# From Safeguard to Surveillance Justification: The Transformation of the Right to be Informed in ECtHR Jurisprudence

Maéva El Bouchikhi

*Public Law and Regulation, Swiss Graduate School of Public Administration (IDHEAP), University of Lausanne*

*Author accepted manuscript. The final version is published in the European Labour Law Journal (2026),*
*https://doi.org/10.1177/20319525261498423*

Abstract:

This article examines the evolving function of the right to be informed in regulating workplace surveillance through a systematic analysis of the European Court of Human Rights' case law. It asks whether workers' prior information continues to operate as a meaningful safeguard against employer monitoring or whether its function within the Court's reasoning has progressively changed. While the Court continues formally to rely on the criterion established in *Bărbulescu v Romania*, a systematic examination of its subsequent case law reveals that workers' information has lost much of its protective force. Once a safeguard whose absence weighed heavily against employers, information is increasingly treated as one criterion among others within the Court's proportionality assessment, readily outweighed by expanding managerial and property-based interests and, once formally satisfied, capable of supporting the very monitoring it was meant to constrain.

The article traces this evolution through two interconnected developments. First, the circumstances in which employers may engage in covert surveillance have progressively broadened. Second, increasingly intrusive monitoring practices have been considered compatible with Article 8 despite limited, ambiguous, or delayed information being provided to workers. As a result, the threshold for complying with transparency obligations has gradually been reduced to a minimal notification requirement. Transparency therefore functions less as an autonomous safeguard protecting workers *ex ante* and increasingly as part of the Court's justificatory reasoning when assessing the compatibility of workplace surveillance with Article 8.

On this basis, the article identifies a transformation in the legal function assigned to workers' information. Prior information progressively ceases to operate as an *ex ante* constraint on monitoring and instead becomes one element within the Court's proportionality assessment capable of supporting its *ex post* justification. Workers' information and transparency requirements, intended to mitigate structural power asymmetries in the employment relationship, may therefore contribute to legitimising workplace surveillance when reduced to formal transparency obligations.

By reconstructing this jurisprudential evolution, the article offers a new explanation for the "*more surveillance approach*" identified in recent scholarship and shows that this development reflects a broader transformation in the Court's reasoning rather than a position confined to a limited number of cases. It further situates this evolution within a European and international regulatory landscape that increasingly reinforces transparency obligations and workers' informational rights. Against this background, the article argues that the effectiveness of informational safeguards ultimately depends less on their formal recognition than on the weight courts are willing to accord them within their proportionality assessment. As new regulatory instruments reinforce transparency and participatory safeguards for workers, the Court may increasingly be called upon to restore the weight attributed to workers' right to be informed of monitoring and the threshold of transparency expected from employers within Article 8 balancing.

Keywords: Workplace Surveillance; European Court of Human Rights; Transparency; Workers' Privacy; Information Right; Article 8; Public Interference; Algorithmic Management;

# 1. Introduction

Digital technologies and algorithmic management have profoundly transformed the organisation of work and the means through which employers monitor employees' activities. Email monitoring, video surveillance, and increasingly data-driven monitoring systems allow employers to observe, record and evaluate workers' behaviour with unprecedented precision. These developments raise important concerns for workers' fundamental rights, particularly their right to respect for private life under Article 8 of the European Convention on Human Rights (ECHR). As labour law scholars have long emphasised, the employment relationship is characterised by structural power asymmetries between employers and workers, making legal safeguards essential to prevent the expansion of intrusive workplace monitoring.[1]

The European Court of Human Rights (ECtHR) has progressively developed a body of case law addressing workplace surveillance under Article 8 of the Convention. The Court has recognised that workers do not lose their right to private life when entering the workplace and has sought to balance this right against employers' managerial interests.[2] Within this balancing exercise, the question of workers' information regarding monitoring practices gradually emerged as a key procedural safeguard. This development reached a turning point in the Grand Chamber judgment in *Bărbulescu v. Romania*, where the Court established a structured set of criteria to guide its proportionality analysis, including the requirement that workers be informed of the possibility and scope of the monitoring.

In broader scholarship debates, such workers' informational rights actually refer to two facets of the same coin: employers' transparency obligation and workers' right to information. On the one hand, *transparency* refers to the employer's duty to inform workers about the existence, purpose and scope of the monitoring.[3] On the other hand*, workers' right to information* refers to the individual and collective ability to access relevant information about monitoring practices and the data being collected, enabling the workforce to understand, contest, or challenge potential interference with their private lives. Together, these mechanisms aim to mitigate the structural power imbalance inherent in employment relationships and, beyond the Court's recognition,[4] have been gradually reinforced in European and international frameworks in the age of the digital economy and the rise of algorithmic management.[5]

However, recent case law has raised important questions about the contemporary protective function of workers' prior information. Despite the formal persistence of *Bărbulescu's* criteria in its assessment, successive cases have systematically resulted in findings of no violation of Article 8, despite the sensitivity of the data being collected or the increasing intrusiveness of the technologies used to monitor the workforce. Recent scholarship suggests that the Court now adopts, since *Florindo'*s judgment, what the authors called a "*more surveillance approach*".[6] This evolution raises questions in a context where international and European regulatory frameworks increasingly attempt to protect workers in an

[1] Mangan, D., *From Monitoring of the Workplace to Surveillance of the Workforce,* in Tamás Gyulavári and Emanuele Menegatti (ed.), *Decent Work in the Digital Age - European and Comparative Perspectives*, Bloomsbury, 2022.
[2] Hendrickx, F., *Regulating Worker Privacy and Data Protection: Exploring the Global Source System*, in Tamás Gyulavári and Emanuele Menegatti (ed.), *Decent Work in the Digital Age - European and Comparative Perspectives*, Bloomsbury, 2022; Novitz, T., *Regulating Workplace Technology - Extending the Agenda*, Oxford University Press, 2017.
[3] This facet is alternatively called "*right to know*" or "*right to be informed*", creating semantic confusion with workers' information rights.
[4] Molè, M., *The Internet of Things and Artificial Intelligence as Workplace Supervisors: Explaining and Understanding the New Surveillance to Employees Beyond Art. 8 ECHR*, Italian Labour Law e-Journal 15(2), 2022.
[5] The broader evolution of workers' informational rights in European and international labour regulation is examined within the author's PhD thesis (forthcoming). For instance, the ILO Convention on decent work in the digital economy extends the right to information to non-traditional workers under Article 13.
[6] Molè, M., & Mangan, D., '*Just more surveillance': The ECtHR and workplace monitoring*, European Labour Law Journal, 14(4), 2023, pp. 694-700.

increasingly digitalised workplace, notably through the strengthening of employers' transparency obligations and workers' informational rights.[7] Against this background, this article aims to investigate how workers' right to be informed of workplace monitoring has evolved within the Court's jurisprudence and whether it continues to operate as an effective safeguard for workers' right to privacy.

Through a doctrinal analysis of the Court's case law, the article argues that the role of workers' information within the proportionality analysis has gradually shifted, losing its protective function. This evolution can be shown through two related developments and observations. First, from the earliest case law to *Bărbulescu v. Romania*, workers' information gradually gained importance until being clearly consolidated as one of the criteria taken into account by the Court in its assessment of the lawfulness of monitoring techniques at the workplace. However, in its subsequent case law, employers' obligation to inform workers has increasingly declined, easily being overridden by employers' managerial interests, and based on broader rhetoric, managerial objectives, and mere suspicion of any employees' wrongdoing. Second, even when workers are informed, the threshold for companies to comply with their transparency requirement before the Court undermined its ability to protect against increasing intrusive surveillance. Satisfied by a mere notification, without systematically assessing the quality and extent of information being provided to workers concerning the monitoring, transparency operates more as a formality or compliance check than a substantive safeguard, thus ceasing to constrain *ex ante* intensive monitoring techniques and sometimes instead participating in supporting their justification *a posteriori* regardless of the intrusiveness of the technology being used.

Consequently, this analysis bears several contributions. First, it situates the "*more surveillance approach*" within a broader and earlier jurisprudential trajectory. If recent scholarship has already theorised the "more surveillance approach" adopted by the Court,[8] this historical reconstruction shows that this Court's shift was gradual rather than sudden, as such evolution was already visible in all the successive decisions following *Bărbulescu*, notably through the lens of the weight attributed to workers' information in the Court's assessment of the proportionality principle. Second, it contributes to broader debates on the "*transparency paradox*"[9] and the limits of transparency-only-based safeguards as the main response to society's digitalisation. Originally intended to protect workers, it progressively contributes to legitimising workplace surveillance if not taken into account, reduced to a mere information notification, or mobilised to subject workers to more technological scrutiny, within the Court's proportionality assessment. Third, it situates its results within broader European and international regulatory frameworks that increasingly reinforce employers' transparency obligations and workers' informational rights in response to workplace digitalisation and algorithmic management.[10] Consequently, this article argues that the Court may increasingly be called upon to restore the weight attributed to workers' prior information in its assessment in the light of contemporary evolving regulatory developments in order to protect what remains of workers' right to privacy in an increasingly algorithmised workplace.

---

[7] El Bouchikhi, M., *'The Janus Face of Occupational Safety and Health, Between Protection and Surveillance in the Digital Workplace'*, PhD Thesis, University of Lausanne (*forthcoming*).

[8] Molè, M., & Mangan, D., (n 6).

[9] The notion of "*transparency paradox*" is used here in a legal sense to describe situations where transparency requirements intended to enhance protection may instead facilitate the expansion or legitimisation of surveillance practices. While the transparency paradox has been discussed in organisational and privacy scholarship, notably by Bernstein in relation to workers' behavioural adaptations to monitoring, this article adopts a perspective closer to Nissenbaum's analysis of the limits of transparency-based privacy safeguards in the employment context.

[10] See, for instance, European Parliament resolution of 17 December 2025 with recommendations to the Commission on digitalisation, artificial intelligence and algorithmic management in the workplace - shaping the future of work (2025/2080(INL)); See also the ILO Convention on decent work in the platform economy.

# 2. The Evolution of the Right to be Informed in ECtHR Workplace Surveillance Jurisprudence

Over the past three decades, the ECtHR's case law on workplace surveillance and workers' right to respect for private life under Article 8 of the Convention has progressively expanded the scope of protection. Early judgments generally adopted a protective approach, frequently finding violations of Article 8 where monitoring practices interfered with workers' private lives in the absence of sufficient legal safeguards. As illustrated in Table 1, this protective approach largely characterised the Court's case law until the Grand Chamber judgment in *Bărbulescu v. Romania*.

| **Year** | **Case** | **Grand/Chamber** | **Violation** | **Unanimous vote or thin majority** | **Separate opinion(s)** | **Public interference or Private competing interests** |
|---|---|---|---|---|---|---|
| 2024 | *Tena Arregui v. Spain* | *Chamber* | No | Unanimity | No | Public |
| 2022 | *Florindo de Almeida Vasconcelos Gramaxo v. Portugal* | *Chamber* | No | Four against three | Joint Dissenting Opinion | Private |
| 2022 | *Adomaitis v. Lithuania* | *Chamber* | No | Six against one | Partly Dissenting Opinion | Public |
| 2019 | *López Ribalda and Others v. Spain* | *Third and Grand Chamber* | No | Fourteen against three | Joint Dissenting Opinion | Private |
| 2018 | *Libert v. France* | *Chamber* | No | Unanimity | No | Public |
| 2017 | *Antovic and Mirkovic v. Montenegro* | *Chamber* | Yes | Four against three | Joint Concurring Opinion and Joint Dissenting Opinion | Public |
| 2017 | *Bărbulescu v. Romania* | *Grand Chamber* | Yes | Eleven against six | Partly Dissenting Opinion and Joint Dissenting Opinion | Private |
| 2010 | *Köpke v. Germany* | *Chamber* | Case inadmissible | Unanimity | No | Private |
| 2007 | *Copland v. United-Kingdom* | *Chamber* | Yes | Unanimity | No | Public |
| 1997 | *Halford v. United-Kingdom* | *Chamber* | Yes | Unanimity | Dissenting Opinion | Public |
| 1992 | *Niemietz v. Germany* | *Chamber* | Yes | Unanimity | No | Public |

*Table 1. Reconstruction of ECtHR's workplace surveillance case law.*

However, the overview provided in this table reveals a subsequent shift in the Court's jurisprudence. From *Libert v. France* onwards, and more clearly following the Grand Chamber judgment in *López Ribalda v. Spain*, the Court systematically concluded that monitoring practices may be compatible with Article 8. The fact that both *Bărbulescu* and *López Ribalda* were delivered by the Grand Chamber is particularly significant, as such judgments are generally understood as clarifying and structuring the Court's case law and show a paradigm shift in the Court's assessment.

A closer examination of the cases nevertheless suggests that this evolution is not necessarily characterised by a clear consensus within the Court compared to its initial case law. First, the table shows that since *Bărbulescu*, many recent judgments have been adopted by narrow majorities and have been accompanied by dissenting opinions advocating for finding a violation under Article 8,[11] and second, that frequently dissenting judges question the Court's reasoning, particularly with regard to prior workers' information in the proportionality assessment of the monitoring or the interference.[12]

Against this background, a more detailed examination of the Court's reasoning is necessary. The following sections, therefore, reconstruct how workers' information progressively emerged and was consolidated as a protective safeguard within the Court's earlier jurisprudence until *Bărbulescu,* before examining how its function has progressively evolved and been diluted post *López Ribalda, contributing* to the normalisation of surveillance practices.

## 2.1 From *Niemietz* to *Bărbulescu* - The Emergence and Consolidation of Workers' Informational Safeguard

This section reconstructs how the Court's jurisprudence on the right to privacy in the case of workplace surveillance moved from negative obligations restraining public authorities' interference to positive obligations in private employment, and how, along this path, worker's right to be informed crystallised into a central procedural safeguard.

### *a) Public Authority Interference and the Early Signals of Workers' Informational Protection*

Since the 1990s, the ECtHR has increasingly protected workers' right to privacy, even in professional contexts, notably to protect individuals against interference by public authorities.[13] First, in *Niemietz*, a lawyer's office was searched as part of criminal proceedings against a third party. In this case, the Court developed a broad definition of the right to privacy in a professional context[14]. In this context, the Court ruled that States must refrain from interfering with an individual's right to private life. If interference occurs, it has to be in accordance with the law, pursue a legitimate aim, and be *"necessary in a*

[11] It is important to note that in *Halford v. United Kingdom, Judge Russo joined a dissenting opinion expressing that the Court should also have ruled for a violation of Article 8,* not only for the interception of the applicant's professional phone call but also of her home phone calls. On the contrary, dissenting opinions in successive case law argued for a violation of Article 8, while the majority ruled on non-violation.
[12] Such dissenting opinions are more precisely discussed in the discussion below.
[13] ECtHR, *Niemietz v. Germany*, n°13710/88, 16 December 1992, §31.
[14] *Ibid*., §29.

*democratic society".*[15] In this case, the Court found that the search of the applicant's office constituted an interference and a violation under Article 8 of the Convention as it was not in accordance with the law and based more on *suspicions than facts,* even though the aim of criminal proceedings was found to be a legitimate purpose.

The Court gradually extended such protection against public interference to cases involving interception of workers' communications and correspondence. In *Halford*, the applicant saw her phone calls (professional and private) being intercepted by her employer, the Merseyside Police headquarters. They tried to obtain information to use against her in the framework of her complaint against discrimination. The Court, similarly to *Niemietz,* concluded that the conversations held by Ms Halford on her office telephones fell within the scope of the notions of "*private life*" and "*correspondence*"[16] and that there was a reasonable likelihood that calls made by the applicant from her office were intercepted. Such interception constituted an "*interference by public authority*" within the meaning of Article 8 para. 2 of the Convention[17] and was found not in accordance with the law, as domestic law "*did not provide any regulation of interceptions of calls made on telecommunications systems outside the public network*".[18] The Court concluded there had been a violation of Article 8 in relation to the interception of calls made on Ms. Halford's office telephones.[19]

The criteria developed in the context of the interception of communications were later similarly applied in a case involving the monitoring by public authorities of an employee's internet and communications. Ms. *Copland* was a personal assistant to the college's principal. Following the appointment of a new deputy principal, her telephone, email and internet usage were monitored to "*ascertain whether the applicant was making excessive use of College facilities for personal purposes*".[20] In this case, the Court considered that the collection and storage of personal information relating to the applicant's telephone, email and Internet usage, *without her knowledge,* amounted to an interference with her right to respect for private life and correspondence within the meaning of Article 8[21]. The Court established that the interference constituted a violation of Article 8 and domestic laws did not provide adequate protection to the applicants.[22]

In these cases, the Court not only paved the way for workers' protection against public authorities but also began to recognise workers' information as an important criterion in the case of workplace surveillance. It is first noticeable in *Halford*, where the British government claimed that an employer could monitor and intercept its workforce's communications without informing them.[23] While the Court remained silent on that aspect, the Article 29 Working Party,[24] a European advisory body, echoed part of the legal doctrine at that time that implied that such silence meant that if a worker was warned in advance about the possibility of his/her communications being intercepted, then they may lose their expectation of privacy and that such interference would not constitute a violation under Article 8[25]. On

---

[15] *Ibid*., §37.
[16] ECtHR, *Halford v. the United Kingdom*, n°20605/92, 25 June 1997, §46.
[17] *Ibid*., §48.
[18] *Ibid*., §50.
[19] *Ibid*., §§51 and 60: While telephone conversations made from home are covered as well by the notions of private life and correspondence, the Court did not find a violation of Article 8 due to the lack of evidence.
[20] ECtHR, *Copland v. UK*, n°62617/00, 3 April 2007, §10.
[21] *Ibid*., §44.
[22] *Ibid*., §51.
[23] ECtHR, *Halford* (n 16) §43: "*The Government submitted that telephone calls made by Ms. Halford from her workplace fell outside the protection of Article 8, because she could have had no reasonable expectation of privacy in relation to them. At the hearing before the Court, counsel for the Government expressed the view that an employer should in principle, without the prior knowledge of the employee, be able to monitor calls made by the latter on telephones provided by the employer*."
[24] Article 29 Working Party (WP 29) was an independent European advisory body on data protection and privacy established under Article 29 of the Directive 95/46/EC until 25 May 2018 (entry into force of the GDPR).
[25] WP 29, Working document on the surveillance of electronic communications in the workplace, 29 May 2002, pp.8-9.

the contrary, Article 29 shared the view that workers' advance notice was insufficient to justify any infringement of their data protection rights, even if such information might reduce workers' legitimate expectations of privacy[26]. The Court explicitly confirmed the importance of workers' information in *Copland*, paying particular attention to whether or not the employee was informed of the interference[27]. In sum, the Court gradually began to *signal* that knowledge and foreseeability matter, and that an employer's monitoring "*without [the] knowledge*"[28] of their workforce constitutes an interference and ultimately a violation of their right to privacy.

*b) Private Employment Protection and the Consolidation of the Informational Safeguard*

The Court gradually extended workers' right to private life beyond the State's negative obligations not to interfere, to the recognition of positive obligations in the context of private employment. During the extension of this protection, the Court formally recognised workers' information as a key procedural safeguard against monitoring.

In *Köpke*, a supermarket had deployed camera surveillance, with the help of a detective agency, due to suspicion that some employees were stealing from the store. Following the analysis of the footage, an employee was dismissed. While this case was found inadmissible, the Court still provided insights regarding the State's positive obligations regarding the interests at stake between an employee's right to private life and the employer's property rights. The Court explained that if Article 8 aims to protect individuals against arbitrary interference by the public authorities, it "*does not merely compel the State to abstain from such interference*". States also have positive obligations inherent in ensuring effective respect for private life and in adopting *measures* designed to secure such a right in the sphere of relations between individuals. Their positive obligations could, for instance, consist of legislative provisions providing a framework for reconciling competing interests. Applied to this case, the Court had to analyse whether the national authorities had struck a fair balance between the applicant's right to her private life and the employer's interest in the protection of its property rights guaranteed under Article 1 of Protocol no. 1 of the Convention, despite the large margin of appreciation of the State.

Given this heightened suspicion of theft, the Court was satisfied that respect for private life was still adequately protected by domestic courts[29]. The Court explained that the employer was authorised to set up video surveillance if "*there was a prior substantiated suspicion that the employee had committed an offence and if such surveillance was altogether proportionate to the aim of investigating the offence at issue*". If covert surveillance must be considered as a "*considerable intrusion"* into an employee's private life, employees still have the obligation, under the employment contract, to perform the work. In this regard, the Court found that the video surveillance was carried out with guarantees: it was deployed after losses were detected, limited in time and to a specific area, accessible by a limited number of persons, and for the purpose of terminating the employment relationship. Thus, this interference was "*restricted to what was necessary to achieve the aims pursued*" and there would have been no other

[26] *Ibid.*
[27] ECtHR*, Copland v. UK*, n°62617/00, 3 April 2007, §44.
[28] *Ibid.*
[29] ECtHR*, Köpke v. Germany,* n°420/07, 5 October 2010: The Court took the view that "*covert video surveillance at the workplace following substantiated suspicions of theft does not concern a person's private life to an extent which is comparable to the affection of essential aspects of private life by grave acts in respect of which the Court has considered protection by legislative provisions indispensable*".

equally effective means to protect the employer's property rights which would have interfered to a lesser extent with the applicant's right to respect for her private life.[30]

Outside of the case of legitimate suspicion, an employer's legitimate surveillance cannot be unlimited. Already in *Köpke*, the Court warned that, despite its reasoning aligning with national courts that found a non-violation of Article 8, a different weight might be given to the competing interests in the future, as intrusions into workers' private life were made possible by new and more "*sophisticated technologies*".[31] In this regard, the Court's landmark ruling in *Bărbulescu* established clear criteria to be taken into account[32] when analysing the State's positive obligations in cases of interference with workers' right to private life through monitoring technologies.[33] Similarly to *Copland*, an employee's communications, internet use, and personal messages to his brother and fiancée have been monitored, compiled and recorded. The employer sought to demonstrate that the applicant had used the internet for personal purposes, which constituted a breach of internal regulations[34] that led to his dismissal. In this case, the applicant was not suspected of any misconduct or theft, but the employer wanted to verify that its workforce was not using the company's professional facilities for personal purposes, in accordance with its internal regulations and to ensure the smooth running of the company.

The Court ruled that employers' legitimate surveillance and internal regulations cannot reduce employees' privacy to zero. In *Bărbulescu*, the Court questioned the extent to which the employer's internal restrictive regulations left employees with a reasonable expectation of privacy. According to the Court, "*an employer's instructions cannot reduce private social life in the workplace to zero. Respect for private life and for the privacy of correspondence continues to exist, even if these may be restricted in so far as necessary*"[35]. In the present case, it meant examining whether an "*outright ban on personal internet use entitled the employer to monitor its employees, and whether the employer had to give reasons for such monitoring*".[36] The Court also had to analyse the responsibility of national authorities for failing to secure the applicant's enjoyment of the right to private life.[37] In its assessment, the Court recalls that, at the time, there was no European consensus on this issue[38] and that contracting States must be granted a wide margin of appreciation.[39] However, this "*discretion […] in this field cannot be unlimited*" as domestic authorities should ensure that the introduction of monitoring techniques, irrespective of the extent and duration of such measures, is accompanied by adequate and sufficient safeguards.[40]

Aware of the "*rapid developments in this area*", meaning the increasing deployment of monitoring techniques at the workplace, the Court considered that procedural guarantees were essential.[41] Consequently, the following factors when assessing the necessity of the monitoring should be taken into consideration: a) whether *the employee has been notified* of the possibility of the monitoring, and of the implementation of such measure;[42] b) the *extent* of the monitoring and the *degree of intrusion* into the

[30] The case was found inadmissible. However, the Court agreed with the domestic courts' analysis.
[31] ECtHR*, Köpke v. Germany,* (n 29), p.13.
[32] ECtHR, *Bărbulescu v. Romania*, n°61496/08, 5 September 2017, §121.
[33] *Ibid.* §111.
[34] ECHR, *Copland*, (n 20), §18.
[35] ECtHR, *Bărbulescu v. Romania,* (n 32)*,* §80.
[36] *Ibid*, §86.
[37] *Ibid.*
[38] *Ibid*., §118: the judgment states that at that time, only a few Member States had explicitly regulated the exercise by employees of their right to respect for their private life and correspondence in the workplace.
[39] *Ibid*., §119.
[40] *Ibid*., §120.
[41] *Ibid*., §121.
[42] *Ibid*., §121(i): the notification should normally be clear about the nature of the monitoring and be given in advance.

employee's privacy;[43] c) whether the employer has provided *legitimate reasons to justify monitoring the communications* and accessing their actual content;[44] d) whether it would have been possible to establish a monitoring system based on *less intrusive methods and measures*;[45] e) the *consequences* of the monitoring for the employee and notably the results of such monitoring operation to achieve the declared aim of the measures;[46] and f) whether the *employee had been provided with adequate safeguards*, especially if monitoring operations were of intrusive nature.[47] Applied to this case, it was found that national authorities failed to strike a fair balance between the interests at stake, thereby violating Article 8.[48] The Court concluded that national courts did not examine the degree of intrusion into the applicant's privacy,[49] nor the legitimate reasons to justify the monitoring of the communications,[50] the seriousness of the consequences of the monitoring and of the disciplinary proceedings,[51] or whether the aim could have been pursued with less intrusive methods than accessing the actual contents of the applicant's communications.[52]

The Court paid particular attention to the first criterion and to whether the applicant had been informed and had received prior notification before the monitoring occurred.[53] If the applicant was informed of the ban on personal internet use, it is unclear whether he was informed *prior* to the monitoring of his communications. For the Court, national authorities omitted to ascertain whether the applicant had been *informed* before it began,[54] as well as its extent and nature, including the employer's possibility of accessing the actual *contents* of his communications.[55] According to them, domestic courts failed to determine whether the applicant received prior notice that his communications might be monitored, whether he was informed of the nature and extent of the monitoring and the degree of intrusion into his private life and correspondence, and whether the communications might have been accessed without his knowledge.[56]

Consequently, *Bărbulescu* firmly established workers' information right as a clear procedural guarantee in the Court's assessment. This consolidation is important as it enables workers to challenge illegitimate surveillance, as illustrated a few months later in *Antovic and Mirkovic v. Montenegro*. Two university professors complained about the deployment of seven video surveillance cameras in auditoriums. The applicants deplored their lack of control over such a system, deployed, according to the Dean, to ensure the security of the school and its people, as well as the "*surveillance of teaching*". The Court recalled that video surveillance of an employee, covert or not, must be considered a considerable intrusion into an employee's private life and should occur in accordance with the law, pursue one or more legitimate

[43] *Ibid*., §121(ii): The Court makes the distinction between the monitoring of the flow of communications and their content as well as whether the monitoring was limited in time and the number of people who had access to the results. The Court also specifies that the same applies to spatial limits to the monitoring; ECtHR, *Köpke v. Germany*, *quoted above*.
[44] *Ibid*., §121(iii): the Court specified that since monitoring of the content of communications is by nature a distinctly more invasive method, it requires "*weightier justification*".
[45] *Ibid*., §121(iv): in this case, it means assessing whether it would have been possible to deploy measures other than directly accessing the content of the employee's communications, or achieve the same result without directly accessing the full contents of the communications.
[46] *Ibid*., §121(v).
[47] *Ibid*., §121(vi): such safeguards should ensure that the employer cannot access the actual content of communications unless the employee has been notified in advance.
[48] *Ibid*, §141.
[49] *Ibid*., §134.
[50] *Ibid*., §135: the County Court has *"touched"* this question in its initial ruling, the employer justified such monitoring by the need to avoid IT systems being damaged in the event of illegal activities committed by the employee in cyberspace and to avoid company's trade secrets being disclosed.
[51] *Ibid*., §137.
[52] *Ibid*.
[53] *Ibid*., §133.
[54] *Ibid*., §§77-78.
[55] *Ibid*, more particularly due to the intimate nature of the communications with his fiancee.
[56] *Ibid*, §140.

aims to which that provision refers, and be necessary in a democratic society to achieve that aim. Domestic courts did not examine the first condition as they did not consider surveillance to be a public interference in the first place. However, the Personal Data Protection Agency[57] explicitly held that it was not in accordance with the law,[58] and such analysis was joined by the Court. According to them, if video surveillance was introduced to ensure the security of the University, the surveillance of teaching *was "not provided for by the law at all as a ground for video surveillance*".[59] They concluded that the interference constituted a sufficient violation under Article 8 and that it was not necessary to examine the other requirements of the second paragraph.[60]

Workers' information and ability to challenge are even more important when two legitimate purposes are invoked to deploy monitoring techniques, or when there is a risk of data reuse. In *Antovic*, while it was claimed to be deployed for mainly security purposes, surveillance of teaching activities was still put forward as a secondary purpose. According to Judges Vucinic and Lemmens, in their concurring opinions, this purpose was indeed pursued, as the Dean had access to the tapes and the camera was not placed at the entrances and exits of the building but within the auditoria themselves.[61] In these circumstances, the professors' notification of the camera's deployment enabled them to challenge the decision, regain control of their data,[62] and have the system removed within a limited time following the decision.[63]

In sum, by the time of *Bărbulescu* and *Antovic*, the Court had a particular protective and restrictive view on the circumstances under which covert or not monitoring could operate, and prior specific notice/information of an interference/monitoring served as an *ex ante* constraint against illegitimate surveillance. However, the following section underscores the Court's paradigm shift, demonstrating how subsequent judgments recast information and employers' transparency as a flexible, context-dependent factor, facilitating a broader normalisation of workplace surveillance.

## 2.2 To *López Ribalda* and Onwards: The Progressive Dilution of the Right to be Informed

Despite the gradual expansion of workers' privacy protection in earlier case law, the judgments delivered after 2017 reveal a different trajectory. All subsequent cases that were brought before the Court resulted in a finding of no violation of Article 8.[64] This chronological evolution raises the question of whether the Court was confronted only with cases involving a grave suspicion of serious misconduct, breach of employment obligations, or breach of any internal policy, or whether it reflects a deeper lowering of the level of protection afforded to workers' private life, and in particular their right to be informed.

While the Court's earlier case law progressively strengthened workers' informational safeguards, the judgments delivered after *Bărbulescu* reveal a different trajectory. Although the Court continues to refer to the criteria established in 2017, the role attributed to workers' information in the proportionality

[57] The national data protection authority.
[58] ECtHR, *Antovic and Mirkovic v. Montenegro*, 28 November 2017, n°70838/13, §57.
[59] *Ibid.* §59.
[60] *Ibid.*, §60.
[61] *Ibid.*, Joint concurring opinion of judges Vucinic and Lemmens, §4.
[62] Applicants complained on the ground of their lack of control over their personal data.
[63] Applicants were informed in February 2011, they complained in March, a decision was issued in April, and they were notified by the School in January 2012, when the camera had been removed.
[64] See Table 1.

assessment appears to have changed progressively. Rather than operating as a central safeguard structuring the legality of monitoring practices, transparency increasingly functions as a contextual factor that may be outweighed by other considerations.

### *a) From "Substantiated Suspicion" to Routine Surveillance: Information as a Procedural Right to a Mere Guarantee*

In *Libert,*[65] an employee of the French national railway company (SNCF) was dismissed following the discovery, in his absence, of a massive quantity of pornographic images. The applicant argued that such interference was disproportionate and unlawful because the adjective term was "*personal*" in the hard disk's default name rather than "*private*". The company's internal rules allowed its staff to *occasionally* use their computer facilities for private purposes. The Court recalled that non-professional data, clearly identified as private, stored by an employee on a computer, might be deemed to relate to his private life. In this case, given that the applicant's files had been opened on his work computer, and *without his knowledge*, while he was absent, there might have been an interference with his right to respect for private life. The question was whether those files had been clearly identified as personal. The Court recalled the French Cour de Cassation's case law[66] holding that unless there was a serious risk, or in exceptional circumstances, employers could only open files identified by an employee as personal in their presence, physically or by phone.[67] According to the employer, the interference was intended to safeguard the protection and "*the rights of others*" following the colleague's alert about the discovery of the files. For the Court, the domestic authorities had not overstepped their margin of appreciation and found no violation of Article 8.

This case began to illustrate the shift in the Court's paradigm, first, on the grounds under which an employer might interfere with an employee's right to private life. The French government argued that the interference aimed to protect the "*rights (...) of others*",[68] namely the employer's, and the Court agreed that an employer "*can legitimately want ensuring employees are using the computer facilities placed at their disposal for the purpose of carrying out their duties in line with their contractual obligations and the applicable regulations*".[69] In this case, such a ground is slightly broader compared with its earlier rulings. Previously, the Court recognised that if the employer might have a legitimate interest in ensuring the "*smooth running of the company*",[70] notably through mechanisms to check whether employees were performing their professional duties adequately and with the necessary diligence,[71] such interference was not unlimited. It should be based on facts, not suspicion,[72] especially to avoid abuse by public authorities,[73] and as technologies become increasingly intrusive, it requires a weightier justification.[74] Such justification should demonstrate that the employee committed a particular offence, breached his/her contract, or caused harm to the company's interests or rights. If it is not unusual in previous cases that employers deployed surveillance to determine if employees were using

[65] ECtHR, *Libert v. France*, n°588/13, 22 February 2018.
[66] The highest court of the French judiciary system.
[67] Alternatively, after calling him or her to their office.
[68] ECtHR, *Libert v. France*, (n 65), §46: translation from French by the author.
[69] *Ibid*.
[70] ECtHR, *Bărbulescu v. Romania*, (n 32)*,* §*127.*
[71] *Ibid*.
[72] ECtHR, *Niemietz v. Germany*, (n 13).
[73] ECtHR, *Halford* (n 16) and Copland (n 20).
[74] ECtHR, *Bărbulescu v. Romania*, (n 32), §121(iii).

*"professional facilities in an excessive manner for personal usage"*,[75] in the Court's jurisprudence it was clear that mere surveillance was *"not at all"* a ground for surveillance,[76] or that monitoring employees to check whether they were using their computers for personal purposes was not sufficient, especially when justified by hypothetical risks or claims that did not demonstrate that employee's behaviour or personal usage was detrimental to the company.[77] In *Libert*, while we might agree that the interference was based on facts following the discovery of the files by one of his colleagues to whom the computer has been transferred[78], and if the Court claimed that the legitimate aim was the protection of the "*rights of others*",[79] it is not clear in its reasoning how such abusive use of the storage was detrimental to the company as the main legitimate aim put forward focused only on the legitimacy of the employer to put *"in place mechanisms to verify that its employees are performing their professional duties adequately and with the required speed"*.[80]

This case, secondly, illustrates the Court's emerging shift regarding workers' information prior to monitoring. The Court underlined the balance struck under French law, which seeks to protect private life by *informing* the worker, in person or by phone call, that their files might be disclosed, and aims to allow them to explain themselves[81]. The Court found this notification *ex ante* to be an adequate balance. However, there was no mention of worker's knowledge that their communications might be subject to disclosure, whether under internal SNCF's regulations or through prior information at any time during their contract, in the Court's assessment. The *informed worker* here only concerns an *ex ante* notification of the upcoming interference, without assessing whether the worker might have been aware of such a possibility existing.

Such a gradual erosion of the right to prior information of the worker will be clearly formalised in *López Ribalda*. Similar to *Köpke*, in which a supermarket deployed covert CCTV surveillance due to the suspicion of theft, 14 employees were dismissed, including the five applicants, following the discovery of the images. During the initial ruling of *López Ribalda*, the Court's Chamber found a violation of Article 8[82]. Although the system was deployed amid a legitimate suspicion of theft, the Court found that the deployment was too broad in scope, not limited in time, affecting all workers and all their working hours, and that employers failed to give prior information on the collection and processing of workers' data, thus failing to meet the proportionality principle.[83] For the Court, the employer's rights could have been secured by informing the applicants, even in a general manner, of the installation of the system.[84] The Grand Chamber overruled the Chamber's decision and formalised the erosion of workers' information in its assessment. Even though the Court recalled that workers' information is fundamental in nature, particularly in the context of employment and due to the significant employer's powers with regard to employees and the risk of abuse of powers[85], they detailed that there is no requirement from international and European standards to require "*the prior consent of individuals placed under video*

[75] ECtHR, *Copland v. UK*, (n 20).
[76] ECtHR, *Antovic and Mirkovic v. Montenegro*, (n 58), §59.
[77] *Ibid*., §59; ECtHR, *Bărbulescu v. Romania*, (n 32), §135: the domestic court, the County Court, touched this aspect as they tried to justify more precisely the need for the company's IT systems are not damaged, avoid illegal activities in cyberspace or for the company's trade secrets to be disclosed. However, the Court found such examples to be only theoretical, as there was no suggestion that the applicants had actually exposed their company to such risks.
[78] *ECtHR, Libert,* (n 65), §44: Such discovery could be considered as a particularly severe risk/exceptional circumstance under the jurisprudence of the Cour de Cassation.
[79] *Ibid*., §46.
[80] *Ibid.*
[81] *Ibid*., §44.
[82] ECtHR, *López Ribalda and Others v. Spain*, n°1874/13 and 8567/13, 9 January 2018; ECtHR, *López Ribalda and Others v. Spain*, n°1874/13 and 8567/13, 17 October 2019, §§69-70.
[83] ECtHR, *López Ribalda and Others v. Spain*, n°1874/13 and 8567/13, 17 October 2019, §79.
[84] *Ibid.*
[85] *Ibid*., §131.

*surveillance at the workplace*"[86] but a "*general obligation to be informed of the monitoring*".[87] According to the Court, such notification "*is just one criterion to be taken into account*" to assess the proportionality of the measure. If this condition is lacking, "*the safeguards deriving from the other criteria will be all the more important*".[88] Consequently, workers' information becomes merely a criterion that could be justified by other overriding interests,[89] notably the need to effectively detect serious misconduct. In this context, informing workers is seen as potentially hampering this aim,[90] and in the present case, due to the "*general climate of mistrust*" within the company.[91] Consequently, the Court found that there was no violation of Article 8.[92]

The Court confirmed this erosion in *Tena Arregui v. Spain*. In this case, a member of a political party was suspected of negotiating with another political party.[93] A private company was hired to monitor his emails to determine where his loyalties lay.[94] The Court explicitly stated that the applicable principles developed in its jurisprudence regarding interference/monitoring in the private and public sectors were similar, as both contexts aimed to strike a fair balance between the competing interests of the individual and the community as a whole[95]. Consequently, they referred to the criteria developed in *Bărbulescu.*[96] However, despite this formal continuity, the Court upheld the domestic decision and found no violation of Article 8. The Court justified its approach by explaining that the context inherent to a political party diverged from the traditional "*employer-employee relationship*"[97] characterised by contract and legal obligations, while the other is characterised by organisational autonomy, freedom of association and power of discipline[98]. If the Court acknowledged that "*political loyalty expected of party members [...] cannot result in an unrestricted opportunity to monitor [their] correspondence*",[99] and must be accompanied by adequate safeguards against abuse[100], the Court found that the Constitutional Court was "*coherent and respectful in the content of fundamental rights affected*"[101] and did not find that domestic authorities failed to afford adequate protection of the applicant's right to private life. Consequently, the Court found no violation.[102]

While formally recalling *Bărbulescu*, the Court parsimoniously applied its criteria, notably in assessing workers' information. The Court did not assess the quality, scope and timing of the information provided to the applicant. Instead, the Court relied on internal rules indicating that emails could be monitored, and this approach was criticised by two domestic dissenting judges[103] who complained that domestic authorities failed to analyse whether the applicant had known and consented to the internal rules and the

[86] ECtHR, *López Ribalda and Others v. Spain*, (n 82) (17 October 2019) §131.
[87] *Ibid*., §§115-116(i); *ECtHR, Bărbulescu v. Romania*, (n 32), §§121-122.
[88] ECtHR, *López Ribalda and Others v. Spain*, (n 82) (17 October 2019) §§115-116(i).
[89] *Ibid*., §§133-134.
[90] *Ibid*., §§128 and 132: For the Court, there were no less intrusive methods that might have pursued the legitimate aim.
[91] *Ibid*., §134.
[92] *Ibid*., §137.
[93] ECtHR, *Tena Arregui v. Spain*, n°42541/18, 11 January 2024.
[94] *Ibid*., §1.
[95] *Ibid*., §33: Such margin has however, limits, more particularly when the interference concerns a "*particularly important facet of an individual's existence or identity is at stake, or where the activities at stake involve a most intimate aspect of private life, the margin allowed to the State is correspondingly narrowed".*
[96] *Ibid.,* §34. The Court recalls *Bărbulescu*, notably §§113-115.
[97] *Ibid*., §38.
[98] *Ibid.,* §38.
[99] *Ibid*., §38.
[100] *Ibid*. §38 citing mutatis mutandis *Bărbulescu* (n 32) §120: safeguards against abuse are required *"irrespective of the extent and duration of such measures"*.
[101] ECtHR, *Tena Arregui v. Spain*, (n 93), §40.
[102] *Ibid*., §§44-45.
[103] *Ibid*., §17.

use of the email account and whether he had been informed of the possibility that the political party might access his email's account without his consent.[104]

Consequently, a closer examination of the Court's subsequent evolution of its case law reveals a substantive shift in the function of workers' right to information. Initially conceived as a procedural safeguard designed to protect workers against disproportionate monitoring and to enable them to contest intrusive interference or monitoring, it is increasingly treated as a contextual factor within the proportionality assessment, overridden by managerial interests. More worrisome, information ceases to operate as a protective mechanism, and instead transparency becomes a justificatory claim through which surveillance practices are retrospectively legitimised.

*b) When Transparency Turns Against Workers*

The evolution of the Court's case law reveals a more subtle transformation: transparency may paradoxically operate against workers. While informational rights were initially conceived as safeguards against surveillance,[105] recent judgments suggest that transparency can be mobilised as a justificatory rhetoric that legitimises monitoring practices. This section illustrates how the Court increasingly accepts broader uses of data collected through more intrusive devices, including secondary data uses, while workers' control over such information remains limited.

In *Adomaitis v. Lithuania*, the Court first confirms the decline of workers' information in the case of interference with their communications. In 2022, the communications of a prison governor were intercepted due to suspicion that he had, for pay, provided inmates with better conditions and had also awarded them incentives.[106] The information and data intercepted were then used in the proceedings of his dismissal for misconduct.[107] Later, the governor requested access to the information gathered during the criminal intelligence investigation and was provided with only part of the transcripts of the telephone conversations[108] that led to his dismissal. The applicant requested that the department release all the information gathered about him, but the department refused.[109] Consequently, he complained that he had not been able to see in a timely manner the materials used against him, even though the institution had had access to that information.[110] The Court recognised that in principle public authorities should notify of the interference, however, the criteria of foreseeability of the law "*cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly*".[111] Consequently, the absence of prior notification of interception

[104] *Ibid*., §41.
[105] In the Court's case law. In labour law, workers' information and consultation rights also refer to participation rights that are intended not merely to keep employees passively informed, but also to enable them to participate in the life of the company, see for instance F. Hendrickx, I. Durri and C. Stylogiannis, 'Worker Participation in the Enterprise' in M. Freedland and others (eds), *The Oxford Handbook of Law and Work* (OUP 2024) 467-480.
[106] ECtHR, *Adomaitis v. Lithuania*, n°14833/18, 18 January 2022, §7.
[107] *Ibid*., §25.
[108] *Ibid*., §13.
[109] Argued on the ground that those documents contained specific information about the devices used, installation, dismantlement and identities of secret participants.
[110] ECtHR, *Adomaitis v. Lithuania*, (n 106), §60.
[111] *Ibid*., §84

was compensated by strict conditions regarding the implementation of the surveillance measures and interception of its communications[112] and the Court found no violation of Article 8[113].

The Court also revealed how transparency may turn against workers. In this case, the Court invoked the principle of public servants' transparency to justify the reuse of secondary data that were initially not intercepted within the framework of the corruption investigation. Due to the suspicion of corruption-related activity, the Court agreed that the (re)use of declassified information gathered during the phase of secret surveillance could be used in the framework of the disciplinary proceedings out *"of guaranteeing the transparency and openness of public service, and [...] to ensure that the aims of statutory institutions were not ignored"*[114].

Such reuse of secondary data was criticised by Judge Koskelo in a partly dissenting opinion[115] calling for additional safeguards to workers' right to privacy with the rise of more sensitive technologies. According to him, it appeared that, as domestic authorities relied on the fact that interference was lawful for criminal investigation, the same applied to its use in the framework of disciplinary proceedings against the applicant.[116] However, if such interference was necessary and justified for the first intended purpose, any further use of the records and the data raised distinct issues under Article 8.[117] Because tapping and other forms of interception of telephone conversations constitute a serious interference, Judge Koskelo explained that the law should be particularly precise *"especially as the technology available for use is continually becoming more sophisticated"*,[118] and be provided with adequate safeguards, and in the light of contemporary principles relating to data protection in the case of data reuse,[119] which should also meet the requirements of lawfulness, necessity and proportionality.[120] Consequently, the judge was not convinced that in the present case, such an assessment of the necessity and proportionality had been made, which would have justified a violation.[121]

Judge Koskelo's call for more protection under data protection is even more important, as the Court systematically finds no violation of Article 8 despite the heightened sensitivity and duration of the data collected. In the case *Florindo de Almeida Vasconcelos Gramaxo*,[122] a company installed a geolocalisation tracking system within company cars. Following the discovery of anomalies during a car's inspection, another hidden tracker was installed, without the applicant's knowledge,[123] to check whether the employee was using the car for personal purposes and was lying about his mileage declarations. Data obtained from the second hidden device confirmed a discrepancy between data from the first tracker and the employee's declaration. The employer engaged disciplinary proceedings and dismissed the applicant on the grounds that he had increased the distances driven for professional purposes to reduce his private distance, failed to work the prescribed working hours, and had interfered with the operation of the GPS during the weekend.[124] The Court found that national authorities had not failed to comply with their positive obligation to protect the applicant's right to respect for his private

[112] *Ibid*. §83: "*In the present case, the Court also finds that the absence of prior notification of interception was compensated for in the Law on Criminal Intelligence, accessible to the applicant, as that Law laid down strict conditions with regard to the implementation of the surveillance measures*". Such strict conditions were not detailed in the case.
[113] *Ibid*., §90.
[114] *Ibid*., §84.
[115] ECtHR., *Adomaitis* (n 106), partly dissenting opinion of Judge Koskelo.
[116] *Ibid*., §3.
[117] *Ibid*., §4.
[118] *Ibid*., §5.
[119] *Ibid*., §§5-6.
[120] *Ibid*, §7.
[121] *Ibid*., §§ 8-10.
[122] ECtHR, *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, n°26968/16, 13 February 2022.
[123] *Ibid*., §37.
[124] *Ibid*., §21.

life as, contrary to previously mentioned cases, he had been aware that the company had installed a GPS system in his vehicle to monitor the distances travelled in the course of his professional activity[125] and, where applicable, on his private journey. According to the Court, the extent of the intrusion into the applicant's private life has been reduced to what was strictly necessary to achieve the legitimate aim pursued, namely, to monitor the company's expenditure and that there was no violation of article 8.[126]

Consequently, *Florindo* consolidates the post-*López Ribalda* approach. Despite the increasing invasive nature of the technologies being deployed, the Court systematically prevails employers' property rights over workers' right to privacy while treating workers' information as merely a minimal transparency requirement capable of justifying extensive surveillance practices once reasonable suspicion is invoked, rather than as a procedural safeguard structuring the balance of interests at stake.

# 3. Discussion: The Normalisation of Workplace Surveillance

The analysis of the Court's case law reveals two broader structural transformations in the regulation of workplace surveillance. First, the threshold justifying monitoring practices appears to have progressively lowered as employers' managerial justifications have expanded, often involving multiple and overlapping purposes. Second, the function of workers' right to information has transformed from being a central *ex ante* safeguard against covert monitoring to become a *mere* criteria within the Court's proportionality analysis. Together, these developments contribute to a gradual normalisation of workplace surveillance.

## 3.1 Lowering of the Threshold of Suspicion

Despite the Court's promise to adjust its assessment as technological intrusiveness increases,[127] the Court appears to have lowered the threshold of suspicion that can justify surveillance. Formally, the Court still formally acknowledges that "*power of discipline cannot result in an unrestricted opportunity to monitor*" their workforce,[128] or that privacy cannot be reduced to zero,[129] and that *mere*[130] or "*the slightest suspicion of misappropriation or any wrongdoing on the part of employee [… should not] justify the installation of covert surveillance*"[131] but should be *"substantiated [, demonstrating] that the employee had committed an offence and [that] surveillance was altogether proportionate to the aim of investigating the offence at issue*".[132] However, post-*Bărbulescu's* rulings increasingly tolerate

[125] *Ibid*, §116.
[126] *Ibid*, §§120 and 124-125.
[127] ECtHR, *Köpke v. Germany,* (n 29), p.13: If the Court notes that the competing interests might well be given a different weight in the future, having regard to the extent to which intrusions into private life are made possible by new, more and more sophisticated and intrusive technologies. The Court also noted that such a balance aimed to "*reflect and comply with the increased vigilance in protecting private life which is necessary to contend with new communication technologies which make it possible to store and reproduce personal data*".
[128] ECtHR, *Tena Arregui v. Spain*, (n 93), §38.
[129] ECtHR, *Bărbulescu (n 32) and López Ribalda (n 8*2).
[130] ECtHR, *Halford v. UK,* (n 16).
[131] ECtHR, *López*, (n 82), §134.
[132] ECtHR, *Köpke v. Germany,* (n 29).

monitoring based on broader rhetoric, such as general mistrust, verifying compliance with internal rules[133], protecting organisational interests, or controlling companies' resources and expenses[134].

This observation becomes particularly salient in cases involving multiple intended aims and the secondary uses of data. Such a situation is not only noticeable in *Adomaitis*, but similar observations apply to *Florindo's* case. Employers' internal communication stated that the intended purpose aimed to tackle *"a concern relating to the safety of the vehicle and its passengers, as well as the correct use of a work tool that [the company] own[s] and make[s] available to [employees] in order to facilitate the proper performance of [their] duties".*[135] During the proceedings, the applicant claimed that additional purposes were argued by the employer beyond the control of the company's expenses, such as verifying whether he went to sites he declared he went to, executed his contractual obligation of 8 hours per day, to control the number of km used for private purposes, as well as to guarantee location safety and protection of the user of the vehicle, and guarantee in case of theft or sinister.[136] Similarly, in *Antovic*, the Dean also claimed to deploy surveillance for the safety of the building and its occupants, while, according to the dissenting judges, it was ultimately deployed primarily for managerial purposes and *"the surveillance of teaching".*[137]

This widening of legitimate aims pursued occurs in a context where the Court parsimoniously applies its own criteria, both in the private and public sectors, when assessing the necessity and proportionality principles. As illustrated in Table 1, since *Bărbulescu* most rulings have shown a narrow majority and often include dissenting opinions, indicating a certain opposition within the Court in contrast to earliest case law as more intrusive technologies have proliferated. This lack of clear consensus among the judges is noticeable in *Florindo,* in which dissenting judges argued that geolocalisation data are inherently intrusive, expanding beyond professional activities, and might reveal movement patterns, habits, and aspects of an individual's private life,[138] thus differing this case from the previous ruling.[139] According to them, the balance found in *Florindo* was inadequate as the interference was serious,[140] especially as the employer had at his disposal a control of 24 hours per day, extended to periods when the applicant was not working, and during three years, exceeding the threshold of strict necessity usually admitted by the Court.[141] They based their evaluation on the decision of the Portugal's national data protection authority, which highlighted that alternative and less intrusive means, such as the installation of "*a 'simple' switch to distinguish between professional and private use of the company vehicle*",[142] might have achieved the same purpose. Such a case is not isolated, as since *Bărbulescu*, the Court has almost never systematically assessed the strict necessity test for monitoring, and, notably, its impact on workers.[143]

The importance of the strict necessity test in case of workers' monitoring is even more critical as the evolving data protection framework aims to address the erosion of the boundary between professional

[133] ECtHR, *Adomaitis v. Lithuania*, (n 106).
[134] ECtHR, *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, (n 122), §120.
[135] *Ibid*., §13.
[136] *Ibid*., §40.
[137] ECtHR, *Antovic and Mirkovic v. Montenegro*, 28 November 2017, n°70838/13, Joint concurring opinion of judges Vucinic and Lemmens, §4.
[138] ECtHR, *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, n°26968/16, 13 February 2022, Joint dissenting opinion of Judges Motoc, Pastor Vilanova and Guerra Martins, § 6.
[139] *Ibid*., §4.
[140] *Ibid*., §10.
[141] *Ibid.*
[142] *Ibid*., §17.
[143] Molè, M., & Mangan, D., (n 6); Molè, M., & Ponce Del Castillo, A., *'Worker monitoring vs worker surveillance: the need for a legal differentiation'*, in *Castillo (Ed.), Artificial intelligence, labour and society*, ETUI, 2024, pp. 157-172; Polajžar, A., *'Covert Surveillance at the Workplace and the ECtHR Approach: Possible Risks of Breaching GDPR Rules'*, in *E-Journal of International and Comparative Labour Studies*, 12(03), 2023.

and private life. More and more companies allow their employees to use professional facilities for personal usage,[144] and such use is tolerated to the extent that it is not detrimental to the company's facilities or expenses.[145] In early international and European data protection frameworks, as highlighted in *Bărbulescu*, advisory authorities underlined how a blanket ban[146] on employees' personal use of the internet or professional facilities does not appear reasonable and fails to reflect how such use could assist them in their daily lives.[147] Following this logic, controlling workers' activities should not be permitted as a rule,[148] except in cases to safeguard employers' property and/or detect, prevent and control *serious* offences. The *"prevention [of the offence] should be more important than [its] detection"*,[149] and even in the case of legitimate monitoring, employers should aim to minimise workers' data collection and limit the risks they are exposed to.[150] However, as illustrated by *López* Ribalda or *Adomaitis*, the Court has gradually accepted that mere detection or surveillance of any employee wrongdoing might constitute an adequate purpose, and as illustrated in *Florindo*, regardless of the data-hungry technology being used.

Surprisingly, such evolutions occur in a context where the Court is aware of, and relies on, the relevant national,[151] European,[152] and international data protection legal frameworks[153] and jurisprudence[154] to assess its cases. Consequently, it is interesting and questionable to note that workers' informational rights have declined, despite their initial importance in case law for protecting workers' right to privacy, as in the framework of the digital economy: workers' information and employers' transparency requirements have been reinforced.[155]

## 3.2 The Decline of Informational Safeguards in an Age of Transparency

The analysis also shows that workers' informational rights, once central to the Court's protection of workers' right to privacy, has become instrumental. While the Court still claims the importance of workers' information, *López Ribalda* relegated this procedural guarantee as a mere criterion. On one hand, worker's information and notification of the interference/monitoring do not structure *ex ante* the assessment of the necessity to monitor or interfere anymore. On the contrary, it is mobilised to validate,

---

[144] The personal usage of professional facilities was mentioned both in *Halford* and *Köpke*. In *Libert*, internal SNCF regulations clearly allowed their employees, to a certain extent, to use their professional computer for personal use.
[145] ECtHR, *Bărbulescu v. Romania*, (n 32): the company must be able to demonstrate the loss/potential damage invoked.
[146] *Ibid*., §§46-49.
[147] WP29, Working document on the surveillance of electronic communications in the workplace, adopted on 29 May 2002, p.4.
[148] WP 29, Opinion 8/2001 in the processing of personal data in the employment context, adopted on 13 September 2001, p.22.
[149] WP 29, (n 147), p.4.
[150] Council of Europe, Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment: the "*use of data-processing methods by employers should be guided by principles designed to minimise any risks that such methods might pose to employees' rights and fundamental freedoms, in particular their right to privacy*".
[151] First in *Copland*, the Court recalled the Data Protection Act of 1984.
[152] In *Köpke*, the Court referred to the German Federal Data Protection Act and the Directive 95/46/EC of the European Parliament of 1995. European data protection frameworks were systematically recalled in *Bărbulescu*, *López Ribalda*, *Florindo*, and *Tena Arregui*.
[153] In *Bărbulescu*, the Court took into consideration the International Labour Organization's Code of Practice of 1997, Protection of workers' personal data.
[154] For instance, in *Bărbulescu v. Romania,* (n 32)*,* §50*:* the Court recalled the jurisprudence of the Court of Justice of the European Union that has interpreted the provisions of Directive 95/46/EC in the light of the right to respect for private life as guaranteed by Article 8 of the Convention in the case *Österreichischer Rundfunk and Others* of 20 May 2003.
[155] El Bouchikhi, M. (n 7).

*a posteriori*, the employer's interference or surveillance,[156] underlining a "*transparency paradox*":[157] safeguards designed to empower individuals through information may, when reduced to formal disclosure obligations, fail to meaningfully constrain the expansion of surveillance practices. Employers begin to rely on a discourse based on transparency obligations to justify the need to *know more* about workers,[158] their habits or/and their journey.[159] This discourse is coupled with *a posteriori* compliant strategies, such as the construction of a legal framework after the case,[160] to justify the monitoring to the Court. This unknown monitoring operates in a context that allows extensive employers' prerogatives, such as data reuses,[161] regardless of the sensitivity of the data at stake, and for an extensive period of time.[162] On the other hand, workers are increasingly being monitored but face obstacles to obtaining full access to their data.[163] This evolution is exactly the ground on which the applicant complained in *Bărbulescu*. According to him, the Chamber initially had incorrectly distinguished the present case from *Copland* as the *"decisive factor"* was not *"whether the employer had tolerated personal internet use, but the fact that the employer had not warned the employee that his communications could be monitored."*[164] For him, his employer *"had first placed him under surveillance and had only afterwards given him the opportunity to specify whether his communications were private or work-related"*.[165]

Such a decline of workers' right to information is heavily criticised by dissenting judges and civil society as it questions the remaining place of workers' privacy in the digital age. In *López Ribalda*, the European Trade Union Confederation (ETUC) intervened as third party and explained the extent to which the "*right to be informed of the collection of personal data*" was recognised in domestic law but also at the international and European level and was regarded *"as a right derived from Article 8 of the Convention, constituting a procedural safeguard"*.[166] This criticism was made by dissenting judges in *López Ribalda*.[167] According to them, such an information *lacuna* raises broader questions about the remaining place of workers' rights to privacy[168] and the types and levels of surveillance currently acceptable within our society.[169] Despite the Court's *"increased vigilance"*[170] to protect workers' right to privacy, "*[s]ince then, surveillance technologies and the data collecting using them have been significantly developed […] with little control and not much trace*"[171] about who might have access to them and for what purpose. Consequently, dissenting judges call for stronger safeguards as there is a need to preserve workers' right to private life.[172] As they witness *"the growing influence that technology has on our society",* they ring the bell on the fact that *"we cannot afford to let individuals take justice into their own hands and allow the right to a private life […] to remain insufficiently protected when faced with*

---

[156] ECtHR, *Adomaitis v. Lithuania,* (n 106); ECtHR*, López Ribalda and Others v. Spain,* joint dissenting opinion of Judges De Gaetano, Yudkivska, and Grozev, §4.
[157] Nissenbaum, H., *A Contextual Approach to Privacy Online*, in *Daedalus*, 140 (4), 2011, pp. 32-48.
[158] *Ibid*.
[159] The Court relied heavily on workers' general awareness of the geolocalisation as sufficient to satisfy the transparency dimension of proportionality.
[160] ECtHR, *López Ribalda*, (n 82), joint dissenting opinion of Judges De Gaetano, Yudkivska, and Grozev, §4: dissenting judges raised the fact that national authorities developed a legal response after the case, undermining the foreseeability of the legal framework.
[161] ECtHR, *Adomaitis v. Lithuania*, (n 106).
[162] ECtHR, *Florindo (n 122) and López Ribalda (n 8*2): the monitoring was conducted for 3 years and 10 days.
[163] ECtHR, *Adomaitis v. Lithuania,* (n 106), notably the second report made on his account, as well as non-disclosed documents.
[164] ECtHR, *Bărbulescu*, (n 32), §86.
[165] *Ibid*.
[166] ECtHR, *López Ribalda,* (n 82)*,* §107.
[167] *Ibid*., joint dissenting opinion, §§4-7.
[168] ECtHR, *López Ribalda and Others v. Spain*, (n 82), §107.
[169] ECtHR, *Florindo* (n 122), joint dissenting opinion, §5; In the same line of thought, ECtHR, *López Ribalda* (n 82), Joint dissenting opinion, §4.
[170] ECtHR, *López Ribalda* (n 82), Joint dissenting opinion, §3.
[171] *Ibid*.
[172] ECtHR, *Florindo* (n 122), Joint dissenting opinion, §5.

*such new challenges".*[173] Such responsibility is not solely the State's, but also the Court's, as by not finding a violation in *López Ribalda, "the Court has decided to allow the unlimited use of covert video surveillance in the workplace without affording sufficient legal safeguards to those whose personal data will be collected and used for purposes unknown to them".*[174]

This jurisprudential evolution contradicts the broader European and international framework increasing workers' protection in light of transparency requirements and participatory rights. At the outset of workers' data protection in the 1980s, workers' information was not conceived as a mere formal *"notice requirement"* that passively informed workers of any interference.[175] It is coming from a long development[176] and is conceptualised as a cornerstone of workers' individual and collective protection,[177] participation,[178] in a context where the workplace is becoming increasingly digitalised. Such an obligation to provide workers' information has been reinforced under current data protection laws through employers' transparency requirements and clear workers' individual rights,[179] and was recently extended to non-traditional workers, platform workers, due to the increasing algorithmic management to which they are subject to.[180] As data protection law is nonetheless considered imperfect in the context of the workplace, legal scholars imagine new solutions aiming to provide *"sufficient legal safeguards to those whose personal data will be collected and used for purposes unknown to them".*[181] For instance, some argue that artificial intelligence systems should be considered as *unlawful "by default"* when being deployed at the workplace[182] due to the numerous risks they may present, and that this presumption would only be reversed if the employer is able to demonstrate that such systems are strictly proportionate and necessary to achieve a *good* intended goal, while taking into account their potential impacts on workers', and notably their fundamental rights.[183]

---

[173] ECtHR, *López Ribalda* (n 82), Joint dissenting opinion, §15.
[174] *Ibid*.
[175] For instance, *Libert* (n 65); See also El Bouchikhi M (n 7).
[176] Workers' right to information has been at the core of workers' protection for 30 years. It was already mentioned in the 1988 Additional protocol to the 1961 version of the European Social Charter, and was later codified in Article 21 of the 1996 revised version. It has been successively enshrined within numerous directives of the EU during the 1990s, before being formally recognised within the Directive 2002/14/EC dedicated to providing a general framework for informing and consulting workers, as well as under Article 27 of the EU Charter of Fundamental Rights in 2000.
[177] El Bouchikhi, M. (n 7).
[178] Hendrickx, F., Durri, I., & Stylogiannis, C., *Worker Participation in the Enterprise*, in *The Oxford Handbook of Law and Work,* 2024.
[179] Council of Europe, Convention 108+ and the recommendations of the Council of Europe dedicated to the employment context, see CM/REC(2015)5; See the numerous guidelines of Article 29 concerning the employment context in conjunction with the Directive 95/46/EC. Most of the provisions of the Directive were reinforced in 2018 by the General Data Protection Regulation, the successor to the 1995 Directive, including individuals' rights to information, access, and rectification, as well as stronger transparency requirements.
[180] Directive (EU) 2024/2831 on improving working conditions in platform work, arts. 9(1) and 13-14 and recital 30; See ILO's Convention on decent work in the platform economy, art 13.
[181] ECtHR, *López Ribalda* (n 82), Joint dissenting opinions of Judges De Gaetano, Yudkivska, and Grozev, §15.
[182] Malgieri, G., & Pasquale, F., *From Transparency to Justification: Toward Ex Ante Accountability for AI*, *Brooklyn Law School, Legal Studies Research Paper no 712*, 2022.
[183] Weerts, S., Naous, D., El Bouchikhi, M., & Clavien, C. (2022). AI Systems for Occupational Safety and Health: From Ethical Concerns to Limited Legal Solutions 21st IFIP WG 8.5 International Conference on Electronic Government (EGOV)/ Conference on E-Democracy and Open Government Conference (CeDEM)/ IFIP WG 8.5 International Conference on Electronic Participation (EPart), Linkopings University, Linkoping, Sweden. Springer.

# 4. Conclusion

This article has examined the evolving function of the right to be informed in regulating workplace surveillance by technological means through a systematic analysis of the European Court of Human Rights' case law. The analysis reveals a gradual transformation in the function attributed to employers' transparency requirements and workers' prior information under Article 8 of the ECHR. While the Court continues to formally rely on the criterion established in *Bărbulescu v. Romania*, an analysis of its subsequent case law suggests that workers' right to privacy has progressively diminished, notably through the limited weight given to workers' prior information in the Court's proportionality assessment.

By reconstructing the Court's jurisprudential trajectory, this article explains the doctrinal mechanism through which the Court has progressively developed a "*more surveillance*" approach in its case law, while showing that this evolution reflects a more gradual transformation than an abrupt shift within its jurisprudence. Beyond the turning points frequently associated with *López Ribalda* or more recent judgments such as *Florindo*, the analysis highlights how elements of this shift were already visible in earlier case law in a context where covert or overt monitoring practices were increasingly justified through broader managerial and property-based claims, as well as mere suspicion rather than factual evidence of any substantive, serious offence by the employee.

More importantly, by examining this evolution through the lens of workers' prior information in the Court's assessment, it illustrates the limits of transparency-based safeguards through the "*transparency paradox*": originally conceived by the Court as protecting workers *ex ante* against intrusive and illegitimate surveillance, it increasingly appears as a mere minimal transparency requirement, rather than as a substantive safeguard, able to legitimise *a posteriori* intensive surveillance practices. In several cases, monitoring practices have been found compatible with Article 8 despite the absence of information, or limited or ambiguous information provided to workers, and regardless of the intrusiveness of the technology used or the sensitivity of the data collected. At the same time, while the threshold of transparency expected from companies is declining, workers themselves are expected to become more transparent. In judgments such as *Florindo*, concerning the tracking of a worker's movements, and *Adomaitis*, which speaks explicitly of the transparency expected of public officials, the demand for transparency increasingly bears on the worker, whose conduct must itself be rendered visible to justify closer scrutiny through technological means.

Thus, this jurisprudential evolution appears to be at odds with broader European and international regulatory developments. Over the past decades, from early data protection regimes to current initiatives, transparency obligations and workers' informational rights have been progressively reinforced in response to digitalisation and algorithmic management.[184] These developments suggest that transparency requirements and workers' right to information are becoming an increasingly central component of the regulatory architecture governing digital workplaces. Yet, the Court's recent approach suggests that informational rights alone may not be sufficient to counterbalance the structural asymmetries inherent in employment relationships and to prevent the abuse of workers' data.

Ultimately, the Court's evolving approach raises important questions regarding the capacity of workers' informational rights to provide meaningful protection in increasingly data-driven workplaces. As new European and international regulatory instruments reinforce transparency obligations and workers' participatory safeguards in the framework of the digital workplace, the Court may increasingly be called

[184] El Bouchikhi, M. (n 7).

upon to reassess the role attributed to workers' informational rights within its Article 8 balancing exercise. Thus, preserving the substantive protective function of these safeguards will be crucial if transparency is meant to serve as a genuine defence of workers' fundamental rights, rather than a mechanism through which intrusive forms of workplace surveillance become progressively normalised and legitimised.

## 5. Acknowledgement

The author thanks Prof. Sophie Weerts for her continuous feedback and wonderful suggestions during the writing and editing process. The author also thanks the participants of the conference Lawtomation Days 2024 at IE University, Madrid, and notably Prof. Aloisi Antonio, Prof. Albin Einat and Prof. Collins Philippa, for their insights during the initial presentation and version of this article. The author would also like to thank the reviewer for their valuable comments and suggestions, which greatly helped to improve the quality of the manuscript.

## 6. Declaration of conflicting interests

The author declares having no conflicts of interest.

## 7. Funding

This research is funded by the Swiss National Science Foundation (grant no. 187429) within the Swiss National Research Programme (NRP77) on "Digital Transformation". For the purpose of Open Access, the author has applied a CC BY public copyright licence to the author accepted manuscript version arising from this submission.