The case presents a remarkable particularity: the person who accessed the e-mails was a **partner of the company**. Obviously, the adverse party questioned the legitimacy of his access simply because he lacked the authority to do so. Although the Court did not go into the merits of the case with a pronouncement on this point, it did state that "*it is*

highly questionable whether the mere condition of partner of a company, without any management responsibility whatsoever, qualifies him to exercise functions of control and supervision of the business activity, outside the channels of the right to information guaranteed by the sectorial legislation".

Ruling of the **Superior Court of Justice of Madrid** No. 671/2022, of September 23, p. Moreno González-Aller:
Subject matter: evidentiary validity of the recording of a telephone conversation between two workers obtained by the employer.

The Superior Court of Justice of Madrid heard the case of an employer who, in the context of a labor dismissal proceeding, provided the recording of the telephone conversation held by the dismissed worker with another colleague, in which the former insulted and threatened the latter.

From the text of the judgment it can be inferred that the recording was obtained by the company, not by the insulted and threatened worker. However, it was the latter who reported what had happened to his superiors, agreeing that the company should use the recording as a source of evidence in the legal proceedings that his employer had against the other worker. The consent to the recording on the part of one of the interlocutors would have occurred *ex post*.

Judgment of the **Superior Court of Justice of Catalonia** no. 5693/2022, of October 28, p. Bono Romera:
Subject matter: validity of the evidence obtained by the employer from the employee's social networks.

The Superior Court of Justice of Catalonia ruled in this decision on the possibility that an employer may use as a valid source of evidence in a labor proceeding the photographs that an employee may have posted of herself on her personal *Facebook* account.

The Social Chamber of the TSJ of Catalonia confirms the admissibility of the evidence with the argument that the employee would have made an act of liberality with respect to the personal photographs posted on the social network, without any restriction to her contacts, to whom she allows access to her profile, on their possible use or dissemination.

State Attorney General's Office

On December 20, 2022, the State Attorney General's Office published Circular No. 2/2022, on the extraprocedural activity of the Public Prosecutor's Office in the field of criminal investigation, revising and updating the criteria provided on the matter in Circular No. 4/2013, on Investigative Diligences.

Three sections of the Circular are worth mentioning here. The one on the treatment of anonymous complaints (point 4.2.3), the one on the admissibility of evidence obtained by private individuals (point 5.9) and the one on the securing of data or information contained in computer systems, as a precautionary measure (point 7.2).

- Anonymous complaints (point 4.2.3)

In the words of the State Attorney General's Office, regardless of any irregularities of a formal nature that may be present in the complaint filed with the Public Prosecutor's Office, nothing will prevent its admission for processing and the consequent initiation of the appropriate investigative proceedings when the facts reported appear to be criminal in nature and present indications of verisimilitude.

- Admissibility of evidence obtained by private parties (item 5.9)

Regarding the validity of evidence obtained by private individuals, the Prosecutor's Office endorses the doctrine set forth by the Plenary of the Constitutional Court in STC No. 97/2019 (*Falciani cases*).

The instruction addressed to the members of the Public Prosecutor's Office is that evidence obtained by the private individual in violation of fundamental rights should not, as a general rule, be admitted. However, in the light of the doctrine established by the Plenary of the Constitutional Court, the Prosecutors should assess the convenience of taking them into account based on the following parameters:

i) The nature and characteristics of the infraction, weighing its instrumental, objective or subjective connection with the investigation carried out by the public authorities.

ii) The result of the action and, specifically, its greater or lesser impact on the essential nucleus of the violated right.

iii) The risk of favoring practices that compromise pro future the effectiveness of the fundamental right at stake in the event of admitting the assessment of the evidence in the specific case, i.e., its potential appeal effect.

Particularly interesting are the indications contained in relation to the recordings of private conversations. They are reproduced verbatim because of their special interest:

a)The use in criminal proceedings of recordings of private conversations made by one of the interlocutors does not violate the right tosecrecy of communications.

b) Nor does it violate the right to privacy, except in exceptional cases in which the content of the conversation affects the personal or family privacy of one of the interlocutors.

c) Recordings made from a position of institutional superiority (agents of authority or hierarchical superiors) to obtain an extra-procedural confession obtained by deception violate the fundamental right not to testify against oneself and not to confess guilt and, consequently, are null and void as evidence.

d) The recordings made in the private sphere do not violate the fundamental right not to testify against oneself and not to confess guilt.

e) The right to due process may be violated by a recording in which the person has been brought to the meeting using trickery with the premeditated intention of making him state facts that could be used against him, in which case the circumstances of the case must be considered as a whole. of concurrent circumstances will have to be weighed.

At least two extremes seem to us to be noteworthy. Firstly, the possibility of considering recordings of conversations on core aspects of privacy as an infringement of the right to privacy (point (b)), which implies a relativization of the rule, which seemed to be established, that the recording of the conversation by the interlocutors is (no longer) always lawful.

Second, that deception as to the purpose or nature of the conversation by one of the interlocutors or a third party may result in the recording being contrary to the right to due process. This consideration is particularly relevant in the area of internal

investigations. According to the provisions of the Circular, it can be deduced that **covert or surreptitious interviews or interrogations**, recorded without having previously informed the interlocutor, are not acceptable.

- Securing of data or information contained in computer systems (item 7.2)

The Circular clarifies that the precautionary measure of securing data contained in computer systems does not require prior judicial authorization or a qualified motivation on its part, since this measure does not affect the right to privacy or secrecy of communications. Securing does not imply access to the contents. It simply guarantees their preservation