**Vilnius University Faculty of Law**

**Department of Public Law**

Naima Jebin Eti,

2nd study year, International and European Law Study Programme Student

Master's Thesis

# Article 8 of the ECHR in the context of labour law

# EŽTT 8 straipsnis darbo teisės kontekste

Supervisor: Prof. Dr. Tomas Davulis

Reviewer: Justinas Usonis

**Vilnius**

**2025**

## ABSTRACT

This thesis examines when and how Article 8 of the European Convention on Human Rights applies in employment contexts. Particular attention or focus is provided to workplace monitoring and the processing of sensitive personal data. It focuses on three domains in which tensions between managerial interests and employee privacy most frequently arise. They are related to: the monitoring of professional communications, visual and location surveillance through CCTV and GPS technologies, and identity-related practices such as vetting and the use of medical or criminal-record data at work. Relying on a doctrinal analysis of leading judgments of the European Court of Human Rights, the thesis analyses how the Court identifies interferences with private life in professional settings and how it assesses their justification under Article 8(2).

On the basis of this analysis, the thesis develops a concise, factor-by-factor proportionality framework that can be applied across different workplace measures. The study finds that compliance with Article 8 in labour-law disputes is primarily determined by the quality and foreseeability of the legal basis, clarity of purpose, narrow targeting in time, space and scope, the presence of prior notice or overriding reasons for its absence, effective limits on access and retention of data, and the documented consideration of less intrusive alternatives. These factors guide the balancing exercise required of domestic authorities and provide practical criteria for courts, employers and employees when assessing workplace monitoring measures under Article 8.



***Keywords:*** *workplace privacy, Article 8, proportionality, communications monitoring, CCTV, GPS tracking, security vetting*

# Contents

# INTRODUCTION

**Background and relevance.** Workplaces are changing fast. Digital communications are now part of routine work (Mačiulaitis, 2023). Email, instant messaging and team platforms create constant streams of data. Employers also use tools that observe space and movement. CCTV is a common feature in shops, warehouses and offices. GPS devices are used in vehicles and company equipment. Some sectors rely on drug or alcohol testing. Some roles include health checks or other integrity measures. These practices generate new frictions between privacy and management. They also create legal questions about the reach of human rights at work.

Article 8 of the European Convention on Human Rights protects private life, family life, the home and correspondence (Sychenko & Chernyaeva, 2019). The provision is a qualified right. This means the state may interfere in limited and regulated situations. It also means that domestic authorities must protect the right against private interference when the situation demands it. In employment settings, the lines between private life and professional life are not always clear. Modern work often blends personal and professional communication (Ponce Del Castillo & Molè, 2024). The workplace can hold many forms of personal data. Employers have legitimate aims. They must protect property, ensure safety and monitor performance. They may also investigate misconduct. But they must do so in a way that respects human dignity and legal safeguards. The European Court of Human Rights has developed a body of case law that addresses these tensions. Its judgments examine legality, legitimate aims and necessity in a democratic society. They also translate these general standards into fact-specific conclusions. The Court looks at notice and transparency. It evaluates scope and intrusiveness. It asks whether less intrusive means were available. It considers the sensitivity of data and the consequences of measures, including a dismissal (Ásványi, 2022). This case law now serves as a guide for national courts, employers and employees. Yet its application in concrete disputes remains complex. This thesis addresses that gap in a focused and practical way.

The topic is relevant for several reasons. First, employers adopt monitoring technologies at scale. They manage larger datasets than before. They rely on those datasets in routine HR decisions. Second, employees face growing risks to their autonomy and private life. Even small practices can have cumulative effects on trust and dignity (Pollicino, 2022). Third, courts and regulators need simple criteria that work across different modalities. Clear

and consistent criteria improve predictability. They also reduce the need for litigation. Finally, legal education and training benefit from concise tools. A structured view of Article 8 in the workplace can support teaching and practice across the region.

**Problem statement and research gap.** The central problem is straightforward. There is no single, short and practical framework that legal actors can apply across common workplace scenarios under Article 8. The case law is rich. It spans communications monitoring, video surveillance, location tracking and testing. It grows over time and reflects diverse settings. Many academic works discuss parts of this field. Some focus on individual judgments. Others discuss broader privacy theory. These works are valuable. But they often do not give a compact and reusable tool for day-to-day decisions in employment disputes.

The Court uses consistent language on legality, legitimate aim and necessity. It looks at proportionality and fair balance. Still, the translation of these standards into workplace practice is uneven (Ásványi, 2022). One cause is factual variation. Some measures are narrow and time-bound. Some are broad and continuous. Some involve content. Others involve metadata or less sensitive data. Another cause is institutional context. Some workplaces are safety-critical. Others deal with high-value goods. Some have a record of loss or misconduct. These differences matter. They will continue to appear in new cases. Practitioners need a stable method to weigh these differences. The gap, therefore, is not a lack of doctrine. The gap is a lack of a concise, modality-neutral set of factors, stated in plain language which a court or employer can apply in a repeatable way . The thesis addresses this gap by extracting a small set of recurring factors from a short and representative case list and by expressing those factors in a summarised manner that fits the constraints of a master's project.

**Aim and research questions.** The aim is to determine how the European Court of Human Rights balances Article 8 rights in employment contexts and to derive a compact set of recurring factors that guide outcomes across different types of workplace measures.

The research questions are clear and limited:

- When and how does Article 8 apply to workplace situations, including professional spaces and professional communications?

- What are the main factors that drive the Court's proportionality analysis in communications monitoring, visual and location surveillance and testing measures?
- How do notice, scope and the availability of less intrusive means influence the outcome?

These questions remain within the boundaries of a master's thesis. They support a practical tool that readers can use in many disputes.

**Object and subject of research.** The object of research is the case law of the European Court of Human Rights on Article 8 in employment-related settings. This includes public and private employment. It also includes cases where the Court reviewed how national authorities balanced competing interests in disputes between private parties. The subject of research is the Court's reasoning on proportionality. The thesis examines how the Court identifies an interference. It then follows how the Court tests legality, aims and necessity. The core focus is the set of safeguards that the Court expects in the workplace. This approach separates two elements. The object identifies what legal materials the thesis studies. The subject identifies the part of legal reasoning that the thesis analyses. The object is the judgments and decisions. The subject is the logic of balancing under Article 8. This separation keeps the work centred on a clear analytical task.

**Scope and delimitations.** The thesis limits itself to a representative case list. It emphasises judgments that involve digital communications monitoring, video surveillance, location tracking and testing or health-related measures. It includes both earlier and more recent developments. It pays attention to leading or Grand Chamber judgments. It includes other decisions when they help to illustrate a factor of interest. The scope remains within the European Convention system. The thesis does not conduct an in-depth analysis of Court of Justice of the European Union case law. It refers to that jurisprudence only when needed for context or clarity. The thesis does not run empirical fieldwork or surveys. It uses doctrinal and comparative reading of judgments and legal sources. The thesis does not attempt to cover every case in the Strasbourg database. It also does not aim to make novel theoretical claims about the nature of privacy. The focus is applied and limited. The goal is a practical set of factors that can be tested against a small number of facts and then used by others. This keeps the workload realistic. It also enhances the clarity of the final conclusions.

**Methods and methodological approach.** The thesis uses doctrinal legal analysis as the main method. It reads and interprets the text of Article 8 and the relevant judgments. It identifies the operative parts of the Court's reasoning. It pays attention to the structure of interference, legality, legitimate aim and necessity. It examines how the Court handles proportionality in workplace contexts. It looks at safeguards such as prior notice, the scope and intensity of the measure and the presence of less intrusive means. It further evaluates the sensitivity of data and the consequences for the employee. The thesis supports this doctrinal reading with a simple and systematic comparison. It applies the same small set of factors to each selected case. It records the presence or absence of those factors. It notes the context in which the measure was used. It notes whether the employer had a concrete and serious reason. It notes whether the measure was targeted in time, space, or subject. It asks whether the measure involved the content of communications or only traffic data. It asks whether the measure was covert or visible. It observes how the presence of safeguards aligns with the outcome. This method is transparent and repeatable. It does not require complex tools. It fits the level of a master's project. Finally, the thesis uses limited comparative and systematic thinking. It does not compare legal systems in depth. But it compares modalities and contexts within the Convention system. It asks whether similar safeguards produce similar results across different types of measures. It also asks why certain contexts, such as safety-critical roles, may justify stronger interventions. This supports a clear and consistent synthesis in the conclusion.

**Key sources and case selection strategy.** The thesis relies on three groups of sources. The first and most important group is primary law and court materials. This includes the text of the European Convention on Human Rights. It includes judgments and decisions of the European Court of Human Rights that address workplace privacy. It also includes official materials, such as the Court's guides and factsheets, where they help to orient the analysis. The second group is selected academic literature. The thesis uses a small set of high-quality sources. These sources clarify the meaning of private life in professional spaces. They explain the structure of proportionality and necessity. They discuss the Court's approach to positive obligations and fair balance. They are used to support and verify the doctrinal reading. They are not used to generate new theory beyond the scope of this project. The third group is contextual materials. The thesis refers to data-protection principles only where they help to explain why a safeguard matters. For example, notice and purpose limitation can illuminate the discussion of foreseeability and scope. These references remain background. They do not replace or displace

the Court's own standards. The thesis also notes selected national judgments only when they are relevant to the Strasbourg analysis cited by the Court. The case selection follows a clear and simple logic. The thesis includes a short list of cases that together represent common workplace scenarios. It covers communications monitoring, video surveillance, location tracking and testing. It ensures that the list includes leading decisions and more recent cases. It chooses cases that show different outcomes, so that the analysis can contrast the presence and absence of key safeguards. Each case is chosen for its relevance to at least one factor under study.

**Originality and expected contribution.** The originality of the thesis lies in its method and in its format of results. The method is modest but strict. It reads a small number of cases in a consistent way. It records the same factors across all of them. It uses those observations to produce a compact and reusable tool. The format of results is a short checklist stated in plain language. The checklist is grounded in the Court's own reasoning. It can be used by judges, lawyers, employers and employees. It can also support teaching. It reduces the distance between doctrinal statements and real decisions in the workplace. The expected contribution is twofold. First, the thesis clarifies how Article 8 applies to common workplace measures. It does so without adding unnecessary complexity. It shows how notice, scope, less intrusive means, data sensitivity and consequences tend to move outcomes. It also notes the role of legality and the clarity of the employer's aim. Second, the thesis provides a small and concrete tool. The tool can help actors evaluate a measure before it is used or challenged. It can reduce uncertainty and litigation. It can also improve the quality of internal policies and judicial reasoning. This contribution is appropriate for a master's thesis. It is not a comprehensive treatise. It is a focused and useful addition to existing literature and practice.

# 1. LEGAL FRAMEWORK OF ARTICLE 8

## 1.1 Article 8 of the ECHR in the context of labour law

Article 8 protects private life and correspondence. It is not a narrow or domestic concept. It is a living standard which adapts to social as well as technological change. Its scope extends beyond the home along with social identity and relationships (Mačiulaitis, 2023). That reach matters for work. People form ties then define identity and process personal information in the workplace. For that reason professional life is simply not excluded from protection by default. The Convention accepts that many work situations fall within private life or correspondence while that they must be assessed within the Article 8 structure rather than rejected at the threshold. This is the starting point for labour law in Europe. It is also the reason that national courts are obliged to regard many measures taken in the workplace as potential interferences with a human right and not as matters of internal discipline alone.

The bridge that is linking human rights as well as labour relations is established on positive obligations and horizontal effect. The Convention is binding on states. But the vast majority of employers are private (Ligthart, 2019). The Court deals with this by looking at whether or not domestic law then the domestic courts have ensured effective respect for the right of private life in disputes between employees as well as private employers. It asks whether the national legal order offered an accessible framework with clear rules and remedies. It also questions whether the courts did any actual balancing of competing interests. This is how Article 8 enters the everyday practise of labour law. It is not an external add-on. It is embedded in the form of statutes while the collective agreements as well as internal policies and judicial reasoning that meets the quality of the Convention.

A threshold device helps identify when Article 8 applies at work. It is reasonable expectation of privacy. The question becomes whether in the concrete setting an employee could reasonably expect that his or her privacy would be respected (Galetta & De Hert, 2014). The answer depends on the nature of the activity, the presence and clarity of the rules at work and the intrusiveness of any monitoring. Ownership of the device while labelling may be important. So can if a measure is covert or overt then how long it lasts and how wide it ranges. The reason this test is important is because it leads to the justification stage. It is not conclusive. Even where expectations are reduced by clear or specific notice then a measure still requires

justification under Article 8(2). This avoids the erosion of privacy by broad disclaimers and keeps the core analysis one of legality and proportionality.

The first requirement of justification is lawfulness. It is not satisfied through any reference to rules. The legal basis has to be accessible and predictable in its operation. It should impose limits on discretion and provide safeguards against abuse (Ahonen et al., 2008). In labour settings, the basis may be a statute, a collective agreement, a clear internal policy or judge-made law. The label is not decisive. The quality is decisive. Rules that are hidden, vague or open ended will fail this limb. For an employee it should be possible to anticipate in advance when and how privacy would be curtailed, by whom, for what purpose and under what safeguards. This insistence on quality is what transforms the internal discipline into a human rights compliant framework. It permits differences in the form of national systems on the basis of converging on a common standard of protection.

A second limb relates to legitimate aims. Article 8(2) contains a closed list. In work disputes, there are three aims that can be seen over and over again. The protection of the rights and freedoms of the others, including property, the interests of customers and safety of colleagues (Gotthardt, 2020). The prevention of disorder or crime which frequently occurs within a loss prevention or sensitive assets context. The economic welfare of the country which sometimes can emerge when the discipline and continuity of services are at stake. The aim needs to be real and link with the interference. It cannot be a post-hoc justification for broad or indefinite measures. The manner in which domestic courts formulate and investigate the aim is therefore key to the quality of their reasoning under the Convention.

Necessity in a democratic society is the decisive enquiry. This is an expression of proportionality. The Court asks: Was there a pressing social need? and interference no more than required? In the labour context, that assessment is based on recurring and concrete factors. Prior notice and transparency are checked first. Scope and intrusiveness are then taken into account. A targeted and time-limited measure is easier to justify than a blanket and continuous measure (Kovač-Orlandić, 2020). The distinction between content and metadata is important. Covert measures invite a harsher scrutiny and must have heavy reasons. The availability of less intrusive means, is a constant test. If the same end could have been secured by sampling, by a narrower access, or a shorter retention, broad measures will fail. The sensitivity of data and quality of handling also count. Access controls, retention limits, audit trails and use-

limitation are all safeguards that affect the balance. Finally, consequences to the employee, such as dismissal or loss of reputation and fairness of proceedings, have a lot to do with it. These elements are not an abstract "to-do" list. They are the tools the Court uses to test whether domestic authorities struck a fair balance in real workplaces.

This way of Convention is within a larger European legal system. Neighbouring law is data-protection law. Its principles of notice, purpose limitation, data minimisation and storage limitation point in the same direction as Article 8 safeguards (Sychenko & Chernyaeva, 2019). But a compliance to one regime does not mean compliance to the other. A measure may be lawful under data rules, but fail the Convention test because the measure is disproportionate in the scope or effects it has. The reverse can occur theoretically as well. For an analysis of labour law the lesson is straightforward in practise. Data-protection principles can clarify how safeguards should be designed, but Article 8 supplies the final constitutional balance. It is the standard against which the national courts are still reviewed.

Variation across Member States raises two tensions which seem to go on. One is as to what counts as law for the lawfulness limb. Specific labour privacy legislation is based on some legal orders. Still others are based on general clauses in the civil code, case law, or collective agreements. Strasbourg has accepted many forms as long as the quality test is fulfilled (Ifeoma Ajunwa, 2017). That flexibility is a great thing, but it can cause the lines to blur and for employees and employers who work across boundaries to have inconsistent expectations. The second involves intensity of review. Member States have a margin of appreciation in organising the life of the workplace. That space is smaller with intrusions that are serious, covert or content-based, or where the safeguards are weak. It is wider where targeted measures are taken to address specific, credible risks and are set against a clear and foreseeable framework. The end result is not instability. It is an ordered form of deference which rewards careful ex ante design and careful ex post reasoning.

In labour practise in the EU, the consequences are real. Legislatures and regulators can minimise litigation by offering certain rules for monitoring, GPS, CTV and workplace IT, purpose statements, authorisation routes, oversight and retention schedules. Social partners can incorporate the same structure in collective agreements and internal policies which employees can read and understand. Employers may limit the measures to specific aims, keep access limited and record proportionality from the outset (Ásványi, 2022). Courts and tribunals can

impose reasons commensurate to the gravity of the measure, demand consideration of alternatives, or apportion factor-by-factor balance in decisions. Unions and workers can frame struggles in terms of gaps in the law, overbreadth of the law, lack of notice, improper treatment of data and discriminatory sanctions. These are not policy preferences. They are direct derivatives from the Convention test as applied to workplaces.

The doctrine also provides for limits. Article 8 does not create a zone of absolute secrecy at work. It does not disable legitimate management aims, security needs or loss prevention. It entails that such aims be pursued under rules of adequate quality, with safeguards and with a close fit between means and ends. It requires, too, that the more intrusive the step, the more serious must be the reason for taking it. When that logic is followed, domestic systems both comply with the Convention and maintain effective labour governance. In the event that it is not, Strasbourg will intervene. That is how Article 8, read as a living instrument, sets the constitutional baseline for privacy in EU workplaces today.

## 1.2 The broad and evolving concept of "private life"

Private life under Article 8 is broad. It does not possess a definite and exhaustive definition. It covers autonomy, identity and relations. It is not something restricted to the home and only intimate matters. The concept changes with social and technological change (Sychenko & Chernyaeva, 2019). The Convention is interpreted as a living instrument. Its scope changes with the conditions of the present day. New forms of personal activity, digital life may fall within them.

Personal autonomy is the key. Article 8 protects the space to shape ones life. It is a safeguard of self-development and dignity. It involves governance of personal information and lifestyle choices. The Court has also emphasised that private life is not an inner circle only. It contains the right to have a private social life. This means the ability to establish and maintain social ties. That understanding opens the door to work place settings. People develop identity and relationships at work as well.

The content of private life is contextual. It covers the physical and the psychological integrity. It also includes reputation, name, gender identity, sexuality and personal data. Any matter that is related to identity or personal development might fall inside it (Ponce Del Castillo & Molè, 2024). Matters that are clearly in the public domain can be outside it. Scholars have

called this the shift of privacy towards a personality right. The shift is helpful in addressing modern data and platform issues.

This breadth has two consequences for labour law. First, many work situations may engage Article 8 at the threshold. This includes personal communications, personal files at work and social interactions at work. These are related to identity and social life. Second, not everything at work is private. The analysis is based on the context. The blending of personal and professional is what is important.

This chapter takes an understandable approach. It recognises the broad scope of private life. It also recognises limits. It treats workplace situations as potentially within Article 8 where identity, autonomy, or relationships are affected (Buelens et al., 2016). It eschews the notion of a clear boundary between home and work. It also prevents that each workplace issue is a privacy issue. The goal is a balanced account that corresponds to doctrine and practise.

Finally, changing character of life: private life supports a cautious method. The remainder of the chapter will establish definitions of threshold tools and limits. It will then turn to lawfulness and aims. It will end with the necessity and proportionality. This sequence follows the structure of Article 8(2) and common academic treatment. It helps to keep the analysis focused on what is important for labour contexts.

## 1.3 Extending “private life” to the professional sphere

Private life under Article 8 reaches into work. Professional or business activity is not excluded by default. This means a person does not lose his or her protection against intrusion into privacy when entering the workplace (Sychenko & Chernyaeva, 2019). The approach of the Courts reflects the way of lived life of people. Most adults make relationships and develop social identity at work. These social ties belong to the private life and deserve respect.

Work settings can therefore fall within Article 8. Office premises and work communications could involve private life in which there is a personal element. This includes personal documents sitting at a desk, or private emails sent from an office email account. There is no hard-and-fast line to keep the professional sphere out of the privacy protection.

The extent of privacy at work is contextual. Some data or conduct will be purely professional and may not trigger Article 8. But where work and personal life overlap, Article 8 is usually engaged and a justification analysis becomes necessary (Ifeoma Ajunwa, 2017).

The effect is practical. Unlike excluding issues of lawfulness, aims and proportionality at the outset, it frames subsequent questions regarding it.

This extension also implies positive obligations. States must ensure that there is effective respect for employees private life in their disputes with private employers. Domestic laws and courts should offer rules and remedies to prevent arbitrary intrusions at work. In short, Article 8 applies in principle to the professional sphere. The details of any measure are then tried out against the qualified right structure that follows in this chapter.

## 1.4 “Reasonable expectation of privacy” as a threshold test

This test has a simple first question. Was the employee reasonably expected to have privacy in the circumstances? If yes, Article 8 is engaged. If no, there is usually no interference to justify. The test is important but not conclusive. This opens the door to the justification stage, it does not determine final outcome.

Expectation is contextual. It depends on such facts as prior notice, written policies, type of space or communication and intrusiveness of the measure (Gotthardt, 2020). Ownership of devices and labelling may also be significant. So may whether monitoring is covert or overt and its duration and scope. Where there is no advance notice, the expectation will be greater. Clear, specific notice can minimise it.

Employees may have a reasonable expectation in personal items or communications at work. Examples may include a personal folder on a work computer, or a private phone call made from the office. But an open-plan environment or an obvious monitoring policy can constrain that expectation.

Scholars note two cautions. For one, the test is applied flexibly. It is used in many surveillance contexts, but not in every Article 8 case (Ponce Del Castillo & Molè, 2024). This selective use makes for some uncertainty. Second, employers may attempt to manage expectations by general policies. If a policy states no privacy, however, the test could be weakened. For that reason, legality and proportionality are still insisted on in later sections even when expectation is not good.

In short, the expectation test is a gateway. It ensures that many workplace intrusions are examined under Article 8 rather than excluded at the outset. Once the gateway is passed, the analysis proceeds to a consideration of lawfulness, aims and proportionality.

## 1.5 The qualified nature of Article 8: lawfulness and legitimate aims

Article 8 is a qualified right. An interference can be justified if there are strict conditions. Three questions follow. Is the measure in accordance with the law? Is it seeking a legitimate objective? Is it required in a democratic society? This subsection deals with the first two.

There must be a basis in law. The law must be available and predictable. It needs to place limits and safeguards to avoid arbitrary action. In the workplace, this could mean statutes, clear internal policies, collective agreements or settled case-law, as long as they meet quality of law standards. Employees should be able to anticipate how and when privacy may be limited. Vague rules or holes in regulation will not satisfy this limb. A commonly used statement sums up the point: The law must be foreseeable and sufficiently clear in showing when measures affecting rights may be used.

In horizontal settings, lawfulness may be more difficult to define (Arroyo-Abad, 2021). The Court has occasionally accepted company policies or collective agreements as part of the legal structure. Scholars caution that a formal, foreseeable framework is the safer course to avoid arbitrary intrusions. The debate reflects a grey area: the degree of demands the quality of law test needs to be where private employers are active and the state plays a role through positive obligations.

Only aims listed in Article 8(2) qualify. These are national security, public safety, economic well-being, prevention of disorder or crime, protection of health or morals and protection of the rights and freedoms of others. In labour disputes, common objectives are the protection of the rights of others (such as property or safety), the prevention of disorder or crime and occasionally economic wellbeing. The purpose evoked must be real and relevant to the interference.

Lawfulness must have a clear and foreseeable framework with safeguards. The legitimate aim needs to be appropriate to the closed list of Conventions and the workplace context. These two elements are a necessary but not sufficient condition. The next subsection focuses on necessity and proportionality.

## 1.6 Necessity and proportionality

Even if an interference is lawful and pursues a legitimate aim, it must be **necessary in a democratic society**. This is a proportionality test. The measure must answer a pressing social

need and be no more than required to achieve the aim. The Court weighs the employee's privacy against the employer's or public interests. It checks if the degree of intrusion matches the importance of the aim.

In workplace contexts, all relevant circumstances are assessed. Key factors include prior notice, scope and intrusiveness, targeting vs blanket measures, the availability of less intrusive means, data sensitivity and handling and the narrowness of use. Safeguards such as limited access and retention rules also matter. If a narrower option could achieve the same aim, the measure is not necessary. The Court has articulated a structured approach for employment monitoring. It looks at whether employees were notified, how serious the intrusion was, whether the goal was specific and legitimate and whether the information gathered was used in a limited way. These considerations feed the final balance. States enjoy a margin of appreciation, but it is not unlimited. The Court supervises proportionality closely and will intervene where the balance is not reasonable. In sum, necessity requires convincing reasons, tailored measures and effective safeguards. Where the interference is excessive or poorly justified, Article 8(2) fails.

# 2. DIGITAL COMMUNICATIONS

## 2.1 Analysis

This chapter deals with privacy where employees are using phones, email, messaging and the internet at work. The starting point is simple. Communication made from work systems can be included in private life and correspondence (Mačiulaitis, 2023). That position was established early for office telephones and carried across to email and internet log. The result is that monitoring of digital use is usually a meddling with and must be justified. The key questions are lawfulness, a legitimate aim and necessity. The analysis then switches on context, notice, scope and safeguards. The classic example from the public sector illustrates the importance of a clear legal basis. In Copland, the college was a public body which kept records of telephone numbers, email addresses and web sites without warning or statute. That collection and storage of personal data were held to be an interference. The interference did not pass the lawfulness limb. The Court was not obliged to reach proportionality (Sychenko & Chernyaeva, 2019). The point for labour law is that traffic data and usage logs are not free for employers to take. A framework that is foreseeable is required before any monitoring can take place. Earlier, Halford had already recognised a reasonable expectation of privacy for calls made from an office line. There the issue was once again legality. There had been no regulation or control over the internal police system. Interception in such lines could not be justified without definite rules. The same case also linked Article 8 to effective remedies. Where there was no legal framework there was no effective remedy either.

Private-sector places lifted a different posture. In Brbulescu, the positive obligations of the States were at stake. The employer had prohibited the personal use and tracked a work messaging account. The national courts accepted the dismissal without testing key safeguards. The Grand Chamber set out what proportionality requires in monitoring in the workplace. Prior and specific notice is of the essence. Scope and intrusiveness needs to be looked at. Content access requires better reasons than traffic cheques. Less intrusive means must be considered (Galetta & De Hert, 2014). Use and consequences matter. On the facts, the domestic courts had not conducted that review and so violation was found. For labour law, this decision supplies the structure that national courts and employers are expected to use when digital monitoring is in issue. A series of cases then illustrate how expectations may be calibrated by internal rules and labelling. In Libert, a public-law employer opened files in a computer at

work and discovered a large cache of pornographic images. National law and a user charter imposed clear rules. Files marked private had a better protection and could be opened only in the presence of employees, except. The applicant had used a generic personal label, instead of the required term. The access and discharge of the courts were held to be proportionate. No violation was found. The implication is that foreseeable internal regimes can narrow expectations and provide for measured access, as long as there are safeguards and rules.

Finally, serious role specific contexts influence weight and outcome. In Adomaitis, calls from prison governors were intercepted by means of criminal intelligence powers. The probe was dropped but limited use of the material was permitted in discipline. The legal framework, authorisation and judicial control were decisive. The Court accepted that a fair balance had been struck. No violation was found. This shows that even content-level measures can be compatible with Article 8 where the aim is concrete, the setting is sensitive and use is tightly controlled. Across these authorities there are common issues. Many disputes remain centred on the lack or weakness of legal bases, notice quality and the leap from traffic data to content. The border between professional and private use, on workplace systems, also continues to be a recurring fault line. Each of the above cases are discussed in more details in the next sub-section for better understanding.

## 2.2 Case Study and Recommendations

**Relevant Case 1**

*Bărbulescu v Romania* [ECHR], No. 61496/08, [05.09.2017].

**Outcome:** Violation

In Bărbulescu v Romania the Grand Chamber sets out the most influential guidance on digital communications monitoring at work and shows, in a private employment setting, how the Article 8 framework described in Chapter 1 operates in practice. The applicant, an engineer, had been instructed to create a Yahoo Messenger account for customer support. His employer maintained internal rules prohibiting private use of company equipment and, relying on those rules, monitored the account during working hours, compiling logs and printouts of all conversations. These materials revealed that the applicant had exchanged messages with family members and others and they were used directly to justify his dismissal, the most severe disciplinary sanction available.

The Court began by confirming that Article 8 was engaged. In line with the broad understanding of "private life" and "correspondence" outlined in Chapter 1, it treated instant messaging as part of the applicant's private social life, even when the messages were sent from the workplace and through an account created for professional purposes. The employer's ownership of the IT infrastructure and the general prohibition on personal use were relevant context, but they did not, by themselves, extinguish the applicant's reasonable expectation of privacy. A crucial step in the Court's reasoning was that the applicant had never been given clear, specific notice that his employer might systematically monitor his messenger account or access and print the full content of his conversations. Applying the expectation-of-privacy gateway discussed in section 1.4, the Court therefore treated the monitoring as an interference with private life and correspondence that had to be justified under Article 8(2).

Structurally, the case is analysed under the States' positive obligations rather than as a direct complaint against a public employer. The dispute was between private parties, but Romania remained responsible for ensuring that its legal and judicial framework secured effective respect for Article 8 in labour relations, as outlined in section 1.1. The Grand Chamber did not insist on a single legislative model for workplace monitoring and accepted that Contracting States may rely on a combination of statutory rules, labour law and data-protection principles. What it did require was that domestic courts carry out a concrete and structured proportionality assessment, reflecting the bundle of factors highlighted in section 1.6: notice, scope and intrusiveness, legitimate aim, availability of less intrusive means, safeguards and the consequences for the employee.

On that basis the judgment formulates, in relatively general terms, what courts should examine when faced with employer monitoring of communications. Employees ought to receive prior and specific information not only that monitoring may occur but also about its nature, extent and the possibility of content access. The scope and intensity of the measure must be scrutinised: whether monitoring is limited in time, in the number of employees affected and in the types of data processed, or whether it amounts to broad and continuous surveillance. Domestic courts should identify the concrete purpose of the monitoring—for example, checking compliance with internal rules or protecting property—and then ask whether that aim could have been achieved by less intrusive means, such as relying on traffic data rather than content, narrowing the temporal window, or conducting targeted checks triggered by particular incidents. They must also take into account the sensitivity of the information obtained and the

seriousness of any disciplinary consequences, as well as the presence of safeguards such as restrictions on access, logging and effective judicial review. These elements echo almost point-for-point the proportionality grammar developed in Chapter 1.

Measured against this framework, the national decisions in Bărbulescu were found wanting. The Romanian courts did not determine whether the applicant had been adequately informed in advance that his employer might read and retain the substance of his personal messages. They failed to assess the actual extent of the monitoring, including how long it lasted and how many communications were captured and they did not consider whether the employer could have limited itself to examining traffic data or adopting a narrower measure focused on specific periods or suspicions. Little weight was given to the fact that the conversations contained strictly private exchanges with family members and that they were used to support dismissal, a sanction with obvious repercussions for the applicant's livelihood and reputation. Finally, the point at which the employer first accessed the content and the internal safeguards surrounding that access were left largely unexplored, creating precisely the sort of transparency deficit that the Article 8 requirement of "quality of law" and constrained discretion is designed to prevent.

In the absence of a careful balancing exercise along these lines, the Grand Chamber held that Romania had not fulfilled its positive obligation to secure respect for the applicant's private life and correspondence and found a violation of Article 8. For the purposes of this thesis, Bărbulescu crystallises several core propositions already signposted in Chapter 1. Workplace ownership of systems and abstract bans on private use do not eliminate the protection of Article 8; the decisive issues lie in specific notice, scope and intrusiveness, consideration of alternatives, safeguards and the gravity of the consequences. Access to the content of communications stands at the more intrusive end of digital monitoring and therefore requires particularly weighty reasons and well-designed safeguards. As such, the case occupies a central place within the digital communications theme of Chapter 2 and provides a template for the structured proportionality analysis that subsequent judgments and this thesis, seek to apply.

In Copland v the United Kingdom the Court addresses public-sector monitoring of workplace communications at an early stage in the development of digital technologies and uses the case to clarify the lawfulness limb of Article 8 in an employment setting. The applicant

worked in a state-administered further education college, initially as a personal assistant and later in close cooperation with a deputy principal. At the deputy principal's instigation, the college began monitoring her workplace communications. It obtained itemised telephone bills showing numbers dialled, dates, times, durations and costs; it logged the websites she visited, with timestamps and durations; and it recorded email traffic data, including addresses and timestamps. There was no college policy on monitoring at the time and, more generally, no domestic legislation in force that regulated employer surveillance of telephone, email or internet use. Later statutory schemes on interception and monitoring would be introduced, but these post-dated the events in question. Because the college was a public body, its actions were directly attributable to the State and the case was framed as one of negative obligations: the State's duty not to interfere with private life and correspondence without satisfying the requirements of Article 8(2).

The threshold question under Article 8 was readily resolved. Consistent with the broad and evolving concept of "private life" and "correspondence" described in Chapter 1, the Court recalled that it had already treated telephone calls made from business premises as falling within the scope of Article 8 and it extended the same logic to emails sent from work and to personal information derived from internet usage. In the absence of any warning that monitoring might occur, the applicant could reasonably expect a measure of privacy in her telephone calls and in her email and internet activity, even though these took place on her employer's systems. The systematic collection and storage of traffic data—who she called which sites she visited, when and for how long—was therefore characterised as an interference with her private life and correspondence. In line with the analytical framework of section 1.2 and 1.4, the Court emphasised that it was the gathering and retention of structured personal data about her communication patterns, without her knowledge, that engaged Article 8; it did not matter that the college could obtain itemised bills as a commercial customer, nor that the information was not disclosed to third parties or used in disciplinary proceedings.

Unlike in Bărbulescu, the decisive issue in Copland did not lie in proportionality but in lawfulness and the judgment is frequently cited for its insistence on the "quality of law" requirement outlined in section 1.5. For an interference to be "in accordance with the law", the underlying rules must be accessible and foreseeable: individuals must have a sufficiently clear indication of the circumstances and conditions in which public authorities may resort to monitoring measures. The Government argued that the college's statutory powers—formulated

in broad terms as powers to do what was "necessary or expedient" to provide education—were enough to authorise the monitoring. The Court rejected that argument. General institutional powers could not serve as a clear and specific legal basis for the systematic surveillance of personal communications. At the material time there were no provisions, either in domestic legislation or in the college's own regulatory instruments, that governed if, when or how an employer could monitor employees' telephone, email or internet use. From the perspective of the employee, there was thus no way to anticipate that her communication data might be collected and analysed in this way. On that basis the Court held that the interference failed at the lawfulness limb, without needing to proceed to the questions of legitimate aim or necessity in a democratic society.

Because lawfulness was absent, the Court expressly declined to decide whether there might be circumstances in which monitoring of workplace communications would be necessary and proportionate in pursuit of a legitimate aim. It left open, in principle, the possibility that properly regulated monitoring could be compatible with Article 8, thereby aligning with the qualified-right structure presented in Chapter 1: interferences are not excluded in the workplace, but they must rest on a clear, accessible and constrained framework that limits discretion and embeds safeguards. What Copland condemns is not the very idea of monitoring but public-sector monitoring conducted in a legal vacuum, where employees have neither prior notice nor any structured protection against arbitrary interference.

For the purposes of this thesis, Copland performs an important foundational role within the digital communications theme. It confirms that telephone, email and internet-use data generated at work fall squarely within the protection of Article 8 and illustrates how the expectation-of-privacy threshold and the requirement of "quality of law" operate when the employer is a public body. The case stands for a simple but far-reaching principle: public-sector monitoring of employee communications—whether content or traffic data—requires a clear, accessible and foreseeable legal basis with defined limits and safeguards. Absent such a framework, even the collection and retention of usage logs, without disclosure or disciplinary use, constitute an unlawful interference with private life and correspondence.

**Relevant Case 3**

*Libert v France* [ECHR], No. 588/13, [22.02.2018].

**Outcome:** No violation

In Libert v France the Court examined employer access to files stored on a work computer and, unlike in Bărbulescu, concluded that the national authorities had remained within their margin of appreciation under Article 8. The applicant worked for the French national railway company, SNCF. In 2008 the employer accessed the hard drive of his workstation in his absence and discovered a very large number of pornographic images and other non-professional material. The total volume of these files was substantial. On that basis the applicant was dismissed for abusing the company's IT facilities. He complained that his private life had been infringed because he had renamed the hard drive so that it appeared as a "personal data" disk and believed this label should have protected the contents from inspection.

Article 8 applied in principle. Consistent with the approach outlined in Chapter 1, the Court accepted that data clearly identifiable as non-professional and stored by an employee on a work device can fall within private life. SNCF allowed limited personal use of its computer systems, subject to internal rules. The opening of the files without the applicant's knowledge and outside his presence was treated as an interference with his private life. Since SNCF was a public-law entity under state supervision and providing a public service, the case was analysed from the angle of the state's negative obligation not to interfere with Article 8 rights, rather than as a question of positive obligations in a purely private employment relationship.

The interference was, however, found to be in accordance with the law. French labour law contained general proportionality conditions for restrictions on employees' rights and the case-law of the Court of Cassation had developed specific guidance on employer access to files stored on work computers. That case-law established a presumption that files on a professional computer are of a professional nature which the employer may consult in the employee's absence, unless they are clearly identified as private. At the same time, it provided a safeguard: files that are explicitly marked as private may only be opened in the employee's presence, save in exceptional circumstances. Read together, these rules formed a framework that indicated when and how employers could access stored data and the Strasbourg Court considered this sufficiently clear and foreseeable to satisfy the lawfulness requirement described in section 1.5.

A legitimate aim was also present. The measure was directed at protecting the rights of others, in this case the employer's interest in ensuring that its IT resources were used

consistently with contractual duties and internal rules. The immediate context was a decision to check the workstation because of concerns about misuse and the Court did not doubt the sincerity of that purpose. The main issue therefore became whether the interference was necessary in a democratic society within the meaning of Article 8(2), applying the proportionality grammar set out in Chapter 1.

On necessity, the Court attached weight to the way national law and internal policies calibrated the employee's expectation of privacy. French law required the employer to respect a safeguard for private life by insisting that files identified as private should only be opened in the employee's presence. The internal user charter at SNCF built on this by instructing staff to identify protected material using the specific label "private". The domestic courts found that the label chosen by the applicant, indicating "personal data" on the hard drive as a whole, did not correspond to this scheme. It was generic and could also refer to professional files handled personally by the employee; it did not clearly mark out particular folders or documents as belonging to his private sphere. The courts also took into account the sheer amount of storage space occupied by pornographic material and other non-professional content. In their view, this represented a serious and long-lasting breach of internal rules which justified a strict disciplinary response. On that basis they concluded that dismissal was not disproportionate.

The Strasbourg Court reviewed this reasoning and found it relevant and sufficient. It noted that the domestic courts had applied a national framework designed to balance private life at work with the employer's need to control the use of its equipment. They relied on the presumption that unmarked files are professional, on the protective rule that applies when data are explicitly marked as private and on the detailed internal charter communicated to staff. They also evaluated the gravity of the employee's misuse and the employer's interest in enforcing its rules. In these circumstances, the Court held that the state had not overstepped its margin of appreciation and that there had been no violation of Article 8.

The principle that emerges is narrow but significant for the digital communications theme. Employer access to files on a work computer can be compatible with Article 8 where there is a clear and accessible legal framework, where internal policies specify how employees can mark data as private, where the employee does not use the designated method to signal that protection and where the scope of access responds to serious and demonstrable misuse. The case shows how expectations of privacy at work can be shaped by labelling and policy and

how digital content stored on workplace IT may legitimately be used in disciplinary proceedings when proportionality and safeguards, as outlined in Chapter 1, are respected.

**Relevant Case 4**

*Halford v the United Kingdom* [ECHR], No. 20605/92, [25.06.1997].

**Outcome:**

Article 8: **Violation** (office telephones) / **No violation** (home telephone),

Article 13: **Violation** (office telephones)

In Halford v the United Kingdom the Court dealt with the interception of the telephone calls of a senior police officer and used the case to clarify both the expectation of privacy in workplace communications and the requirement of a clear legal framework for secret surveillance. Two sets of lines were at issue: first, the applicant's office telephones on an internal system operated by Merseyside Police; second, her home telephone on the public network. The background was a sex discrimination dispute brought by the applicant against her employer and she alleged that her calls had been intercepted in order to obtain material useful to the police in defending those proceedings. The case therefore arose squarely in an employment context but involved a public authority acting through its own telecommunications infrastructure.

Consistent with the broad understanding of private life and correspondence set out in Chapter 1, the Court had little difficulty in accepting that telephone calls made from business premises may fall within the scope of Article 8. The applicant could reasonably expect a degree of privacy when using her office lines for personal and professional communications. That expectation did not disappear merely because the phones belonged to the employer or because the system was an internal one run by a public body. The critical question, once an interference with Article 8 was established, was whether there was any lawful basis for intercepting those calls. On the evidence, the Court considered it reasonably probable that the office calls had been intercepted and that the purpose was to secure an advantage for the employer in the discrimination litigation. This amounted to an interference by a public authority and triggered the legality and proportionality tests described in section 1.5.

For secret surveillance measures, the Court repeated its established view that domestic law must be particularly clear and detailed. Individuals must be able to foresee, at least to a reasonable degree, in what circumstances and under what conditions the authorities are empowered to intercept communications. At the material time, however, United Kingdom law contained no provisions that regulated interception on internal telephone systems operated by public bodies such as Merseyside Police. There were statutory rules for interception on public networks, but nothing addressed calls made over the force's own internal lines. This regulatory gap meant that the interference with the applicant's office calls could not be regarded as "in accordance with the law" within the meaning of Article 8(2). The case therefore failed at the lawfulness limb and the Court found a violation of Article 8 in respect of the office telephones without needing to examine whether the interception pursued a legitimate aim or was necessary in a democratic society.

The position was different for the home telephone. The Court again accepted that Article 8 applied in principle to calls made from a private line, but here it focused on the factual question whether any interception had actually occurred. Unlike the situation with the office telephones, the applicant could not show, even on the standard of reasonable likelihood applied in secret-surveillance cases, that her home calls had been tapped. Earlier authorities where covert measures had been established were distinguished. In the absence of sufficient proof that any interception measure had been applied to the home line, the Court concluded that there had been no violation of Article 8 on that aspect of the complaint.

Article 13 which requires an effective domestic remedy for arguable breaches of the Convention, led to a parallel finding. As regards the office telephones, the absence of any legal framework governing interception on internal systems meant that there was also no effective remedy capable of addressing the applicant's Article 8 grievance; a violation of Article 13 was therefore found. For the home telephone, by contrast, there was no arguable claim of interception and thus no separate issue under Article 13. The Court awarded non-pecuniary damages and part of the pecuniary loss, together with a contribution to costs.

The principle that emerges from Halford remains relevant for digital communications. Employees may retain a reasonable expectation of privacy in calls made from work lines and interferences with such communications by public authorities must rest on a legal basis that is

accessible, foreseeable and sufficiently precise to prevent arbitrary secret surveillance. The mere fact that t

**Relevant Case 5**

*Adomaitis v Lithuania* [ECHR], No. 14833/18, [18.01.2022].

**Outcome:** No violation (Article 8), No violation (Article 6 §1)

In Adomaitis v Lithuania the Court examined the interception of a prison governor's telephone communications and the later use of that material in disciplinary proceedings and concluded that there had been no violation of either Article 8 or Article 6. The applicant was the governor of a high-risk prison. Criminal-intelligence measures were authorised against him on suspicion of abuse of office. His telephone communications were intercepted over a significant period. In the end the criminal investigation was discontinued for lack of evidence, but the authorities relied on parts of the intercepted material in disciplinary proceedings that led to his dismissal. The applicant complained that both the monitoring and the reliance on the resulting material infringed his right to respect for private life and that the domestic process was unfair.

The Court accepted, in line with the general approach described in Chapter 1, that telephone conversations fall within private life and correspondence and that covert interception of their content is a particularly serious interference. The key question therefore became whether the interference and the subsequent use of the data could be justified under Article 8(2). Here the judgment turns heavily on the quality of the domestic legal framework, the weight of the aims pursued and the way in which scope and use of the data were controlled. Lithuanian legislation provided for criminal-intelligence measures subject to authorisation and supervision. It laid down conditions for initiating interception, defined its possible scope and duration and regulated record-keeping, access and storage. Judicial authorisation and periodic review were built into the scheme and the existence of a paper trail for the operations reduced the scope for arbitrary action. Given the applicant's senior position in a sensitive institution, the Court had no difficulty in accepting that the authorities were pursuing legitimate aims, namely the prevention of disorder or crime and the protection of the rights of others, within an environment where abuses of office could have serious consequences.

When assessing necessity in a democratic society, the Court looked at the overall context rather than at the interception in isolation. The measure was undoubtedly intrusive,

since it involved content-level monitoring, but it was targeted at a single high-ranking official in a high-risk prison and based on tangible suspicions associated with his role. Authorisations had been issued, the duration and scope of the interception were subject to judicial control and the domestic courts later scrutinised both the legality of the measure and the fairness of relying on it in the employment context. Importantly, the intercepted material was used in discipline only to the extent necessary to resolve the specific employment issues in dispute. The national courts examined whether the disciplinary bodies had stayed within the purposes allowed by law, whether confidentiality and access controls had been respected and whether the applicant had a real opportunity to challenge the evidence and the inferences drawn from it. This part of the analysis connects closely to the proportionality grammar outlined in Chapter 1: the Court considered the seriousness of the suspicions, the targeting of the measure, the safeguards built into the legal framework and the narrow, employment-related use of the data.

Giving weight to that domestic scrutiny, the Court found that the Lithuanian authorities had struck a fair balance between the applicant's Article 8 rights and the public interest in preventing serious misconduct in a sensitive public service. It considered that the interception regime met the requirements of legal quality, that the scope of action and the later use of the material were sufficiently constrained and that the state had remained within its margin of appreciation. On the Article 6 complaint, the Court held that the disciplinary proceedings had not been unfair: the applicant could challenge the use of the intercepted communications and the domestic courts gave reasoned decisions addressing his arguments. No violation of Article 6 § 1 was therefore found.

The principle emerging from Adomaitis is that content-level interception of an employee's communications can, in exceptional circumstances, be compatible with Article 8 where there are serious, role-specific risks, where the measure is clearly authorised and supervised under a detailed legal framework and where any subsequent disciplinary use of the material is tightly linked to a legitimate aim and controlled by independent courts. Insuch conditions, the decisive factors are the quality of the law, the targeting and duration of the measure and strict limits on how the data are used. This case therefore marks the point, within the digital communications theme, where the Court accepts that highly intrusive monitoring may be justified when safeguards and use-limitation closely follow the standards set out in Chapter 1.

**Recommendations**

This chapter develops one central recommendation. Domestic legal orders should provide that any monitoring of the digital communications of employees should be based on a clear and foreseeable legal framework and that access to content should be used as an intrusive, exceptional measure to be justified only in the case where there are specific, weighty reasons to do so and other, less intrusive means would be inadequate. This claim follows from the qualified-right architecture of Article 8 and from the Courts treatment of workplace communications as part of private life and correspondence. In terms of legality, the need is not met by general managerial clauses or broad internal discretions, a rule of sufficient quality must specify when monitoring may be used, by whom, for what purposes and subject to what protections. In the terms of necessity, prior and specific notice should ordinarily precede any monitoring, the scope and duration should be targeted to the stated aim and access to content should be separately justified by concrete, case-linked considerations that cannot be addressed by traffic data or narrower tools. Where these conditions are not met, interferences with employees communications will be prone to fail at the in accordance with the law limb or at the proportionality stage.

A corollary recommendation is with respect to adjudication. National courts should carry out a structured analysis of proportionality in workplace monitoring disputes and require an evidential record enabling review on each element of the test. The analysis should cover, in order, existence and quality of legal basis, legitimacy and specificity of aim, intrusiveness of measure in view of the reasonable expectations of the employees, consideration of less intrusive means, handling, retention and access to data obtained and consequences visited upon the employee. Content access must be a different interference which increases the intensity of review. Omission of one or more of these elements subverts the test of fair balance and runs the risk of turning judicial scrutiny into deference to disciplinary results. A consistent, factor-by-factor approach is better too for foreseeability ex ante, because employers and workers can calibrate behaviour and policies with reference to the parameters that will later be applied in court.

These recommendations take into account the margin of appreciation while limiting arbitrariness. They do not deny that there may be serious institutional contexts, role-specific duties, or very concrete suspicions that justify incisive measures. Rather, they insist that such

measures are embedded in law of adequate quality and employed in a purpose bound, proportionate way which is open to judicial verification. Within the labour landscape of the European Unions, this approach harmonises at the Convention floor, without pre-empting choices by Member States on institutional design. Legislatures can ensure the implementation of the framework through statute, social partners can through collective agreements and clear user charters and regulators through audit trails, access logs and retention schedules. For their part, courts can require justification commensurate with the seriousness of intrusion and can deny reliance on evidence obtained or used beyond the prescribed bounds. In this way, the lawfulness and necessity requirements of Article 8 are given practical effect in the digital workplace and the integrity of both managerial prerogatives and worker dignity is preserved.

# 3. VISUAL & LOCATION MONITORING (CCTV AND GPS)

## 3.1 Analysis

“Private life” under Article 8 extends into the workplace. It covers the way a person builds professional and social identity at work and the recording of conduct that cannot be avoided during working hours (Antović and Mirković v. Montenegro). Even in public-facing spaces, continuous or systematic recording and later processing may affect private life. The expectation of privacy is context-dependent. It is highest in spaces such as toilets or cloakrooms. It remains meaningful in closed offices and classrooms. It is lower at open tills and customer areas, yet not extinguished (López Ribalda and Others v. Spain [GC], , Köpke v. Germany (dec.)) The first filter is lawfulness and the “quality of law”. Foreseeable legal bases are required. Duties to inform and to define purposes act as safeguards. Where a statute sets preconditions for video surveillance, those conditions must be observed and examined by courts. A failure to do so defeats lawfulness (Antović and Mirković). Judge-made safeguards may suffice where practice is well settled and protective in effect, especially when monitoring is narrow and targeted (Köpke (dec.)). Prior notice is a core element of foreseeability. Lack of prior notice is not always fatal, but it raises the bar for justification and for compensating safeguards (López Ribalda [GC]).

Legitimate aims usually arise. Protection of the rights of others, including property and the smooth running of the company, is commonly relied upon. Cost control for fleet mileage is a cognisable aim. By contrast, pedagogical oversight as such may fall outside enumerated statutory grounds when a specific law requires a danger to persons or property (Antović and Mirković). Aims must match uses. If the purpose is cost control, reliance on data for performance monitoring may be unlawful unless a separate and clear legal basis exists (Florindo de Almeida Vasconcelos Gramaxo v. Portugal) Necessity and proportionality require a granular assessment. The Court has distilled factors from workplace monitoring cases. Notice and transparency are first. Where notice is absent, other safeguards must be stronger. These include strict spatial targeting, short duration and limited access (López Ribalda [GC]). The scope and intrusiveness of the measure must fit the problem. Covert video over limited time at a public till, targeted at two suspected employees, was accepted as a narrow response to substantiated suspicion Köpke (dec.), . By contrast, continuous coverage of all checkouts without ex ante limits weighed against necessity at the Chamber stage of López Ribalda (López

Ribalda (Chamber)), although the Grand Chamber later found no violation owing to weighty reasons and robust safeguards (López Ribalda [GC]).

Less intrusive means must be assessed in context. Open cameras, visible supervision, or stock controls may be considered. If those options are likely to fail or to frustrate an investigation, covert and short-term measures can be justified. Evidence that alternatives are ineffective strengthens proportionality (Köpke (dec.), , López Ribalda [GC]). Data handling is also decisive. Access should be confined to a small group. Retention should be limited. Use must be tied to the stated aim. Domestic courts that exclude overbroad uses and rely only on purpose-linked metrics reduce intrusion and can bring the balance within the margin (Gramaxo) Across these cases, two patterns emerge. First, Article 8 applies across modalities: images, audio-free CCTV and GPS location/mileage. The intensity of review turns on context, safeguards and matching ends to means. Second, proportionality is not a single formula. It is a factor-by-factor record: notice, scope, duration, targeting, alternatives, access/retention and use-limitation. When that record is present and reasons are weighty, States remain within their margin. When statutory preconditions are ignored, or uses exceed purposes, a violation follows (Antović and Mirković, López Ribalda (Chamber), López Ribalda [GC], Köpke (dec.), Gramaxo, all).

## 3.2 Case Study and Recommendations

**Relevant Case 1**

*López Ribalda and Others v. Spain* [ECHR], Nos. 1874/13 and 8567/13, 17.10.2019. ECLI: ECLI:CE:ECHR:2019:1017JUD000187413.

**Outcome**: No violation.

In López Ribalda and Others v Spain the Grand Chamber considered covert video-surveillance in a supermarket and, for the first time, applied the Bărbulescu line of reasoning to workplace CCTV. The applicants were cashiers and sales assistants in a store that had been recording significant and unexplained stock losses over a long period. The employer already used visible cameras covering entrances and exits and had informed staff about those systems. When the losses continued, it installed additional cameras: some remained visible and were notified, others were hidden and focused on the checkout area. The employees were not told about these covert cameras. Over roughly ten days, the hidden devices recorded several workers stealing

items and colluding with customers. The employer dismissed the staff identified and relied on the footage in unfair-dismissal proceedings. The case reached Strasbourg because the employees argued that the secret filming and the use of the recordings in court breached their right to private life and, procedurally, their right to a fair hearing.

The Court began by accepting that Article 8 was engaged. Although the filming took place at work, in a public-facing area open to customers, systematic recording and subsequent processing of images from a defined group of employees still affected their private life within the meaning given in Chapter 1. The expectation of privacy at a supermarket checkout is necessarily limited: employees carry out their duties in front of the public and may reasonably foresee some degree of observation. However, that expectation does not disappear entirely and is altered when activities are recorded continuously and stored for later use. Prior information had been given about the visible cameras, but not about the covert tills-area system which created a transparency deficit. The Court therefore treated the surveillance as an interference with private life and turned to the three-part structure of Article 8(2), with particular emphasis on lawfulness and necessity.

On lawfulness, the judgment focuses on the quality of the domestic legal framework in a way that links back directly to section 1.5. Spanish law required data controllers to inform individuals about CCTV but also allowed competing interests to be weighed, including the protection of property and the prevention of wrongdoing. The Grand Chamber accepted that this framework was accessible and foreseeable in principle. The difficulty in the case was that the employer had not complied with the general duty to inform the staff about the new cameras. The Court did not treat that omission as automatically fatal. Instead, it held that, in the very specific circumstances of serious and ongoing stock losses and a concrete suspicion of concerted theft, the lack of prior notice could be justified by an overriding requirement to protect significant private interests. Advance warning, it reasoned, would likely have alerted those responsible and frustrated the investigation. The absence of notice therefore became one factor that had to be counterbalanced by stricter safeguards on scope, duration and use.

The core of the analysis lay in the proportionality assessment, where the Court expressly adapted the Bărbulescu criteria to video-surveillance. It examined the factors mapped in Chapter 1: the degree of information given to employees, the scope and intensity of monitoring, the weight of the reasons for it, the feasibility of less intrusive measures, the

consequences for those affected and the safeguards in place. The cameras recorded only images, not sound. Their angle was confined to the checkouts and their immediate surroundings, rather than to staff rooms or other more private spaces. The recording period was about ten days and the images were reviewed initially by the store manager, a legal representative of the company and a trade union representative. The footage was used solely to identify those involved in the thefts and to support disciplinary measures and litigation; there was no indication of broader or secondary use. The domestic courts considered whether the employer could have relied on less intrusive methods, such as extending the use of visible cameras or tightening stock controls and concluded that such methods had already been tried without success and that covert surveillance limited to the suspected zone was necessary to confirm and document the misconduct. In this context, the Court characterised the intrusion as not reaching a high level of seriousness when measured against the employer's interest in protecting its property and ensuring the proper functioning of the business.

Finally, the Grand Chamber framed the dispute in terms of Spain's positive obligation to secure respect for Article 8 in private employment relations and assessed whether the national courts had carried out a sufficiently structured balancing exercise. It emphasised that transparency is a fundamental safeguard in employment data processing and that the normal rule is that workers should be told when monitoring is in place. At the same time, it accepted that transparency is not absolute: exceptionally and only where there is an overriding requirement to protect important interests, prior information may be withheld, provided that other safeguards are correspondingly intensified. In López Ribalda those safeguards consisted of narrow spatial and temporal targeting, limited access to recordings, use of the material solely for the stated aim of clarifying the losses and disciplining those involved and detailed judicial review of the necessity and proportionality of the measure. On that basis, the Court held that Spain had remained within its margin of appreciation and that there had been no violation of Article 8. It also rejected the Article 6 complaint, finding that reliance on the footage in unfair-dismissal proceedings had not made the process unfair. The principle for labour law is that covert, short-term and targeted video-surveillance in a public-facing work area may be compatible with Article 8 where there is a concrete and serious suspicion of concerted misconduct, where less intrusive measures have proved insufficient and where robust safeguards constrain access, duration and use in line with the general proportionality framework developed in Chapter 1.

**Relevant Case 2 (Chamber)**

*López Ribalda and Others v. Spain* [ECHR], Nos. 1874/13 and 8567/13, 09.01.2018. ECLI: ECLI:CE:ECHR:2018:0109JUD000187413.

Outcome: Violation.

In López Ribalda and Others v Spain (Chamber judgment of 2018) the Court examined covert video-surveillance in a supermarket and, unlike the later Grand Chamber, concluded that Spain had not met its positive obligations under Article 8. The applicants worked as cashiers and sales assistants in a store that had experienced sustained stock losses. The employer already operated visible cameras at the entrances and exits and staff had been informed about those systems. It then installed additional, hidden cameras above the checkouts and in adjacent areas without informing the employees. Over a period that turned out to be about ten days, the covert cameras recorded several workers stealing items and colluding with customers. The applicants were dismissed and the recordings were used as evidence in unfair-dismissal proceedings.

The Chamber accepted that the surveillance constituted an interference with private life. The filming took place in a public-facing workspace, where employees inevitably operate in view of customers, but the Court stressed that systematic recording and subsequent processing of identifiable individuals can still affect private life. The employees were not singled out in advance; all staff working at the checkouts could be filmed throughout their working day. This combination of continuous recording, later review of the images and the clear identifiability of the workers was enough to bring Article 8 into play, in line with the broad and contextual understanding of private life set out in Chapter 1.

The crucial issue was the quality of the legal framework and, in particular, the obligation of transparency. Spanish data-protection law required that individuals be informed when they were subject to video-surveillance. In principle, therefore, there was a clear, accessible basis in domestic law that also imposed information duties designed to protect employees against arbitrary monitoring. In this case the employer had not informed the staff about the hidden cameras at the tills. For the Chamber, that failure undermined foreseeability in practice and removed an important safeguard. It accepted that the measures pursued a legitimate aim – protecting the company's property and ensuring the proper functioning of the

business – which falls within the protection of the rights of others under Article 8. However, it treated the absence of prior notice as a central defect rather than as a factor that could simply be offset by other considerations.

Necessity and proportionality were therefore decisive. The surveillance was covert; it covered all checkouts and all staff who worked there; it ran continuously during working hours; and no prior limit was set on the duration or on the group of employees to be monitored, even if in fact it ended after about ten days. The monitoring was not restricted to particular individuals against whom specific suspicions existed, nor to particular time bands linked to the losses. The employer also failed to show that less intrusive measures would have been ineffective. The Chamber indicated that alternatives, such as targeted checks, reinforcement of stock controls or time-limited observation of specific tills, had not been seriously explored or documented. Against that background, the lack of prior information became particularly weighty: a key safeguard identified in Chapter 1 was missing and the remaining safeguards on access, retention and use were not strong enough to compensate. Although access to the recordings was internal and the data were used mainly for dismissal and litigation, the consequences for the employees were serious and the breadth and opacity of the monitoring weighed heavily against a finding of necessity.

The Court also reviewed the approach of the domestic labour courts. They had accepted the footage and upheld the dismissals without conducting a sufficiently structured proportionality review along the lines later articulated in Bărbulescu and in the general framework of Chapter 1. In particular, they did not examine in detail the need for covert monitoring, the lack of prior notice, the breadth of the surveillance, or the possibility of less intrusive means. In the Chamber's view, this showed that Spain had not fulfilled its positive obligation to secure respect for private life in employment relations. A violation of Article 8 was therefore found by six votes to one, whereas Article 6 § 1 was not considered violated: the use of the recordings as evidence did not, in itself, render the proceedings unfair.

The judgment was later referred to the Grand Chamber which reached a different conclusion, but the Chamber's reasoning remains instructive for labour law. It illustrates a strict approach to transparency and targeting: covert and continuous camera monitoring of an entire work area, without prior notice and without tight limits in time and scope, is unlikely to be regarded as proportionate, even where there are genuine stock losses. Employers and courts

are expected to address and record why less intrusive alternatives would not suffice and to treat information duties as a central element of the Article 8 balance rather than an optional formality.

**Relevant Case 3**

*Antović and Mirković v. Montenegro* [ECHR], No. 70838/13, 28.11.2017. ECLI: ECLI:CE:ECHR:2017:1128JUD007083813.

Outcome: Violation.

In Antović and Mirković v Montenegro the Court considered overt CCTV in university classrooms and found a violation of Article 8, emphasising that private life extends into professional spaces and that statutory safeguards on video-surveillance must be taken seriously. The applicants were mathematics lecturers at the University of Montenegro. In 2011 the dean decided to install video cameras in seven amphitheatres and near his office. The stated aims were the safety of persons and property and the "surveillance of teaching". Access to the recordings was controlled by codes known only to the dean and the images were to be stored for up to one year. The lecturers complained to the national Personal Data Protection Agency which upheld their complaint and ordered removal of the cameras. In later civil proceedings, however, the domestic courts overturned that outcome, reasoning that amphitheatres were open spaces comparable to courtrooms or parliaments and that professors could not invoke privacy there.

The Strasbourg Court began by deciding that Article 8 was applicable. Drawing directly on the broad and contextual notion of private life outlined in Chapter 1, it treated the amphitheatres as workplaces where lecturers teach, interact with students and develop their professional social identity. Behaviour in that setting forms part of a person's private social life. Video recording in such a space produces a reproducible record of someone's conduct and, because it occurs during working hours in a place where staff are required to be, it cannot realistically be avoided. The Court underlined that the fact a workplace is open to the public does not reduce private life to zero and it rejected the domestic courts' attempt to equate the amphitheatres with purely public forums in which privacy interests would be negligible.

The central defect in the case lay in the lawfulness of the measure. Section 36 of Montenegro's Personal Data Protection Act set specific preconditions for the use of camera

surveillance, linked to concrete risks to persons or property and to clearly defined purposes. The Data Protection Agency had already found that these statutory conditions were not met: there was no proof of any particular danger justifying continuous recording and monitoring the quality of teaching did not fall within the permissible aims listed in the Act. The civil courts did not engage with those statutory requirements and instead treated the nature of the space as decisive. The European Court concluded that, in these circumstances, the surveillance was not "in accordance with the law" within the meaning of Article 8(2). The quality-of-law and foreseeability requirements identified in Chapter 1 were not satisfied, because the cameras were installed and operated outside the limits set by the domestic legislation that was supposed to structure and constrain such measures.

Necessity and proportionality reinforced this conclusion. The cameras covered multiple classrooms where teaching and academic interaction took place. Recording was continuous, retention was planned for up to one year and access was centralised in the hands of the dean. There was no time limit, no targeted suspicion directed at particular individuals and no assessment of less intrusive alternatives. The aims advanced included safety and property protection which are in principle legitimate and a more diffuse goal of supervising teaching which was not covered by the statute. Against the backdrop of a university environment, the Court highlighted that permanent observation risks chilling expression and pedagogy and that any interference with lecturers' private life at work must be supported by concrete reasons. In the absence of evidence of a specific security threat and with no serious attempt to consider narrower measures, continuous classroom recording could not be justified.

By four votes to three the Court found a violation of Article 8 and awarded each applicant a modest sum in non-pecuniary damages. For labour law, the case confirms and sharpens several points from the general framework in Chapter 1. First, overt CCTV in a workplace can engage private life even when the space is accessible to the public. Second, compliance with statutory conditions and safeguards is decisive: a broadly framed managerial preference for control or oversight cannot substitute for concrete risks and clearly defined purposes laid down in law. Third, employer rules and the public character of the workplace cannot reduce private life at work to nothing. Classroom CCTV that monitors teaching, without a concrete safety risk and without meeting statutory preconditions and safeguards, will be unlawful under Article 8.

**Relevant Case 4**

*Köpke v. Germany* (dec.) [ECHR], No. 420/07, 05.10.2010.

Outcome: Inadmissible (manifestly ill-founded).

In Köpke v Germany the Court examined covert video-surveillance at a supermarket checkout and, unlike in López Ribalda (Chamber), found that the State had complied with its positive obligations under Article 8. The applicant worked as a cashier in a supermarket where losses had been detected during stocktaking and accounting checks. Irregularities pointed to her department and suspicion focused on the applicant and another cashier. The employer engaged a private detective agency which installed hidden cameras overlooking the cash desk. The area filmed was open to the public; no audio was recorded. The recording ran for about two weeks and targeted only the two suspected cashiers. The footage showed behaviour treated as theft and the applicant was dismissed without notice. She challenged the dismissal before the labour courts which upheld it; a constitutional complaint also failed before the German Constitutional Court.

The Strasbourg Court accepted that the covert recording of the applicant's conduct at work constituted an interference with her private life. Even in a public-facing workspace, continuous recording and later processing of images of an identifiable individual engages Article 8, in line with the broad understanding of private life and workplace privacy set out in Chapter 1. The case was approached through the lens of positive obligations: the question was whether the domestic authorities, including the labour courts, had struck a fair balance between the applicant's right to respect for her private life, the employer's property rights under Article 1 of Protocol No. 1 and the public interest in the proper administration of justice.

At the material time there was no detailed statute in Germany governing workplace video-surveillance in the context of theft investigations. However, the Federal Labour Court had developed safeguards in its case-law and these judge-made rules were treated as part of the "law" for the purposes of Article 8(2). They required concrete indications of wrongdoing, a focus on the employees actually suspected and limitations in space and time. In Köpke those conditions were found to be satisfied. The cameras covered only the checkout area which was accessible to customers; the measure lasted for about two weeks; and only the two cashiers against whom there were specific suspicions were monitored. Access to the recordings was limited to staff of the detective agency and designated representatives of the employer and the

images were used solely to support the dismissal and in the ensuing labour-court proceedings. Against this background, the Court accepted that, in the absence of a statute, the combination of case-law safeguards and judicial control could still provide sufficient foreseeability and constraint to satisfy the lawfulness requirement discussed in Chapter 1.

Necessity and proportionality were also examined, with reasoning that foreshadows the later Bărbulescu criteria. The domestic courts had considered less intrusive means and explained why they were unlikely to achieve the same aim. Stocktaking and accounting checks had revealed discrepancies but could not identify the individual responsible. More visible forms of supervision, such as close observation by managers or open CCTV, were considered liable to alert potential wrongdoers and therefore unlikely to uncover covert theft. The surveillance, by contrast, was restricted to a public-facing location, of short duration and tightly targeted at employees against whom there was already a substantiated suspicion. The labour courts also noted that the measure had the collateral effect of exonerating other staff by narrowing responsibility to those filmed. In the Court's view, these factors reduced the weight of the interference and showed that the measure had been limited to what was necessary to protect the employer's property and support the proper functioning of the justice system in the dismissal proceedings.

In light of this reasoning, the European Court concluded that the national authorities had not overstepped their margin of appreciation. The balancing performed by the labour courts was reasoned and consistent with the safeguards developed in domestic case-law and the impact on the applicant's private life, while real, did not reach a level that would require a stricter legislative framework in this particular context. The application was declared inadmissible as manifestly ill-founded. For labour law, Köpke illustrates that tightly targeted, short-term covert video-surveillance at a public-facing checkout, deployed in response to concrete suspicions of theft and used only for dismissal and related proceedings, can satisfy Article 8's positive-obligations balance. It also suggests that generalised suspicion or broad, untargeted monitoring in similar settings would not meet the same standard under the proportionality framework developed in Chapter 1.

**Relevant Case 5**

*Florindo de Almeida Vasconcelos Gramaxo v. Portugal* [ECHR], No. 26968/16, 13.12.2022. ECLI: ECLI:CE:ECHR:2022:1213JUD002696816.

Outcome: No violation.

In Florindo de Almeida Vasconcelos Gramaxo v Portugal the Court considered GPS monitoring of a company car and the use of those data to justify dismissal. The applicant worked as a medical representative for a pharmaceutical company. His activity and expenses were recorded in a CRM system. In 2011 the employer installed GPS devices in the company vehicles and informed employees about the installation, its purpose and the possibility that discrepancies between GPS readings and CRM entries could have disciplinary consequences. The applicant signed a written acknowledgment of these terms. He later complained to the national data-protection authority (CNPD). In 2013 the CNPD discontinued the case, finding no breach of data-protection rules and the applicant did not challenge that decision. In 2014 he was dismissed after the employer cross-checked GPS mileage data against the CRM and concluded that he had systematically overstated professional kilometres and understated private use. GPS time data also suggested that he had not worked the expected number of hours per day.

The Court accepted that Article 8 was engaged. GPS tracking generates continuous location-linked information and allows a reconstruction of an individual's movements over time. In this case the device operated around the clock and the car could be used privately, subject to reimbursement for private mileage. The data therefore affected the applicant both during and outside working hours and their use in dismissal proceedings had serious consequences. In line with the general approach set out in Chapter 1, the question became whether the interference with private life could be justified and whether Portugal had fulfilled its positive obligation to secure respect for Article 8 in employment relations.

A protective domestic framework was in place. Portuguese law contained data-protection guarantees and labour-law limits on remote surveillance and the CNPD exercised oversight over GPS monitoring. The applicant did not argue that this framework was deficient in itself and did not seek judicial review of the CNPD's decision. The focus therefore shifted to the way the courts applied this framework in his particular case. On lawfulness and foreseeability, the Court noted that the applicant had been informed in advance about the installation of GPS, the purposes of its use and the potential disciplinary implications and that he had signed a document acknowledging these conditions. The stated purpose was to monitor mileage for business expense control. The GPS devices could not be switched off by employees

which meant that the system also captured movements during private use; this raised questions about scope and intrusiveness rather than about the existence of a legal basis.

The key step in the domestic reasoning and one that the Strasbourg Court attached weight to, was the Court of Appeal's decision to narrow the permissible use of the GPS data. Relying on the Labour Code's prohibition of certain forms of remote surveillance, it held that GPS information could not lawfully be used to monitor performance or working hours. It therefore excluded the time-of-day evidence from the dismissal case and confined reliance to the distance-driven data for expense control. This interpretive move aligned the actual use of the GPS logs with the legitimate aim that had been notified to employees at the outset, namely the protection of the employer's property and the prevention of inflated travel costs and it reduced the interference with the applicant's private life. The applicant did not contest the accuracy of the mileage readings or the fact that they diverged from his own CRM entries. Circulation of the data was also considered: access was limited to staff responsible for assigning visits and approving expenses rather than being shared more widely.

Against this background, the Court examined whether the domestic authorities had struck a fair balance between the applicant's privacy and the employer's interest in monitoring costs. It accepted that the employer's property interests and the integrity of its expense system fell under the protection of the rights of others for the purposes of Article 8 § 2. It also accepted that continuous GPS tracking of a mixed-use vehicle is intrusive and engages expectations of privacy, particularly where use spills over into non-working time. However, it considered that the combination of prior information, written acknowledgment, data-protection oversight and the Court of Appeal's use-limitation analysis had scaled the interference down to what was necessary for the stated aim. By excluding reliance on GPS to assess working hours and by treating that type of use as unlawful remote surveillance, the domestic courts retrospectively corrected the employer's initial overreach and confined the processing to the mileage aspect. In doing so they applied several of the proportionality factors described in Chapter 1: they clarified the legal basis, defined the purpose, limited the scope of data use, considered the sensitivity and consequences and ensured that access was restricted.

The European Court concluded that Portugal had remained within its margin of appreciation and that there had been no failure to secure respect for the applicant's private life. It also rejected the Article 6 complaint, holding that the use of lawfully obtained mileage data,

within the narrowed purpose defined by the Court of Appeal, did not make the proceedings unfair. For labour law, the case illustrates that GPS monitoring of company vehicles may be compatible with Article 8 when employees are informed in advance, when data are used in a purpose-bound way for mileage and cost control and when access and circulation are limited. It also indicates that extending such monitoring to performance or timekeeping raises separate and stricter questions under the prohibition of remote surveillance and may be unlawful unless supported by a clear, narrowly framed justification and additional safeguards.

**Recommendations**

Workplace visual and geolocation monitoring should be authorised only within a narrow, purpose-bound framework. The legal basis should be clear and foreseeable. It should define the aims, the tools and the safeguards. Prior information should normally be given. Where prior information would frustrate an ongoing investigation into serious misconduct, covert monitoring should be allowed only as an exception, with documented overriding reasons and enhanced safeguards (López Ribalda [GC]). Statutory preconditions, where they exist, should be applied in substance and not in form. Courts should not treat workplaces as privacy-free zones. Private life continues to exist at work and cannot be reduced to zero, including in teaching spaces and other professional settings (Antović and Mirković).

The scope of monitoring should be limited ex ante. Spatial and temporal limits should be set before deployment. Narrow angles and short durations should be preferred. Audio recording should be excluded unless a compelling and specific necessity is proven. Continuous or blanket recording should be avoided, save for exceptional risk. Any covert measure should be targeted to concrete suspicion, focused on defined areas and time-limited. The less intrusive means should be considered and recorded. If open measures or human checks would defeat the purpose, this should be reasoned in writing (Köpke (dec.), , López Ribalda [GC]).

Use-limitation should be enforced. Data should be used only for the stated aim. If CCTV was installed to detect stock losses, the footage should not be repurposed for performance appraisal or general discipline. If GPS was deployed for mileage control, the data should not be used for timekeeping or behavioural monitoring without a separate and lawful basis (Florindo de Almeida Vasconcelos Gramaxo). Access should be restricted to a small group. Retention should be short and linked to procedural needs. Access logs should be maintained. Secondary disclosure should be exceptional and justified.

Courts should give effect to the quality-of-law requirement. Where statutes set conditions for video surveillance, those conditions must be applied and reviewed. Failure to examine those conditions should lead to a finding of unlawfulness (Antović and Mirković). Judicial review should remain sensitive to context. Public-facing tills create a lower expectation of privacy, but not its extinction. Classrooms and offices require heightened caution. This differentiation should be explicit in judgments (López Ribalda [GC]).

On the other hand, Decision-makers should adopt a factor-by-factor proportionality record. Each deployment should address, in sequence: notice and transparency, spatial and temporal scope, targeting and the degree of intrusion, existence and effectiveness of less intrusive means, access controls and retention, use-limitation and the concrete consequences for employees. Each factor should be reasoned on the facts. Where prior information is absent, compensating safeguards should be stronger and expressly recorded (López Ribalda [GC]).

In adjudication, courts should respect the margin of appreciation while restraining arbitrariness. The margin should widen where safeguards are robust, the suspicion is concrete and the measure is narrow and brief (Köpke (dec.)). The margin should contract where statutory preconditions are ignored, the measure is continuous or blanket, or the use drifts beyond its stated aim (Antović and Mirković). Purpose fidelity should be policed in practice. Where mixed-purpose systems exist, only the metrics tied to the lawful aim should be relied upon. Other uses should be excluded unless independently justified and authorised (Gramaxo).

This structured method would promote even-handed outcomes across modalities. It would treat images, audio-free video and GPS data under the same proportionality grammar, while recognising their different intrusiveness. It would also align workplace privacy with legitimate managerial interests in property protection, operational continuity and cost control, within Article 8's requirements for lawfulness, legitimate aim and necessity.

# 4. IDENTITY, VETTING & SENSITIVE PERSONAL DATA AT WORK

## 4.1 Analysis

Article 8 protects private life in employment settings where identity and sensitive data determine access to posts and continuity of work. Private life covers employability, reputation

and the handling of confidential information. Medical records, criminal-record data and security files all fall within its scope. Storage, retention and disclosure for hiring or dismissal decisions are interferences that must be justified by law, aim and strict necessity. The five cases trace a common structure. First, the quality of law is tested. Clear and foreseeable rules are required for collecting, retaining and disclosing sensitive data. The rules should define purposes, access roles and time limits. They should also provide supervision and remedies. Where statutory preconditions exist, they must be applied in substance. Where rules are only policy, or are drafted in very broad terms, foreseeability weakens. This theme is consistent across medical confidentiality, criminal-record vetting and secret security files (I. v. Finland, M.M. v. the United Kingdom, Rotaru v. Romania, all ).

The intensity of privacy is highest for medical data. In I. v. Finland, the system allowed hospital-wide reading of an HIV-positive nurse's records and had no audit trail. The absence of technical logging prevented proof of unlawful access. The Court required practical and effective safeguards ex ante. Role-based access, traceability and early pseudonymisation were viewed as necessary. Ex post compensation could not replace upfront protection. Lawfulness failed in practice because the system design did not meet statutory standards and proportionality failed because less intrusive configuration was available and not used. Criminal-record regimes require precision and filtering. In M.M., non-conviction data were retained and disclosed on an open-ended basis for vetting. The change to lifetime retention for a caution was policy-driven and not grounded in clear statute. No assessment of seriousness, time elapsed, or relevance to the post was required. Deletion was exceptional and largely unavailable. The Court found that such indiscriminate retention and disclosure lacked sufficient safeguards and thus was not in accordance with the law. The interference was therefore unjustified. The decision confirms that employability and reputation form part of private life, especially as time passes and the event recedes.

Secret security files raise special questions. Two different models appear. In Rotaru, the keeping and later use of historic political data were permitted by law in general terms, but the framework had no limits on what could be recorded, who could be targeted, access rights, or retention duration. Oversight was minimal. The absence of precise and reviewable rules meant that storage and use were not "in accordance with the law." The Court therefore found a violation and also found that no effective remedy existed to challenge accuracy or retention (Articles 8 and 13, Article 6 on the ignored damages claim). In Leander, by contrast, a security-

vetting system for a national-security post was supported by statute, supervisory authorities and ministerial responsibility. Individual access to the file was refused, but compensating oversight existed. Use was tied to a sensitive installation. A wide margin of appreciation was recognised. No violation was found. Leander marks the upper bound of deference where secrecy is inherent but balanced by a structured framework and independent supervision. Discrimination concerns may arise where sensitive identity data become the basis for blanket exclusions. In Sidabras and Džiautas, a ten-year ban was imposed on former KGB staff across public service and many private-sector areas. The law lacked post-by-post definitions, individualised assessment and review mechanisms. The restriction extended deep into private employment, where loyalty to the State is not an inherent condition. The Court found a violation of Article 14 taken with Article 8. Employability and reputation were harmed by a broad rule detached from present risk and role-specific need. This case shows that even weighty aims such as national security or democratic transition cannot justify indiscriminate bans that spill into ordinary private work without tailoring and safeguards.

Across the cases, legitimate aims are usually accepted. Patient safety, safeguarding, integrity of public service and national security are recognised. The decisive questions concern fit and safeguards. Purpose limitation is central. Data gathered for one aim should not be repurposed without a separate and lawful basis. The protection of property or integrity may justify targeted use, but general performance monitoring or broad exclusion requires additional justification and clear law. Access must be role-based. Retention must be time-bound and reviewable. Accuracy must be enforceable through correction or challenge. Independent oversight should be available and, where secrecy is necessary, compensating mechanisms must exist to prevent arbitrariness (I. v. Finland, M.M., Rotaru, Leander, all). Positive obligations structure the analysis. States must provide frameworks that make protection practical and effective. Technical and organisational measures matter. Logging, access controls and erasure schedules operationalise Article 8. Judicial control matters too. Courts should be able to check whether purposes are narrow, whether alternatives were examined and whether consequences for employment are proportionate. Where that structure is present and the post is security-sensitive with tailored use and independent oversight, a wide margin may be respected (Leander). Where statutory precision, remedies, or safeguards are missing, violations follow (I. v. Finland, M.M., Rotaru, Sidabras and Džiautas, all).

The doctrine therefore sets a coherent grammar for identity, vetting and sensitive data at work. Lawfulness demands clarity and limits. Legitimate aims must match uses. Necessity requires factor-by-factor proportionality. Secrecy may be tolerated in national security, but only with strong safeguards. Private life continues to include employability and reputation and blanket, unreviewable exclusions cannot stand (all ).

## 4.2 Case Study and Recommendations

**Relevant Case 1**

*Sidabras and Džiautas v. Lithuania* [ECHR], Nos. 55480/00 and 59330/00, 27.07.2004.

Outcome: Violation (Article 14 taken with Article 8).

In Sidabras and Džiautas v Lithuania the Court examined wide-ranging employment bans imposed on former KGB staff and treated them as an unjustified interference with private life, combined with discriminatory treatment on grounds of past institutional affiliation. The applicants had worked for the Soviet KGB but, after Lithuanian independence, had been able to obtain public posts; one became a tax inspector and the other a prosecutor. In 1999 a statute was brought into force imposing restrictions on access to employment for former KGB officers. On the basis of this law both applicants were dismissed. They challenged their dismissals and the restrictions before the domestic courts. One was refused the benefit of statutory exceptions; the other initially succeeded but that judgment was overturned on appeal.

The Strasbourg Court approached the case through Article 8 taken together with Article 14. Consistent with the broad conception of private life developed in Chapter 1, it treated employability, professional development and external social relationships as elements of private life. A person's ability to earn a living, to move between jobs and to maintain a reputation compatible with ordinary participation in the labour market forms part of their private sphere. The bans in question affected the applicants' prospects across large parts of the economy and altered how they were perceived. Article 8 was therefore engaged and because the restrictions applied to a specific group defined by their status as former KGB officers, Article 14 was also applicable in conjunction with Article 8.

There was no dispute that the interference had a basis in statute, but the Court considered the quality of that law to be central. The Act imposed a ten-year employment ban

from its entry into force. It covered not only the civil service and posts exercising public authority but also a wide range of private sector occupations. The law did not clearly define which specific posts, functions or tasks were off-limits. It did not require any individualised assessment of present loyalty, current conduct or concrete risk. Its exceptions were narrow and, as the applicants' cases illustrated, applied inconsistently. This lack of precision weakened foreseeability and limited the capacity of the domestic courts to exercise meaningful review, even though a formal legal basis existed.

The aims pursued were accepted as weighty. Lithuania wished to distance its new institutions from a repressive security apparatus and to prevent repetition of past abuses. The Court recognised that national security, public order, economic well-being and the protection of the rights of others could justify restrictions on access to certain sensitive public posts. The difficulty lay in necessity and proportionality. Rather than focusing on particular high-risk roles, the measure relied on a historic status as such, without examining whether the individuals concerned posed any present threat. It did not distinguish between positions involving the exercise of sovereign powers and ordinary private employment. The Court explicitly rejected the idea that loyalty to the state, in the sense relevant to national security, could be treated as an inherent condition for private-sector work. The extension of the ban into numerous private occupations was not supported by any demonstration of need. Less intrusive means had not been considered: the legislature had not explored targeted exclusions, conditions on access, supervisory arrangements or mechanisms for periodic review. The law also entered into force long after the applicants had left the KGB—thirteen and nine years respectively—disrupting careers that had developed in the meantime and aggravating the impact of the measure.

Procedural safeguards were correspondingly weak. The statutory scheme did not require individual, reasoned decisions supported by evidence of specific risks. Judicial review was constrained by the breadth and vagueness of the categories and there was no built-in requirement to reassess or remove the restriction before the expiry of the fixed ten-year term. In these circumstances the Court concluded that the difference in treatment between former KGB staff and other citizens was not reasonably proportionate to the aims pursued. It found a violation of Article 14 taken together with Article 8. No violation of Article 10 was found, since the dismissals and employment bans concerned the nature of the applicants' past employment rather than their present opinions or expression. Just satisfaction was awarded in respect of damage and costs.

For labour law, the case establishes that blanket employment bans based solely on historic institutional affiliation, applied without individual risk assessment, clear job definitions or review mechanisms, are likely to be disproportionate when they extend into the private sector and severely restrict employability and reputation. In the terms of the general framework set out in Chapter 1, the quality of the law, the scope and duration of the measure, the sensitivity of the underlying vetting data and the absence of tailored safeguards all count heavily against proportionality under Article 8 read with Article 14.

**Relevant Case 2**

*I. v. Finland* [ECHR], No. 20511/03, 17.07.2008. ECLI: ECLI:CE:ECHR:2008:0717JUD002051103.

Outcome: Violation.

In I. v Finland the Court dealt with the confidentiality of an employee's hospital records and found a violation of Article 8, stressing the need for practical and effective safeguards where highly sensitive health data are concerned. The applicant was a nurse in a public hospital and was receiving treatment for HIV at the same hospital's infectious diseases clinic. Over time she came to suspect that colleagues who were not involved in her care knew about her diagnosis. At the material time, the hospital's electronic patient register allowed wide internal access: staff across different units could consult diagnoses and treating doctors, including for patients they were not treating. When the applicant raised her concerns with her doctor, the hospital restricted access to personnel in the infectious diseases clinic, registered her under a pseudonym and arranged for a new social security number. These measures, however, came only after the risk of unauthorised access had already arisen.

The Court had no difficulty in finding that Article 8 was applicable. Medical information lies at the core of private life and HIV status is among the most sensitive categories of health data because of the stigma and social consequences associated with disclosure. Confidence in health services depends on the assurance that such information will remain confidential. In this case, the structure of the hospital's records system created a realistic risk that colleagues could read the applicant's file out of curiosity or for other improper reasons. At the same time, the system did not log user access in a way that would allow later verification. The applicant therefore could not prove who had consulted her record, even though the configuration of the system made such access technically possible.

The central issue was the quality of the legal and technical safeguards rather than the existence of a statutory framework on paper. Domestic law required hospitals to control access to patient records

and to maintain audit trails that would make it possible to check who had viewed a file. In practice, the hospital's system did neither at the relevant time: it allowed reading by staff not involved in treatment and did not record access events. The later introduction of restrictions to the treating unit, a pseudonym and a new social security number did not cure the earlier period during which the applicant's data had been widely visible and unlogged. In civil proceedings, the domestic courts placed the burden on the applicant to show specific instances of unlawful access, effectively ignoring the acknowledged systemic deficiencies and the fact that the lack of audit trails made such proof practically impossible. From the Court's perspective, this meant that the statutory safeguards were not being applied in a way that was practical and effective, as required by Article 8 and by the emphasis in Chapter 1 on the "quality of law" and enforceable constraints on discretion.

In its necessity and proportionality analysis the Court underlined that less intrusive designs and stronger safeguards had been available from the outset. Access could have been limited to the treating clinic and other clearly defined roles, with proper logging to allow accountability. Pseudonymisation and changes to identifying numbers could have been considered as preventive tools rather than as belated fixes. Instead, the hospital operated a broad-access, non-audited system until after the applicant's concerns surfaced and the domestic courts then relied on the absence of evidence of concrete misuse to reject her claim. The Court held that ex post civil remedies cannot compensate for the failure to put in place ex ante technical and organisational measures that prevent or at least discourage unauthorised access to highly sensitive health information. It therefore found a unanimous violation of Article 8 and awarded compensation for both pecuniary and non-pecuniary damage.

For labour law and workplace privacy, the case underlines that when employers or public bodies hold employees' medical records, Article 8 requires role-based, auditable and purpose-limited access, especially for conditions such as HIV where stigma is acute. A framework that exists on paper but is not implemented in system design and access control does not satisfy the requirement of practical and effective protection and courts cannot simply shift the burden onto the employee to identify individual breaches when the very structure of the system makes such proof impossible.

**Relevant Case 3**

*M.M. v. the United Kingdom* [ECHR], No. 24029/07, 13.11.2012.

Outcome: Violation.

In M.M. v the United Kingdom the Court considered the retention and disclosure of non-conviction criminal-justice data in employment vetting and found a violation of Article 8, focusing on the lack of clear statutory safeguards and contextual assessment. The applicant,

who lived in Northern Ireland, had been arrested in 2000 after taking her infant grandson for a day in an attempt to prevent his departure abroad following a family breakdown. The prosecution was not pursued; instead she accepted a police caution for child abduction. At that point, policy suggested a five-year retention period. Later, however, the police changed their practice so that cautions in child-related cases were to be retained for life, in effect until the person reached the age of 100. In 2006 the applicant received a conditional job offer in the health sector. She disclosed the caution and a criminal-record check confirmed it. The offer was withdrawn and she complained that the open-ended retention and disclosure of the caution data damaged her employment prospects and violated her right to respect for private life.

The Court accepted that Article 8 was engaged. In line with the approach outlined in Chapter 1, it treated the storage of personal data and their disclosure in vetting as matters that can significantly affect a person's private life. A caution, although arising from criminal proceedings, becomes part of an individual's private sphere as time passes, especially where the underlying incident occurred in a domestic context rather than in public. Systematic central storage enables authorities to bring that event back into view long after it would otherwise have faded from social memory. Disclosure in an employment context directly affects reputation and employability which the Court has repeatedly recognised as aspects of private life. The fact that the applicant signed the vetting form and technically "consented" to the check did not remove the interference: in reality, there was no genuine choice where the employer was entitled to insist on a criminal-record certificate as a condition of hiring.

The judgment turned on the quality of the legal framework rather than on the idea of vetting itself. In Northern Ireland there was no clear, detailed statutory scheme governing the collection, retention and disclosure of caution data. Recording and initial retention were automatic in practice, deletion was rare and reserved for "exceptional" cases and a policy change had extended retention to life for categories such as the applicant's without any legislative debate or structured safeguards. The legislation regulating standard and enhanced disclosures did not differentiate by seriousness of the offence, by context, by time elapsed since the event or by the specific nature of the post applied for. It did not provide for any assessment of relevance before disclosure or for any consideration of whether the person posed an ongoing risk. In the terms used in Chapter 1, the system lacked "quality of law": it did not clearly specify when data would be collected, how long they would be kept, who could access them, for what purposes they could be used and under what conditions they would be erased. The

Court therefore concluded that the arrangements did not provide sufficient safeguards against disproportionate interference and that the retention and disclosure could not be regarded as "in accordance with the law".

Legitimate aims were not in dispute. The Court accepted that public protection and safeguarding, particularly in relation to children and vulnerable adults, are important objectives and that maintaining comprehensive criminal-history records can be legitimate. However, it emphasised that breadth must be matched by safeguards. A system that retains and discloses non-conviction data indefinitely, without filtering and without contextual judgment, fails to demonstrate that the interference is necessary in a democratic society. In the applicant's case no account was taken of the specific circumstances of the caution, of the twelve-year lapse of time by the date of the Strasbourg proceedings, or of the role she wished to take up. There was no tiered "look-back" period, no mechanism for distinguishing minor or one-off incidents from serious offences and no provision for case-by-case balancing at the disclosure stage.

On this basis the Court found that the interference with the applicant's private life was disproportionate. The combination of lifetime retention, automatic disclosure in vetting and the absence of clear statutory rules and filtering criteria produced an indiscriminate and open-ended scheme. In the language of Chapter 1, the system failed on several proportionality factors at once: scope was extremely broad in time and in personal reach; less intrusive options such as time-limited retention, anonymisation or relevance testing were not built in; and the consequences for employability were serious, as shown by the withdrawal of the job offer. The Court unanimously held that Article 8 had been violated. No damages were claimed, but the judgment signalled that retention and disclosure of non-conviction data must be grounded in a clear legal scheme with safeguards, filtering and case-sensitive assessment, particularly where vetting decisions affect access to work. For labour law, M.M. underscores that open-ended, automatic use of historic caution data in employment screening is incompatible with Article 8 and that employers and public authorities must operate vetting systems that are both lawful in form and proportionate in substance.

**Relevant Case 4**

*Rotaru v. Romania* [GC] [ECHR], No. 28341/95, 04.05.2000.

Outcome: Violation (Article 8, also Article 13 and Article 6 §1).

In Rotaru v Romania the Grand Chamber examined the retention and use of a secret security file held by the intelligence service and found a violation of Article 8, together with breaches of Articles 13 and 6. The applicant had been convicted in 1948 for political criticism of the new regime. Decades later, in 1992, he applied for benefits available to victims of political persecution. In those proceedings the Ministry of the Interior produced a letter from the intelligence service summarising entries from a security file kept on him. The letter set out historic information about his studies and political activity in the 1940s and claimed that he had been a member of a far-right movement in 1937. The applicant maintained that this last allegation was false. He brought a civil action seeking damages and an order to amend or destroy the file. The domestic courts rejected his claim on the basis that the intelligence service was merely the "depositary" of archives inherited from the former security apparatus and had no power to alter them. Only years later did the service admit that the membership entry concerned another person with the same name. A review court then nullified that specific entry without awarding damages.

The Court treated the case as a classic example of secret-file interference with private life. Consistent with the broad notion of private life explained in Chapter 1, it held that the systematic collection and storage of personalised information by a security agency, particularly where it includes a person's political history and criminal record, falls within Article 8. The file in question had been kept for decades and contained biographical and political data whose continued retention and use could affect the applicant's reputation and civic standing. The interference was reinforced by the use of the file in court, coupled with the refusal to allow effective refutation of the allegedly false material. Article 8 was therefore clearly applicable.

The central issue lay in the lawfulness and quality of the legal framework. Romanian law allowed the intelligence service to take over and use the archives of the former security services, but it did not set out with any precision the scope and manner of those powers. There were no rules identifying what kinds of data could be recorded which categories of person could be targeted, or under what conditions data could be stored and used. The provision governing access to archives did not specify who could consult files, the procedure for access or the purposes for which consultation was permitted. The national security clause itself was drafted at a high level of generality, without detailed criteria or safeguards. There was also no system of independent supervision, either while the files were being used or afterwards. In the vocabulary of Chapter 1, the law lacked the "quality" required by Article 8: it did not indicate

with reasonable clarity the scope and limits of discretion and therefore did not enable individuals to foresee in a meaningful way how their data might be stored or deployed. The Court concluded that the storage and use of the applicant's file were not "in accordance with the law" and this finding was sufficient to establish a violation of Article 8 without proceeding to a full necessity test.

The absence of clear rules also undermined the effectiveness of remedies. The applicant had no realistic way to contest the existence, accuracy or retention of the file. The general civil action suggested by the Government had not been shown to work in practice: in his own case the courts simply declined to engage with the substance of the complaints on the ground that the intelligence service could not alter the archives. Later legislation on the opening of former security files did not offer any mechanism for challenging the accuracy of entries or the continued storage of data. The Court therefore found a violation of Article 13. It also held that Article 6 § 1 had been breached because the Court of Appeal failed to examine the claim for damages and costs, thereby depriving the applicant of a fair hearing on a crucial aspect of his case.

From the perspective of labour law and employment vetting, Rotaru illustrates the limits that Article 8 imposes on secret security files used to shape a person's civil status or employability. Where historic political or security information may be relied upon in decisions affecting access to public functions or other significant opportunities, it must be governed by clear, precise and reviewable legal rules. Those rules need to define what data may be collected, for how long, who may access it and for which purposes and they must be complemented by mechanisms for access, correction and erasure. In the absence of such safeguards and with no meaningful oversight or remedies, retention and use of security files are not in accordance with the law under Article 8, regardless of the weight of the national security aims invoked.

**Relevant Case 5**

*Leander v. Sweden* [ECHR], No. 9248/81, 26.03.1987. ECLI: ECLI:CE:ECHR:1987:0326JUD000924881.

Outcome: No violation (Articles 8 and 13, no separate breach under Article 10).

In Leander v Sweden the Court examined a secret security-vetting system used to refuse a job in a military installation and, unlike in Rotaru, found no violation of Articles 8 or 13. The

applicant had applied for a technical post at a naval museum located inside a military base. Appointment to that post was conditional on "personnel control" which meant that the security services queried a confidential register. An adverse entry was returned and, on that basis, the applicant was refused the job. He was never told the substance of the information which led to his exclusion. He complained that the storing and secret use of this data and the impossibility of seeing or challenging it directly, violated his right to respect for private life and denied him an effective remedy.

The Court accepted that Article 8 was engaged. Consistent with the broad conception of private life set out in Chapter 1, it treated the systematic collection and storage of personal data in a security register and their use in decisions affecting access to employment, as an interference with private life. The fact that the applicant never gained access to the underlying material did not remove the issue from the scope of Article 8: the decisive point was that personal information about him had been kept and consulted in secret and then used to determine his suitability for a specific post.

The core of the Court's reasoning lay in the assessment of "lawfulness" and the "quality of law". Unlike the vague framework criticised in Rotaru, Sweden's personnel-control regime rested on a combination of statute and detailed regulations. These rules governed the keeping and consultation of security registers for clearly defined sensitive posts connected with national defence. They also set out institutional safeguards: supervision by the Parliamentary Ombudsman and the Chancellor of Justice and political responsibility of ministers for the acts of the security services. The Court accepted that, taken together, these elements formed a legal framework that was accessible and foreseeable, even though it did not include a general right of individuals to see the contents of their own security files.

The legitimate aim was straightforward. The post in question lay within a defence installation and the vetting system pursued national-security objectives by seeking to ensure that only reliable candidates were appointed to positions where they might obtain information relevant to the defence of the State. The Court therefore moved to the necessity and proportionality analysis, applying the qualified-right structure already mapped in Chapter 1 but with a wide margin of appreciation in view of the security context.

On necessity, the Court acknowledged that secrecy is inherently troubling from the standpoint of individual rights: the applicant could not confront or correct the entries that had

harmed his prospects. However, it accepted that, for security vetting to be effective and for informants to be protected, some secrecy may be unavoidable. The question then became whether there were compensating safeguards that could substitute for adversarial access. Here the Court placed considerable weight on the existence of independent oversight and on the narrow use of the information. Complaints could be made to the Ombudsman or the Chancellor of Justice, both of whom had full access to the files and could examine whether the security services had acted within the law. Ministers were politically accountable to Parliament. The information drawn from the register appears to have been used only to assess the applicant's suitability for this particular sensitive post; there was no indication of wider dissemination or use for broader employment blacklisting. In this specific setting, the Court considered that the combination of a clear legal basis, institutional supervision and purpose-limited use of the data struck a fair balance between the applicant's private life and the interests of national security.

Article 13 was examined in parallel. The absence of a right to inspect the security file did not in itself amount to a lack of effective remedy. The Court noted that the applicant could challenge the legality of the vetting through complaints to the supervisory authorities and, more generally, through political and judicial channels. In the specialised context of national-security vetting, these mechanisms were considered sufficient to satisfy Article 13. No separate violation of Article 10 was found, as the adverse entry was treated as a security-suitability assessment rather than a sanction for the applicant's opinions.

From a labour-law perspective, Leander shows the outer boundary of what Article 8 will tolerate in security-vetting schemes. Where there is a clear and detailed legal framework, where the use of confidential data is tightly linked to a defined category of national-security posts and where robust independent oversight compensates for the absence of individual access to the file, secret security-vetting registers may be compatible with Article 8. Secrecy alone is not decisive; what matters is whether quality of law, purpose limitation and supervisory safeguards together provide enough structure to keep interferences with employability within the margin of appreciation recognised in Chapter 1.

**Recommendations**

Rules on medical confidentiality, criminal-record disclosure and security vetting should be set out in clear and foreseeable statutes. The legislation should define purposes, access roles, retention periods, review rights and oversight. Policies alone should not suffice where

employment prospects and reputation are at stake. Indiscriminate or open-ended retention and disclosure should be prohibited. Filters should be statutory, not merely administrative. The framework should require case-specific assessment before disclosure to an employer, with reasons recorded. These features address the lawfulness and foreseeability deficits identified in criminal-record systems and secret-file regimes (M.M. v. the United Kingdom, Rotaru v. Romania). Secrecy in national-security vetting may be accepted, but only when embedded in a precise legal scheme with independent supervision (Leander v. Sweden).

Purpose limitation should be codified. Medical records should be accessible only for care or strictly defined occupational health purposes. Criminal-record data should be disclosed only for posts where the offence type, seniority and risk profile make disclosure necessary. Security-vetting files should be queried only for roles classified by statute as sensitive and only for suitability assessments. Repurposing should require a separate legal basis and a new proportionality test. These constraints track the Court's insistence on a tight fit between aim and use (M.M., Rotaru, Leander).

Protection must be practical and effective in system design, not only in after-the-fact remedies. Statutes should mandate role-based access controls, comprehensive audit logging and tamper-resistant logs for all access to health records and vetting registers. Access should be limited to those with a defined treatment, assessment, or vetting function. Logs should be reviewable by independent bodies and disclosed to the data subject where compatible with the aim. Pseudonymisation should be applied where possible. Early measures of this kind would have avoided the inability to trace unlawful access to medical records (I. v. Finland).

Retention should be time-bound and linked to necessity. For medical data, retention should follow clinical and occupational health schedules, with stricter rules for highly sensitive diagnoses. For criminal-record disclosures, look-back periods should be tiered by seriousness, elapsed time and the nature of the post. Automatic lifetime retention for non-conviction data should be barred. For security files, retention schedules should be published at a level of generality compatible with secrecy, with independent approval and periodic culling. The Court has criticised lifetime and open-ended retention without filtering or review (M.M., Rotaru).

Decision-makers should prepare a factor-by-factor proportionality record for every disclosure or adverse employment decision based on sensitive data. The record should address: purpose and legal basis, data minimisation, role-based access, time elapsed, relevance of the

data to the specific post, alternative measures (such as conditions, supervision, or training) and the foreseeable impact on employability. Where disclosure is refused or limited, the reasons should be logged. Where disclosure is made, the employer's use should be confined to the recorded purpose. This method operationalises the Court's requirement for a granular necessity assessment (M.M., Leander). Effective remedies should be guaranteed. Individuals should have the right to request access, a summary of reasons and correction or deletion, subject to necessary limitations in security cases. An independent authority should verify accuracy, lawfulness and proportionality. Courts should have power to order corrections, erasures and compensation. A mere possibility of post hoc damages is not sufficient where systemic safeguards are missing (I. v. Finland, Rotaru). In the security domain, secrecy-compatible remedies should include complaints to an ombudsman or specialised tribunal with full file access and powers to direct correction or sealed undertakings. This aligns with the model accepted in Leander while avoiding the defects condemned in Rotaru (HUDOC).

Employment prohibitions based on historic affiliation or status should be narrowly tailored. Any exclusion should be tied to specific functions that genuinely require loyalty or security, with reasons documented and subject to review. Private-sector work should not be restricted unless the post is demonstrably sensitive. Rehabilitation and elapsed time should be recognised. Where risk can be mitigated by conditions, that route should be preferred over categorical bans. The Court has rejected broad, decade-long prohibitions that spilled into ordinary private occupations without definitions or individualised assessment (Sidabras and Džiautas v. Lithuania). Tailored criteria, periodic review and appeal reduce arbitrariness and protect employability and reputation within Article 8 and Article 14.

Secrecy may be necessary to protect sources and methods, but secrecy cannot replace legality. A two-pillar approach is recommended. First, enact a precise statutory scheme that defines sensitive posts, authorises classified checks and regulates storage, access, sharing and retention. Second, provide compensating safeguards: an independent overseer with full access, ministerial or parliamentary accountability and a route for individuals to lodge complaints and receive a gist or outcome-focused reasons so far as possible. This balance reflects the deference accorded where safeguards are robust (Leander) and avoids the indeterminate discretion condemned where limits and oversight were absent (Rotaru).

# CONCLUSION

The aims of the thesis have been achieved and the research questions have been answered. Article 8 was shown to govern workplace situations whenever behaviour or identity is recorded or processed for employment purposes. Employer ownership of systems and the public-facing nature of a workspace do not remove applicability. Professional spaces remain within private life. Expectations of privacy vary by context, but they are not reduced to zero in ordinary work areas or in routine communications.

The analysis confirms that private life includes employability, reputation and the systems that determine access to posts and the continuation of work. Communications environments, visual and location monitoring, medical records, criminal-record mechanisms and security vetting files all constitute interferences that require justification. Positive obligations are engaged in employment disputes. Domestic courts are required to perform an Article-8-compliant balance between competing interests and to ensure that safeguards are practical and effective in operation.

The decisive element across all modalities is the quality of law. Clear and foreseeable rules are required on purposes, access roles, retention ceilings, oversight and remedies. Policy-only frameworks and vague mandates do not provide adequate protection. Purpose fidelity is required. Data gathered for one aim may not be reused for another without a separate legal basis and a renewed necessity assessment. Judicial reasoning should therefore track the declared aim and should police use-limitation in practice.

Necessity turns on narrowness and targeting. Spatial, temporal and personal limits, coupled with short duration, are indicators of a proportionate design. Continuous or blanket recording is suspect and demands stronger reasons and stronger safeguards. Less intrusive means must be considered in real time and rejected with reasons that are recorded. Failure to document this analysis weighs against proportionality. Notice remains a default safeguard. Where prior notice is not given for overriding reasons, compensating controls must be strengthened and recorded contemporaneously.

Handling and lifecycle controls are central. Role-based access, audit logging and short, purpose-linked retention are necessary to make protection effective in practice. Ex post compensation does not replace the need for ex ante technical and organisational safeguards.

The sensitivity of the data affects the strictness of the review. Health information and secret security files require the strongest protections. Content of communications requires more protection than traffic or mileage data. The legal analysis must therefore calibrate safeguards to the level of sensitivity and ensure that the depth of justification matches the potential harm.

Consequences for the worker influence the intensity of review. Dismissal, loss of profession, or broad exclusion from parts of the labour market require weightier reasons and tighter safeguards. Blanket, status-based exclusions that extend into ordinary private employment are disproportionate where they lack individual assessment, clear job definitions, or review mechanisms. In the national security sphere, secrecy may be tolerated, but only within a precise legal framework that limits the roles for which vetting is performed, confines use to those roles and provides independent supervision capable of testing legality and proportionality.

In light of these conclusions, two proposals follow. First, purpose-bound statutory schemes should govern workplace monitoring, medical confidentiality, criminal-record disclosure and vetting registers. The law should define purposes, access roles, retention limits, oversight and remedies and should require a factor-by-factor proportionality record for each deployment or disclosure. Second, ex ante safeguards should be mandated as a matter of design. Role-based access, comprehensive logging, short retention aligned to the stated aim, documented consideration of less intrusive means and strengthened compensating controls where notice is withheld should be compulsory. These measures would ensure that Article 8 protection in labour law is practical and effective while allowing targeted, justified uses of data where truly necessary.

# REFERENCES

*Legal Acts*


1. European Convention on Human Rights, 4 November 1950, ETS No. 5 (as amended).
2. Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.
4. Council of Europe Convention 108+ for the Protection of Individuals with regard to Automatic Processing of Personal Data (as modernised), CETS No. 223.
5. Directive 2002/58/EC (ePrivacy Directive) — of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002, p. 37–47.
6. Directive (EU) 2016/680 (Law-Enforcement Directive) — of 27 April 2016 on processing by competent authorities for crime prevention, OJ L 119, 4.5.2016, p. 89–131.
7. Committee of Ministers Recommendation CM/Rec(2015)5 — on the processing of personal data in the context of employment.


*Special Literature*


1. Ahonen, P., Alahuhta, P., Daskala, B., Delaitre, S., Hert, P. D., Lindner, R., Maghiros, I., Moscibroda, A., Schreurs, W., & Verlinden, M. (2008). Dark scenarios. In D. Wright, M. Friedewald, Y. Punie, S. Gutwirth, & E. Vildjiounaite (Eds), *Safeguards in a World of Ambient Intelligence* (Vol. 1, pp. 33–142). Springer Netherlands. https://doi.org/10.1007/978-1-4020-6662-7_3
2. Albuquerque, P. P. D. (2021). The Rights of Workers, Migrant Workers and Trade Unions in the Light of the European Convention on Human Rights: Права працівників, працівників-мігрантів та профспілок за Конвенцією про захист прав людини і основоположних свобод. *Philosophy of Law and General Theory of Law*, *1*, 224–246. https://doi.org/10.21564/2707-7039.1.247534
3. Aloisi, A., & De Stefano, V. (2022). Essential jobs, remote work and digital surveillance: Addressing the COVID-19 pandemic panopticon. *International Labour Review*, *161*(2), 289–314. https://doi.org/10.1111/ilr.12219

4. Arroyo-Abad, C. (2021). Teleworking: A New Reality Conditioned by the Right to Privacy. *Laws*, *10*(3), 64. https://doi.org/10.3390/laws10030064
5. Ásványi, Z. (2022). Technology vs privacy at work: The extent and limitations of organizational control mechanisms. *Management*, *27*(2), 261–282. https://doi.org/10.30924/mjcmi.27.2.14
6. Bernardini, L., & Sanvitale, F. (2023). Searches and seizures of electronic devices in european criminal proceedings:a new pattern for independent review? *Revista Ítalo-Española de Derecho Procesal*, *1*, 73–119. https://doi.org/10.37417/rivitsproc/1475
7. Buelens, W., Herijgers, C., & Illegems, S. (2016). The View of the European Court of Human Rights on Competent Patients' Right of Informed Consent. Research in the Light of Articles 3 and 8 of the European Convention on Human Rights. *European Journal of Health Law*, *23*(5), 481–509. https://doi.org/10.1163/15718093-12341388
8. Galetta, A., & De Hert, P. (2014). Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance. *Utrecht Law Review*, *10*(1), 55. https://doi.org/10.18352/ulr.257
9. Gotthardt, M. (2020). Effective enforcement of EU labour law: A comparative example. *European Labour Law Journal*, *11*(4), 403–412. https://doi.org/10.1177/2031952520905385
10. Harris, D., O'Boyle, M., Bates, E., & Buckley, C. M. (2023). *Harris, O'Boyle and Warbrick: Law of the European Convention on Human Rights* (5th edn). Oxford University Press. https://doi.org/10.1093/he/9780198862000.001.0001
11. Ifeoma Ajunwa, K. C. (2017). *Limitless Worker Surveillance*. https://doi.org/10.15779/Z38BR8MF94
12. Josephina, A., & Andreas, A. (2019). Case Study The Internet of Things and Ethics. *The ORBIT Journal*, *2*(2), 1–29. https://doi.org/10.29297/orbit.v2i2.111
13. Karas, Ž. (2018). *PRIVACY RIGHTS AND POLICING UNDER THE INFLUENCE OF MODERN DATA TECHNOLOGIES*. EU LAW IN CONTEXT – ADJUSTMENT TO MEMBERSHIP AND CHALLENGES OF THE ENLARGEMENT. https://doi.org/10.25234/eclic/7119

14. Koukiadaki, A. (2024). Enforcement of EU Labour Law: Legal foundations and the role of the CJEU. *European Labour Law Journal*, *15*(4), 623–640. https://doi.org/10.1177/20319525241295517
15. Kovač-Orlandić, M. (2020). Employee's right to privacy: Where is the bound of the employer's right to monitor employees' communications. *Strani Pravni Zivot*, *4*, 85–99. https://doi.org/10.5937/spz64-29470
16. Ligthart, S. L. T. J. (2019). Coercive neuroimaging, criminal law and privacy: A European perspective. *Journal of Law and the Biosciences*, *6*(1), 289–309. https://doi.org/10.1093/jlb/lsz015
17. Lugaresi, N. (2017). INTERNET LAW TRENDS IN EUROPE: A CASE LAW PERSPECTIVE - 10.12818/P.0304-2340.2017vBIP305. *Revista Da Faculdade de Direito Da UFMG*, *BI*. https://doi.org/10.12818/P.0304-2340.2017vBIP305
18. M. Yaroshenko, O., O. Melnychuk, N., Ye. Lutsenko, O., M. Vapnyarchuk, N., & I. Sheverdina, V. (2024). EMPLOYEE'S RIGHT TO INFORMATION IN ECHR JUDGMENTS: ANALYSIS OF SPECIFIC CASES WHERE THIS RIGHT WAS VIOLATED OR RECOGNIZED - DOI: 10.12818/P.0304-2340.2024v84p335. *Revista Da Faculdade de Direito Da UFMG*, *84*. https://doi.org/10.12818/P.0304-2340.2024v84p335
19. Mačiulaitis, V. (2023). Boundaries of the employee's privacy in employment relationship. *Entrepreneurship and Sustainability Issues*, *10*(3), 186–198. https://doi.org/10.9770/jesi.2023.10.3(13)
20. Molè, M., & Mangan, D. (2023). 'Just more surveillance': The ECtHR and workplace monitoring. *European Labour Law Journal*, *14*(4), 694–700. https://doi.org/10.1177/20319525231201274
21. Monitoring and Surveillance in the Workplace: Lessons Learnt? – Investigating the International Legal Position. (2007). *Journal of Digital Forensics, Security and Law*. https://doi.org/10.15394/jdfsl.2007.1021
22. Pollicino, O. (2022). The Transatlantic Dimension of the Judicial Protection of Fundamental Rights Online. *The Italian Review of International and Comparative Law*, *1*(2), 277–310. https://doi.org/10.1163/27725650-01020004

23. Ponce Del Castillo, A., & Molè, M. (2024). Worker monitoring vs worker surveillance: The need for a legal differentiation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4861237
24. Sychenko, E., & Chernyaeva, D. (2019). The Impact of the ECHR on Employee's Privacy Protection. *Italian Labour Law E-Journal*, *Vol 12*, 171-188 Pages. https://doi.org/10.6092/ISSN.1561-8048/10015
25. Van Der Sloot, B. (2015). Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data". *Utrecht Journal of International and European Law*, *31*(80), 25–50. https://doi.org/10.5334/ujiel.cp

*Case Law*

1. Bărbulescu v. Romania [ECHR], No. 61496/08, 05.09.2017.
2. Copland v. the United Kingdom [ECHR], No. 62617/00, 03.04.2007.
3. Libert v. France [ECHR], No. 588/13, 22.02.2018.
4. Halford v. the United Kingdom [ECHR], No. 20605/92, 25.06.1997.
5. Adomaitis v. Lithuania [ECHR], No. 14833/18, 18.01.2022.
6. López Ribalda and Others v. Spain [ECHR], Nos. 1874/13 and 8567/13, 17.10.2019 (GC).
7. López Ribalda and Others v. Spain (Chamber), 09.01.2018.
8. Antović and Mirković v. Montenegro [ECHR], No. 70838/13, 28.11.2017.
9. Köpke v. Germany (dec.) [ECHR], No. 420/07, 05.10.2010.
10. Florindo de Almeida Vasconcelos Gramaxo v. Portugal [ECHR], No. 26968/16, 13.12.2022.
11. Sidabras and Džiautas v. Lithuania [ECHR], Nos. 55480/00 and 59330/00, 27.07.2004.
12. I v. Finland [ECHR], No. 20511/03, 17.07.2008.
13. M.M. v. the United Kingdom [ECHR], No. 24029/07, 13.11.2012.
14. Rotaru v. Romania [ECHR] (GC), No. 28341/95, 04.05.2000.
15. Leander v. Sweden [ECHR], No. 9248/81, 26.03.1987.

# SUMMARY

The thesis examined when and how Article 8 of the European Convention on Human Rights applied to workplace settings and which factors guided the proportionality analysis across three domains: professional communications, visual and location surveillance and identity, vetting and other sensitive-data systems. A doctrinal analysis of leading European Court of Human Rights judgments was conducted and the results were synthesised into a structured, factor-by-factor framework suitable for labour-law disputes. It was shown that Article 8 covered professional spaces, workplace communications and systems that determined employability and reputation. Outcomes were driven by the quality and foreseeability of the legal basis, fidelity to stated purposes, narrow targeting in person, place and time, limits on access and retention and the gravity of consequences for the worker, all viewed within a margin of appreciation that widened with robust safeguards and contracted with overbreadth. Notice was confirmed as a default safeguard; where prior notice was withheld, overriding reasons and compensating controls were required and less intrusive means had to be assessed and recorded contemporaneously. Higher protection was required for medical data and secret security files, while mileage or traffic data received lighter scrutiny when use remained purpose-bound. The thesis contributed a unified proportionality grammar that could be applied across modalities without converting the inquiry into a GDPR chapter. Practical implications included the need for purpose-bound legal frameworks and ex ante technical and organisational measures (role-based access, comprehensive logging, short, purpose-linked retention and documented alternatives) to make Article 8 protection effective in labour relations while permitting targeted, justified monitoring where strictly necessary.