MOLINS

Investigaciones Internas

Yearbook 2024

Compilation of the most relevant regulations and case law of the year on internal investigations

January 2025

Internal Investigations Team

Dr. Albert Estrada Cuadras

Cristina Molins Joly

Laura de Dalmases Herrero

Clara Tomàs Vaque

Carla Sans Argilés

Table of Contents

I. Europe

A) Regulations

➢ Regulation (EU) 2024/1689 of the European Parliament and of the Council of of 13 June 2024, establishing harmonised rules on artificial intelligence.

The so-called "AI Regulation," approved by the EU last year, is the first of its kind worldwide. Regarding internal investigations, it is particularly relevant in relation to certain uses of artificial intelligence that may be employed in this type of inquiry. Consider, for example, facial recognition tools, mass data processing, etc.

Under this regulation, which applies directly in Member States upon its entry into force (staggered and in phases), the use of some of these tools may be subject to strict legitimacy conditions or outright prohibited.

For instance, the following prohibitions, set out in Article 5, are noteworthy:

> *"(e) The placing on the market, putting into service for this specific purpose, or use of AI systems that create or expand **facial recognition databases** by indiscriminately extracting facial images from the internet or CCTV footage;*
>
> *(f) The placing on the market, putting into service for this specific purpose, or use of **AI systems to infer a natural person's emotions in workplaces and educational institutions,** except where the AI system is intended to be installed or placed on the market for medical or safety reasons;*
>
> *(g) The placing on the market, putting into service for this specific purpose, or use of **biometric categorization systems that individually classify natural persons** based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sexual life, or sexual orientation; this prohibition does not include the labeling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data, nor the categorization of biometric data in the context of law enforcement compliance."*

While, as a general rule, the Regulation will not become applicable until August 2026, some of its provisions will take effect earlier. This is the case for the aforementioned prohibitions and the rest of the provisions set out in Chapter I (General Provisions) and Chapter II (Prohibited Practices) of the Regulation, which will be directly applicable from **2 February 2025.**

- **Council of the EU's Position on the Proposal for a Directive of the European Parliament and the Council on Combating Corruption, 17 June 2024**

The legislative process for the proposed Directive aimed at harmonizing the criminalization of corruption-related acts in EU Member States, as well as preventive (criminal or non-criminal) measures, is progressing. The Directive covers not only public corruption but also private-sector corruption.

Regarding the proposed criminalization model from Brussels, a broader definition **of private-sector corruption stands ou**t. The proposal seeks to expand the material scope of the offense, so that an offense would be committed by "failing to fulfill the duties" inherent to a position or function in exchange for an undue advantage (Article 8 of the proposed Directive). Currently, the wrongdoing consists of "unduly favoring another in the acquisition or sale of goods, in the contracting of services, or in business relations" in exchange for an undue advantage (Article 286 bis of the Spanish Penal Code).

The proposal explicitly criminalizes wrongful acts by omission, meaning the unjustified failure to act. Although, from a doctrinal perspective, criminal liability for such conduct could already be considered under the theory of commission by omission (Article 11 of the Spanish Penal Code).

However, European legislators do not mandate the criminalization of subsequent bribery or bribery solely for the purpose of obtaining a position (such as the offense described in Article 422 of the Spanish Penal Code).

B) Case Law

- **General Court of the European Union (GCEU) Judgment of 11 September 2024, Case T-793/22**

  Subject: Protection conditions for whistleblowers. Condemnation of the European Parliament for inadequate protection of an institutional employee.

In its judgment of 11 September 2024 (Case T-793/22), **the General Court of the European Union (GCEU) ruled on the protective measures that EU institutions must implement for whistleblowers under Articles 22 bis to 22 quater of the Staff Regulations**. The case concerns an Accredited Parliamentary Assistant (APA) of the European Parliament who, after reporting alleged financial irregularities and harassment, was initially reassigned to the duties of another MEP and later saw a significant reduction in his responsibilities. Once his contract expired, it was not renewed.

In response, the assistant appealed to the General Court, claiming that the non-renewal of his contract constituted direct retaliation for his disclosures. He sought formal recognition of his whistleblower status, the adoption of additional protective measures—including an extension of his employment contract—and compensation of €200,000, arguing that his right to confidentiality and the necessary safeguards against retaliation had been violated.

The European Parliament, on the other hand, maintained that the contract's termination was solely due to its natural expiration and unrelated to the complaints filed. It argued that, while the Staff Regulations impose a duty to protect whistleblowers, they do not create additional employment rights, such as an obligation to renew a temporary contract. According to its position, the measures taken—the initial reassignment and subsequent reduction of duties—were proportionate steps to separate the assistant from the environment associated with the reported irregularities, thereby meeting the statutory protection requirements.

In its analysis, the General Court reiterated that whistleblower protection is automatic and does not require formal recognition. However, it clarified that such protection does not entail the creation of new contractual rights, meaning that there is no general obligation to extend employment relationships. Nevertheless, institutions must demonstrate that they have taken all necessary measures to ensure effective protection against potential retaliation. This obligation includes adequately informing the whistleblower of the steps taken and strictly preserving their identity to prevent any exposure to reprisals.

In this case, the Court found that the European Parliament had failed to provide sufficiently effective protective measures.

Although the reassignment might have been a first step, it was not complemented by additional actions to prevent further harm. The lack of clear communication about the measures implemented and, in particular, the disclosure of the whistleblower's identity constituted a breach of the duty of confidentiality. This failure weakened the protection framework established in the Staff Regulations, exposing the whistleblower to potential retaliation and undermining the effectiveness of the safeguards under Articles 22 bis to 22 quater of the Staff Regulations.

Upon identifying these shortcomings, the Court annulled the tacit decision not to adopt additional protective measures and **ordered the European Parliament to pay €10,000** in moral damages.

- **European Court of Human Rights (ECtHR) Judgment of 7 August 2024, Case A.K. v. Russia, Application No. 49014/16**

  Subject: (In)compatibility of a disciplinary dismissal with the right to private life (Article 8 ECHR) based on photographs uploaded by a teacher on her social media.

  Facts:

Since 2011, Ms. A.K. had been working as a music teacher at a public special education school in Saint Petersburg. In December 2014, she was dismissed for allegedly engaging in immoral conduct incompatible with the performance of educational duties involving minors.

This conduct consisted of posting on social media photographs in which she was seen kissing other women—expressions of affection of an erotic nature that made her homosexuality explicit. In other photographs, she was shown raising her middle finger towards the camera.

The photographs uploaded to Ms. A.K.'s social media profile were not publicly accessible but were available only to her personal network of contacts.

Legal Reasoning :

The representative of Russia argued that the dismissal was not based on the teacher's homosexuality but rather on the fact that she had posted sexually suggestive photographs, as well as other images deemed insolent (e.g., showing her middle finger to the observer). The publication of both types of content, it was claimed, violated ethical standards in Russia.

In its ruling, the Court rejected this argument. A review of several passages from the decisions issued by Russian courts made it evident that making her homosexuality explicit was considered an immoral act, justifying her dismissal.

Nonetheless, the Chamber held that even if it were to accept the Russian representative's argument, the disciplinary dismissal was disproportionate. Before resorting to the most severe employment sanction, less harmful measures should have been exhausted, such as issuing a warning requiring the removal of the images, a reprimand, suspension from work, or a salary reduction, among others. Furthermore, the Chamber noted the lack of a reasoned analysis in the national rulings regarding the severity of the allegedly immoral acts. A proper assessment should have considered the context in which the images were taken, the number of people who could view them, the access conditions for third parties, and other relevant circumstances.

For all these reasons, the European Court of Human Rights found that the disciplinary dismissal in this case constituted a violation of the right to private life under Article 8 of the European Convention on Human Rights (ECHR), as well as a violation of the right to non-discrimination based on sex, as protected under Article 14 ECHR.

II. Spain

A) Regulations

- **Royal Decree 1101/2024, approving the Statute of the Independent Authority for Whistleblower Protection (AAI**

On 29 October 2024, with a delay from the initially scheduled one-year deadline, Royal Decree (*Real Decreto*) 1101/2024 was published, approving the Statute of the Independent Authority for Whistleblower Protection (*Autoridad Independiente de Protección del Informante, AAI*) in Spain. This new institution was created as a result of Law (Ley) 2/2023, of 20 February, which transposed Directive (EU) 2019/1937 on the protection of persons reporting regulatory breaches and corruption into Spanish law.

The AAI was established to ensure that individuals reporting unlawful conduct can do so without fear of retaliation and with full protection of their identity. According to Royal Decree 1101/2024, the AAI is an independent entity with its own legal personality and functional autonomy, tasked with receiving, managing, and safeguarding reports while guaranteeing whistleblower confidentiality at all times.

The structure of the AAI is built around a Presidency, a Consultative Commission, and two main departments: the Whistleblower Protection and the Monitoring and Sanctioning Department The first department is responsible for receiving and processing reports while ensuring whistleblower rights, while the second monitors compliance with regulations, handles administrative proceedings, and, where applicable, imposes sanctions.

The AAI's powers include managing reports submitted via the external reporting channel and implementing protection and support measures for whistleblowers. It also issues opinions on legislative proposals within its scope, develops guidelines and prevention models, and collaborates with national and international institutions. Additionally, it has the authority to initiate, process, and resolve sanctioning procedures for violations established under Ley 2/2023. Notably, decisions issued by the AAI cannot be appealed through administrative or judicial channels. However, rulings concluding a sanctioning procedure initiated as a result of its investigations may be challenged.

One of the main limitations of its functions is that the AAI cannot investigate matters that are already under judicial, prosecutorial, or judicial police review. In such cases, it must suspend its actions—except for whistleblower protection measures—and cooperate with the relevant authorities by providing necessary information.

Regarding the procedure, whistleblowers can submit their reports anonymously through a secure channel, ensuring confidentiality at all times. Once the information is verified, the AAI may refer the case to the Public Prosecutor's Office (*Fiscalía*) if there is sufficient evidence to warrant criminal action.

The sanctioning regime establishes fines of up to €300,000 for individuals and up to €1,000,000 for legal entities in cases of very serious infractions. Additionally, in such severe cases, the AAI may impose additional penalties, such as a public reprimand, prohibition from contracting with the public sector for up to three years, or exclusion from tax benefits for a maximum of four years.

- **Legal Opinion No. 77/2023 of the AEPD Legal Department**

  Subject: Compliance with data protection regulations in the processing of information received via an internal reporting system when it is outside the scope of Law 2/2023.

In this opinion, the Legal Department of the Spanish Data Protection Agency (*AEPD*) addressed a query regarding the possibility of processing personal data contained in an internal report for purposes other than those provided for in Law 2/2023, particularly when the report's subject matter or whistleblower falls outside the law's scope.

Specifically, the question concerned whether such data—submitted through an internal reporting system established under Law 2/2023—could be used for efficiency, transparency, and good governance purposes.

The Legal Department responded negatively. While it is generally possible to process personal data for purposes different from those for which they were originally obtained, the consulting body determined that in this case, the necessary conditions for such processing were not met.

This position is based on the **principle of purpose limitation**, which plays a key role in Law 2/2023 and is designed to maximize data protection. The opinion references several provisions of the law that establish obligations to delete personal data that fall outside the law's scope or are unnecessary for compliance with its duties (see Articles 29, 32.2, 32.4, and 26.2).

Furthermore, the Legal Department rejects the proposed data processing based on material criteria established by the Article 29 Working Party in its Opinion 3/2013 on Purpose Limitation. These criteria include the difference between the original and subsequent processing purposes, the context in which the data was collected and the data subjects' reasonable expectations regarding their use, the nature of the data and the impact of further processing, and the safeguards adopted to prevent undue harm to the rights of the data subjects.

In light of these criteria, further processing for purposes other than those established in Law 2/2023 would not be justified.

➢ AEPD Guidelines for Data Controllers on Wi-Fi Tracking Technologies

Recently, technologies have emerged that allow the **detection** of electronic devices using Wi-Fi **signals within a given area** and the **tracking of their movements** in a specific geographic space. These technologies operate without requiring the device to connect to a Wi-Fi network and without the device owner being aware that their presence is being detected or their movements are being tracked. This occurs because the technologies function based on the signals systematically emitted by the device, even when it is not connected to a network. These signals contain a device identifier code, known as the "device fingerprint" (MAC address – Media Access Control).

Possible applications of these technologies include estimating occupancy levels, analyzing crowd movement patterns, calculating attendance statistics and average dwell times in specific locations, estimating queue wait times, determining the most frequently used routes, and calculating visit repetition rates.

In the guidance document, the AEPD provides a set of recommendations for ensuring that such technologies comply with data protection regulations.

B) Case Law

1. Supreme Court

- **STS (Criminal Chamber) No. 889/2024, of 23 October, p. Judge Martínez Arrieta**

  Subject: Employer's access to corporate email in the absence of a written usage policy. Such access does not constitute the criminal offense of breach of privacy under Article 197 of the Spanish Penal Code.

Facts:

The managing director and majority shareholder of a company accessed the content of emails exchanged between three employees through their corporate email accounts. Among the emails were numerous personal conversations, some of which provided clear evidence of an extramarital romantic relationship between two of the affected employees.

The email accounts in question were not secured by personal passwords. The computers assigned to the employees required a generic password, known by all workers in the small-sized company, to be turned on.

Article 26 of the applicable Collective Bargaining Agreement (*Convenio Colectivo*) for Offices and Administrative Staff classified the use of company tools or materials for personal purposes as a serious offense.

During regular meetings between management and the company's eight employees, the use of company IT resources for personal purposes was repeatedly prohibited. That the employees subject to the search were aware of this restriction was evidenced by several of their emails, in which they discussed the convenience of using alternative communication channels to avoid detection.

The affected employees had signed a document explicitly prohibiting the personal use of the IT resources provided by the company for work-related tasks. It was established as a proven fact that around that time, a backup copy of the company's email server was created due to operational issues caused by excessive storage use. According to the facts of the case, it was during this backup process that the personal emails of the affected employees were discovered.

Three days after the signing of the aforementioned document and the employer's access to the personal content of the emails, the employees were dismissed on disciplinary grounds.

The dismissal was challenged before the Labor Court (*Juzgado de lo Social*), which ruled that the termination was null and void because it was based on evidence obtained unlawfully, violating the fundamental right to privacy (Article 18.1 of the Spanish Constitution).

In the criminal jurisdiction, both the Criminal Court (*Juzgado de lo Penal*) and the Provincial Court (*Audiencia Provincial*) on appeal concluded that the employer's access to the corporate email accounts did not constitute the criminal offense of breach of privacy (*delito de descubrimiento de secretos de la intimidad*) under Article 197.1 of the Spanish Penal Code

Legal reasoning:

After briefly reviewing the Supreme Court's case law on employer access to employee IT resources, from STS 528/2014, of 16 June (Presiding Judge Maza Martín) to the more recent STS 83/2023, of 19 February (Presiding Judge Puente Segura), the Court concluded that the managing director's access to the personal content of numerous emails belonging to three employees did not constitute the offense set out in Article 197.1 of the Penal Code:

> "Analyzing the matter from the perspective of the case before us, it is established in the proven facts that the complainants, now appellants, had been duly warned and had acknowledged the prohibitions against using company IT resources for personal purposes. Furthermore, their emails were not secured by a personal password. The factual account states that they had been informed, without reservation, of the strict obligation to maintain confidentiality regarding work-related information, as well as the exclusive

professional use of company IT systems and software. They had been reminded of this obligation on multiple occasions, and in their own messages, they warned each other about the need to delete them and use alternative communication methods. With these precautions, they were fully aware of the usage limitations imposed upon them. Moreover, the factual account confirms that no act of intrusion took place; rather, during a routine backup of the company email server, it was discovered that the inbox was reaching storage capacity, and its use for non-work-related matters became evident."

This case highlights the existence of different legal standards in the evidentiary-procedural sphere and the substantive-criminal sphere. While the access to emails was deemed unlawful from the perspective of the validity of the obtained evidence (as ruled by the Labor Court of first instance), a finding not contested by the Criminal Chamber of the Supreme Court, the managing director's conduct was not considered criminally relevant. The threshold for conduct to qualify as a criminal offense is higher.

This ruling also reaffirms that the Criminal Chamber applies different standards to access corporate email accounts versus personal accounts. This distinction was already evident in STS No. 328/2021 (Presiding Judge Marchena Gómez), where an employer was sentenced to prison for accessing an employee's personal email account (Gmail), despite the fact that the employer had been able to access it without any obstacles from the corporate computer assigned to the employee.

- **STS (Criminal Chamber) No. 753/2024, of July 22, p. Ferrer García ("Brugal" case).**

  Subject: validity and probative force of sound recordings obtained by individuals.

Facts:

On 22 March 2006, during the bidding process for the waste collection service contract in the municipality of Orihuela (Alicante, Spain), one of the competing businessmen published in the press a recording of conversations he had with a municipal councilor, allegedly revealing that the contract—valued at €8.5 million—had been awarded in exchange for illegal commissions.

The recordings were made public the day after the municipal contracting committee submitted its award proposal to the City Council Plenary Session. The businessman's bid was among those that were unsuccessful.

Following the businessman's public disclosure, the Anticorruption Prosecutor's Office of Alicante filed a complaint before the Courts of First Instance and Preliminary Investigation of Orihuela, which was assigned to Court No. 3. By an order of 8 March 2007, preliminary proceedings were initiated, and a secrecy order was imposed on the investigation from 12 April 2007 to 14 July 2010.

Based on the recordings provided by the businessman, the investigating judge authorized multiple telephone interceptions.

Among the recordings submitted by the businessman, a distinction must be made between audio recordings of his conversations with the councilor, which he obtained by hiding a recording device under his clothing, and video recordings of those meetings, which were made by a private investigator hired by the complainant. Copies of both types of recordings were submitted to the judicial proceedings, but at no point were the original recordings provided.

Regarding the telephone interceptions carried out by the Judicial Police using the SITEL system, these were authorized by court order on 8 March 2007, based on indications of criminal activity derived from the businessman's recordings and subsequent police investigations.

After twelve years of criminal proceedings, the case was tried by the Seventh Section of the Provincial Court of Alicante, with oral hearings beginning on 5 March 2019 and concluding in June of the same year. The first-instance ruling was published approximately one year later, on 3 June 2020.

The court declared the nullity of the proceedings from the start of the investigation, labeling it "radical nullity", on the grounds that fundamental rights under Articles 18.1 and 18.4 of the Spanish Constitution—the right to personal privacy and the right to digital privacy—had been violated. The ruling was based on two key arguments:

i) The recordings provided by the businessman, which justified the initial investigation by the Prosecutor's Office and the subsequent opening of preliminary proceedings, were obtained surreptitiously and without a legitimate interest, in violation of the aforementioned fundamental rights.

ii) Those recordings, as well as the ones obtained by the Judicial Police through court-authorized telephone interceptions, were copies, meaning they did not meet the authentication and integrity requirements necessary for admissibility.

Due to the lack of sufficient incriminating evidence, among other reasons but primarily based on this, all 34 defendants were acquitted of the alleged offenses of administrative misconduct, fraud

against the public administration, misuse of privileged information, bribery, and influence peddling, among others.

In the judgment under review, the First Section of the Criminal Chamber of the Supreme Court overturned the lower court's decision and ordered the Provincial Court of Alicante to deliberate again and issue a new ruling, considering the evidentiary material that had been excluded in its initial decision.

Legal reasoning:

In its ruling, the Supreme Court extensively outlined its jurisprudence as well as that of the Constitutional Court on the admissibility of covert recordings made by one of the parties to a conversation (a private individual, as opposed to a public official or state agent), and their compatibility with the fundamental rights to secrecy of communications (Article 18.3 of the Spanish Constitution) and privacy (Article 18.1 of the Spanish Constitution) of the other parties involved. The ruling also examined the compatibility of such recordings with the right against self-incrimination, the right not to confess guilt, and the right to a fair trial with full guarantees (Article 24.2 of the Spanish Constitution).

The Court summarized its conclusions in an exceptionally clear and concise manner (Legal Grounds 2º):

> "1º) The use of private conversation recordings made by one of the participants in criminal proceedings does not violate, under any circumstances, the constitutional right to the secrecy of communications.
> 2º) Nor does it violate the constitutional right to privacy, except in exceptional cases where the content of the conversation affects the core of an individual's personal or family privacy.
> 3º) Such recordings violate the fundamental right against self-incrimination and the right not to confess guilt, and are therefore inadmissible as evidence, when they have been obtained from a position of institutional superiority (by law enforcement officers or hierarchical superiors) to extract an extrajudicial confession through deception—except in cases where the recordings have been authorized by judicial authorities under Articles 588 et seq. of the Spanish Criminal Procedure Code (*LECrim*).
> 4º) They do not violate the fundamental right against self-incrimination or the right not to confess guilt when made in a private context.
> 5º) They may violate the right to a fair trial with full guarantees if the recorded individual was lured into the conversation through deceit with the deliberate intention of making them disclose facts that could be used against them, in which case all surrounding circumstances must be carefully assessed.
> 6º) Supreme Court jurisprudence avoids classifying the statements made by the accused in these recordings as confessions, instead treating the recordings as corroboration of statements made by other

participants in the conversation, which are considered hearsay evidence regarding the accused's declarations."

Regarding internal private investigations, two key aspects of the Chamber's conclusions stand out: one concerning the fundamental right against self-incrimination and another regarding the right to a fair trial with full guarantees.

As for the right against self-incrimination, the Chamber's stance clearly favors the traditional and restrictive interpretation of this right, according to which this privilege is only applicable in the State-citizen relationship (a vertical relationship) and not in private interactions (theoretically horizontal relationships). In this regard, STS No. 421/2014, of 16 May, is particularly relevant, as it states that "*the State/citizen relationship (…) is the natural domain in which fundamental rights operate*." Similarly, the ruling under review affirms: "*According to Supreme Court jurisprudence, recordings deceitfully made by law enforcement officers to extract an extrajudicial confession would be inadmissible for violating the constitutional right not to confess guilt, but this does not apply to private relationships*."

However, in the Chamber's conclusions reproduced above, point 3 does not refer exclusively to law enforcement officers, but also to hierarchical superiors, stating that recordings of a confession obtained through deception from a position of institutional superiority (such as law enforcement officers and hierarchical superiors) would not be admissible as evidence. Although the Chamber's reasoning does not explicitly mention "hierarchical superiors", a category that could include an employer in relation to their employees, this reference in the conclusions raises doubts about the Chamber's stance on confessions obtained through deception in the context of an internal workplace investigation.

Regardless, the evidentiary validity of such a recording could still be challenged based on the right to a fair trial with full guarantees. In this regard, there is no doubt that the Chamber extends this principle to private relationships (theoretically horizontal) when "*the recorded individual has been lured into the meeting through deceit with the deliberate intention of making them disclose facts that could be used against them*." Notably, STS No. 1066/2009, of 4 November, excluded the admissibility of a recording obtained by a private individual through deception and premeditation. Nevertheless, as explicitly stated by the Chamber, the assessment of evidentiary validity must be carried out on a case-by-case basis, taking into account the specific circumstances of the case: "*the full set of concurrent circumstances must be weighed*."

➢ STS (Social Chamber - Section 1) No. 225/2024, of 6 February

Subject: The role of workers' representatives in drafting IT usage policies (IT or ICT policies).

In its recent ruling No. 225/2024, of 6 February, the First Section of the Fourth Chamber of the Supreme Court confirmed the nullity of the instructions issued by a company to its employees regarding the permitted use of digital devices provided for work purposes, which also outlined the applicable control mechanisms (monitoring, etc.).

The reason for the invalidity of the company's guidelines was the lack of involvement of workers' representatives in their drafting, in violation of **Article 87.3 of the Organic Law on Data Protection** (*Ley Orgánica de Protección de Datos*, LOPD).

Accordingly, the Chamber dismissed the cassation appeal filed by the company, which argued that annulling these instructions infringed its **right to employer control**, recognized under Article **20.3 of the Workers' Statute** (*Estatuto de los Trabajadores*). Specifically, the appellant contended that the instructions challenged by the trade union representation of its workers merely reiterated an existing usage policy that had been established and communicated before Article 87.3 LOPD came into effect in late 2018.

While the Chamber acknowledged that the requirement set forth in Article 87.3 LOPD does not have retroactive effect, it concluded that the disputed instructions were not merely a reminder but instead represented a fundamental change in the applicable usage and control rules within the organization. Consequently, it upheld the nullity previously declared by the National Court (*Audiencia Nacional*).

The denial of retroactive effect to the requirement of mandatory worker participation has significant implications. Firstly, there would be no obligation to update policies drafted and communicated **before** the entry into force of the current LOPD in late 2018. As a result, the lack of worker representation in their drafting should not affect the legitimacy of evidence obtained under such policies.

The Chamber did not rule on the admissibility of evidence collected through IT monitoring based on a digital device usage policy adopted **after** the LOPD came into force (7 December 2018) without the involvement of workers' representatives, as this was not the subject of the dispute. However, it noted that if such guidelines respected the principle of proportionality in relation to workers' rights to privacy and data protection, their nullity would not necessarily render the resulting evidence inadmissible.

- **STS (Social Chamber - Section 1) No. 874/2024, of 5 June, p. Judge Molins García-Atance**

  Subject: Legality of locker or personal belongings searches conducted on an employee.

Through ruling STS No. 874/2024, of 5 June, the First Section of the Fourth Chamber of the Supreme Courtdismissed the cassation appeal and upheld the judgment issued by the High Court of Justice of Andalusia (*Tribunal Superior de Justicia de Andalucía*), which had overturned the ruling of the *Juzgado de lo Social* No. 3 of Huelva and declared the dismissal of an employee at a well-known shopping center to be unfair.

The claimant was dismissed on disciplinary grounds after being stopped in mid-January 2020 at the shopping center's exit with store merchandise. Specifically, the security alarm was triggered, and a security guard searched her personal handbag, discovering four store items inside—including protein bars, snacks, and dog shampoo of minimal economic value. The guard asked her to show her purchase receipts, all without the presence of a workers' representative or another employee of the company.

Immediately afterward, the company reviewed security camera footage and confirmed that the employee had indeed stolen the referenced items from the store premises. Consequently, it proceeded with her dismissal on disciplinary grounds, citing a very serious offense under its internal regulations and the applicable collective bargaining agreement, as well as Article 54.2(d) of the Workers' Statute.

The employee filed a claim for unfair dismissal, and after an unsuccessful conciliation hearing, the case was ultimately decided by the Social Chamber of the *Tribunal Superior de Justicia de Andalucía*, which declared the dismissal null and void. The company appealed the decision, but it was upheld.

The ruling under review centers on determining the legality of searching the claimant's personal handbag when no workers' representative or another employee was present. The High Court of Justice of Andalusia ruled that such a search was unlawful, and consequently, the alleged theft lacked sufficient evidentiary support to justify the dismissal, leading to the declaration of the dismissal as unfair.

The company's legal counsel argued that Article 18 of the Workers' Statute had not been violated, claiming that no actual search of the employee's belongings had taken place. Instead, they contended that the alarm had merely gone off, and that the employee had voluntarily shown the

contents of her handbag to the security guard. Based on this, they maintained that the evidence was valid despite the absence of a workers' representative. The cassation appeal was supported by STSJ Cataluña No. 6486/2018, of 11 December, in which, under what the appellant considered identical facts, legal grounds, and claims, the dismissal had been upheld as fair.

It should be noted that Article 18.1 of the Workers' Statute explicitly requires the presence of one or more persons (a workers' representative or another employee) during the search of a worker's personal effects, such as lockers or personal belongings.

Additionally, the ruling emphasized that the company's action in this case amounted to a form of "private policing", constituting an exception to the general legal framework under Articles 545 et seq. of the Criminal Procedure Code. Special reference was made to Constitutional Court jurisprudence, which establishes that employers must fully respect the right to privacy of employees (Article 18.1 of the Spanish Constitution) in the workplace.

Furthermore, the Court clarified that the presence of another employee or workers' representative during a search is not meant to guarantee respect for the employee's privacy, but rather to ensure the objectivity and evidentiary reliability of the search by involving an impartial third party.

For these reasons, the Supreme Court reaffirmed that "a worker's handbag is a personal belonging protected under Article 18 of the Workers' Statute. It therefore dismissed the cassation appeal, ruling that the search was carried out by a security guard without the presence of a workers' representative or another company employee, in violation of Article 18 of the Workers' Statute, without any justification.

Thus, the Chamber concluded that the unjustified violation of this legal provision renders the evidence obtained from the search inadmissible. Consequently, it held that the dismissal was unfair.

- **STS (Social Chamber - Plenary) No. 1250/2024, of November 18, p. Judge García Paredes**

  Subject: Formal requirements for a valid disciplinary dismissal. The worker's right to be heard before dismissal (right to prior hearing).

Facts:

This ruling concerns a cassation appeal filed by a public higher education institution against the decision of the High Court of Justice of the Balearic Islands (*Tribunal Superior de Justicia de les Illes Balears*), which had declared the dismissal of one of its employees unfair. This contradicted the judgment of Social Court No. 4 of Palma (*Juzgado de lo Social n.º 4 de Palma*), which had dismissed the worker's claim in the first instance.

The employee, a professor at the institution and a member of its management team as Secretary, had been internally reported by several students as well as the institution's Student Association, which filed a formal complaint signed by 56 individuals and including 16 testimonies describing inappropriate behavior. The allegations included making sexually suggestive comments about students' clothing, intimidating stares, invading personal space, and unjustified photography during class.

After internal inquiries carried out by the institution's administration and the Education Inspection Unit of the Balearic Government, which included interviews with students and other faculty members, the worker was dismissed on disciplinary grounds without a prior hearing.

Legal reasoning:

The High Court of Justice of the Balearic Islands declared the dismissal unfair based on Article 7 of the International Labour Organization (ILO) Convention No. 158, ratified by Spain in 1985. According to this provision: "*The employment of a worker shall not be terminated for reasons related to the worker's conduct or performance before he is given an opportunity to defend himself against the allegations made, unless it cannot be reasonably expected of the employer to provide this opportunity*."

The public higher education institution appealed this judgment in cassation, arguing that it was contradictory to the jurisprudence of the Social Chamber of the Supreme Court, as established in rulings such as that of March 8, 1988, delivered by Judge Aurelio Desdentado Bonete. In that decision, as well as in previous rulings, the direct applicability of Article 7 of ILO Convention No. 158 was denied, considering that Spanish labor law already provided sufficient guarantees for workers to defend their legal position, rendering the requirement of a prior hearing unnecessary in Spanish law.

In the ruling under review, the Plenary of the Social Chamber of the Spanish Supreme Court expressly overturned the doctrine established in the 1980s and considered Article 7 of ILO Convention No. 158 directly applicable. The Chamber justified this shift based on value-based reasoning, asserting that the previous position on the matter was incorrect, as well as legislative changes in Spanish law over the nearly forty years since those rulings. These modifications, including Law 25/2014 on Treaties and Other International Agreements and the recognition of the right to a prior hearing for workers' legal representatives, trade union delegates, and union-affiliated employees, support the direct applicability of this provision and the requirement of a prior hearing as a formal prerequisite for disciplinary dismissal of an employee:

> *"The prior hearing before the adoption of the disciplinary dismissal measure, contrary to what this Chamber had previously understood, cannot be confused with other rights available to the worker after the termination of the contract, such as the ability to challenge the disciplinary dismissal measure through judicial proceedings, which is an expression of Article 8 of Convention No. 158 and, in our legal system, is addressed by Article 24.1 of the Spanish Constitution, which recognizes the right of rights holders and legitimate interests to access judicial bodies and obtain a decision based on the law. That is, this process cannot be equated to what Convention No. 158 mandates. (…) The fact that our legal system includes measures to prevent the worker from being in a state of defenselessness after dismissal does not mean that these measures satisfy other obligations imposed by international regulations that are also part of our legal system, such as the one in question. If we understand that this prior hearing adheres to an equity principle—allowing the worker to present any arguments concerning the alleged misconduct before the disciplinary authority makes a decision—then it is simply ensuring a fundamental right to be heard or to defend oneself, which, within the framework of an employment relationship and during its validity, constitutes a formal step in the employer's legitimate exercise of disciplinary authority. (…) All of this means that we are now rectifying the doctrine established by the previous ruling and similar ones. The reason for this shift is not only the reasoning we have just set out but also the legal changes that have occurred over all this time."*

The new jurisprudential doctrine is not retroactively applicable to disciplinary dismissals that have already been adjudicated or are currently under review. The reason is found in Article 7 of ILO Convention No. 158 itself, which contains a reasonableness clause: "*Unless it cannot be reasonably expected of the employer to provide this opportunity [i.e., the prior hearing].*"
Considering that the jurisprudence of the Supreme Court's Social Chamber had previously ruled out the prior hearing as a necessary condition for the validity of disciplinary dismissals since the 1988 precedent, it was not reasonable to require employers to comply with this formality. However, following the issuance and publication of this ruling, the prior hearing will now be a mandatory requirement.

2. High Courts of Justice

- **STSJ Basque Country (Social Chamber - Section 1) No. 1850/2024, of July 23, p. Judge Lajo González**

  Subject: Nullity of the sanction imposed on an employee for accessing pornographic websites using a corporate device. Violation of Articles 10 and 18 of the Spanish Constitution.

This publication discusses STSJ No. 1850/2024, of July 23, issued by the First Section of the Fourth Chamber of the High Court of Justice of the Basque Country (*Tribunal Superior de Justicia del País Vasco*), which upheld an appeal filed by a worker against a first-instance ruling that had dismissed his claim after he was reprimanded for using his corporate mobile phone to access pornographic websites during working hours.

Through STSJ No. 1850/2024, of July 23, the court ruled in favor of the worker's appeal for reversal against the judgment of March 12, 2024, issued by Social Court No. 7 of Bilbao (*Juzgado de lo Social n.º 7 de Bilbao*). It annulled the first-instance ruling and condemned a video surveillance company to pay the claimant €7,501 in compensation for a violation of fundamental rights, with no costs imposed.

The claimant had been working for the respondent company as a security guard for approximately ten years when, on March 31, 2023, he was disciplinarily sanctioned for accessing various pornographic websites during working hours using his corporate mobile phone. As a result, he received a public reprimand, in accordance with the sanctions established in the applicable collective agreement (State Collective Agreement for Security Companies for the period 2023–2026) for a serious offense.

A mandatory conciliation hearing was held but ended without an agreement. In the first instance, Social Court No. 7 of Bilbao dismissed the worker's claim, upholding the company's decision to impose the reprimand. The claimant's legal representation then filed an appeal for reversal, requesting a review, revocation, and annulment of the first-instance ruling.

The claimant alleged violations of Articles 75 and 76 of the applicable collective agreement, as well as Article 60 of the Workers' Statute. He also argued that the company should be condemned to pay compensation for violating his fundamental rights under Article 24 of the Spanish Constitution. Specifically, he claimed an infringement of his right to privacy, and thus a violation

of Article 10 of the Spanish Constitution and Article 183 of the Law Regulating Social Jurisdiction (*Ley Reguladora de la Jurisdicción Social*, LRJS).

Regarding Article 24 of the Spanish Constitution, the claimant argued that this right had been violated because the sanction letter issued by the company did not specify the exact dates or times of the alleged infraction. Consequently, he asserted that such a serious accusation lacked sufficient supporting evidence. Moreover, he claimed that there was no access protocol or authorization for reviewing his device and that his corporate phone was accessed without a workers' representative being present.

The High Court first denied the claimant's request to review the proven facts, stating that such a review was unnecessary and that the first-instance ruling was based on the full content of the sanction letters issued by the company, which specified the dates on which the claimant allegedly misused his corporate phone. Instead, the court focused on the insufficiency of the company's sanction letter in justifying the worker's reprimand.

In this case, there was no explicit prohibition on using the corporate phone for personal purposes, either in the company's policies or in the collective agreement. The sanction letter cited very serious offenses under Article 74 of the applicable collective agreement, particularly Sections 15 ("Committing immoral acts in the workplace or on company premises during working hours") and 20 ("Engaging in games or serious distractions during working hours on company premises"). However, these provisions contained generic references without explicitly prohibiting access to pornographic content. The court ruled that an extensive interpretation of disciplinary regulations in this case would violate the worker's right to privacy.

As a result, the sanction letter did not comply with the formal requirements set out in Article 115.1(d) LRJS, as it contained vague references to accessing sexual content without providing legible evidence or granting access to the supporting materials used to justify the sanction. The STSJ No. 1850/2024 ruling confirmed that this constituted a violation of the worker's right to privacy (see Article 18 of the Spanish Constitution).

Finally, the court compared this case with established case law from the European Court of Human Rights, particularly the well-known "Barbulescu doctrine", as well as precedent from the Spanish Supreme Court and the Constitutional Court ruling of October 7, 2013 (ruling No. 2907/2011). These cases established that an employee must be able to foresee the possibility of the employer exercising its legal right to monitor communications and, therefore, cannot claim a reasonable expectation of privacy when explicitly warned that communications may be subject to oversight.

However, in the present case, the court concluded that the absence of an explicit ban on using the corporate mobile phone for personal purposes created a reasonable expectation of privacy for the worker. The company was found to have committed a very serious violation under the Law on Offenses and Sanctions in the Social Order (*Ley sobre Infracciones y Sanciones en el Orden Social*).

The violation of the worker's right to privacy, as declared in STSJ No. 1850/2024, entitled him to compensation for damages suffered, particularly for moral damages, in the amount of €7,501, as established under Articles 182.1(d) and 183 LRJS.

- **STSJ Catalonia (Social Chamber) No. 6779/2024, of September 23, p. Judge González Calvet**

  Subject: Validity of security camera recordings obtained without prior notification or consent from employees and the Works Council.

In this ruling, the High Court of Justice of Catalonia (*Tribunal Superior de Justicia de Cataluña*) dismissed the appeal for reversal filed by the legal representatives of an employee against the judgment issued on October 27, 2023, by Social Court No. 1 of Terrassa (*Juzgado de lo Social n.º 1 de Terrassa*, case No. 377/2022). The court upheld the first-instance decision, which had rejected the employee's claim and confirmed the validity of the disciplinary dismissal.

The case involved a justified disciplinary dismissal for **copper theft** at a company that had used security camera footage to prove the theft. The dispute centered on whether the recordings were lawfully obtained.

The company **installed cameras** in the galvanizing section—where copper containers were stored—after detecting an unusually high copper consumption that did not correspond with the plant's production levels. Suspecting employee theft, the company implemented video surveillance to identify those responsible.

The dismissed employee argued that the measure violated his right to privacy because **the company had installed video surveillance camera**s in the galvanizing section **without notifying employees or the Works Council**. The appellant claimed this violated his rights to privacy and personal image, as protected under Article 18.1 of the Spanish Constitution, since the recordings were obtained without prior knowledge or consent. He further contended that the company had violated Article 89.1 of the Organic Law on Personal Data Protection and Digital

Rights Guarantees (*Ley Orgánica de Protección de los Datos Personales y Garantía de los Derechos Digitales*), which requires informing employees about workplace surveillance:

"Employers must provide prior, express, clear, and concise notification to employees or public workers and, where applicable, their representatives, regarding this measure."

The company justified the measure, citing the discrepancy between copper consumption and production levels and emphasizing that the cameras were not hidden, thereby minimizing any intrusion into employees' privacy. Additionally, it argued that signs indicating security cameras were already present at the entrance, warehouse section, central hallway of the ground floor, and locker room entrance.

The court analyzed the conflict between the employer's right to monitor employees (Article 20.3 of the Workers' Statute) and the employee's right to privacy (Article 18 of the Spanish Constitution). While the court acknowledged that there was no explicit notification in the galvanizing section, it noted that the cameras were visible from the ground, meaning their presence was not entirely covert or "surprising."

The court ruled that the measure was: appropriate, as it effectively identified those responsible for the theft; necessary, as there was no less intrusive alternative that could provide the same effectiveness in identifying the culprits; and proportionate, as the benefits of the measure outweighed any harm to the worker's privacy.

Consequently, the High Court of Justice upheld the first-instance ruling, which had declared the dismissal justified and validated the security camera recordings. The judgment reaffirmed the balance between employers' monitoring rights and employees' fundamental rights, holding that non-hidden workplace surveillance is lawful for crime prevention purposes, provided it meets the criteria of appropriateness, necessity, and proportionality.

3. Courts of first instance

➢ Social Court No. 11 of Seville, of May 14, 2024, p. Judge Juan-Bosco Rite Zambrano

Subject: Legal protection framework for whistleblowers.

This ruling from Social Court No. 11 of Seville, dated May 14, 2024, and issued by Presiding Judge Juan-Bosco Rite Zambrano, declared the nullity of the dismissal of a worker, ruling that the

termination of his contract constituted a direct act of retaliation for reporting corrupt practices within his company.

The claimant, using the company's compliance and ethics channels, had reported that his immediate superior had unlawfully obtained technical specification documents before their official publication, giving the company an unfair competitive advantage in the awarding of public contracts. The employer subsequently dismissed the worker, citing organizational and production-related reasons but took no action against the accused superior, claiming a lack of conclusive evidence regarding his wrongdoing.

The court determined that the worker's dismissal was directly linked to his whistleblowing, thereby violating his **right to protection from retaliation** (*garantía de indemnidad*), as established in Article 24.1 of the Spanish Constitution, EU Directive 2019/1937 of the European Parliament and Council, and—currently—the Law 2/2023 on the Protection of Whistleblowers.

The judge found that, **despite the complaint being anonymous**, the company's internal investigator had access to information that **allowed the whistleblower to be identified**, ultimately leading to his dismissal. The court classified the dismissal as **retaliatory**, rendering it null and void under Article 55.5 of the Workers' Statute. Additionally, it highlighted that the company failed to justify the organizational grounds cited for the dismissal, as required by Article 52(c) of the Workers' Statute, further supporting the ruling of absolute nullity.

As a result, the Social Court ordered the **immediate reinstatement of the worker** and the payment of all outstanding wages, along with €15,000 in compensation for moral damages.

The judge deemed it necessary to double the standard compensation amount, ensuring not only that the worker was adequately compensated for the moral damage suffered, but also that **future corporate misconduct violating fundamental rights would be discouraged.** This was in line with Directive 2019/1937, which explicitly aims to prevent retaliatory actions against whistleblowers.

Although Law 2/2023, which transposes the Directive into Spanish law, was not yet in force at the time of the events, the transposition deadline had already expired, meaning that whistleblower protection had to be upheld in accordance with European law.