2025, Vol. 14, Issue 2

Tomasz Mirosławski

University of Miskolc, The Central European Academy in Budapest
https://orcid.org/0000-0002-7758-7415
https://doi.org/10.21697/2025.14.2.04

WORKPLACE MONITORING IN EUROPE: A REVIEW OF REGULATORY PERSPECTIVES AND DEVELOPMENTS

Abstract: The main focus of the article is to examine the evolution of European regulations covering workplace monitoring, focusing on the Council of Europe and European Union frameworks. It analyses how concepts of human rights, understanding of privacy and data protection standards, particularly the ECHR, CFREU, Convention 108+ and GDPR, shape national approaches to the issue of employee surveillance. Emphasis is placed on proportionality, transparency and human dignity as core principles guiding social partners in defining employee privacy in the modern surveillance age. The study highlights that the effectiveness of a current framework depends on coherent national implementation, adaptability to digitalisation and active social dialogues addressing emerging monitoring technologies within workplaces.

Keywords: workplace monitoring, employee privacy, European Union law, Council of Europe, data protection

1. Introduction

The issue of monitoring in the workplace and, even broader, the issue of the right to privacy, which encompasses monitoring, has become an integral element of labour law over time. However, phenomena such as the dynamic development of technology in recent decades, its impact on worker privacy and the increasing pressure to globalise markets and the work process itself, have resulted in the demand for appropriate regulation to address and protect against the negative effects of these changes.[1] In this

1 Hendrickx, "Privacy 4.0 at Work: Regulating Employment, Technology and Automation", 147.

context, international and European regulations have played a significant role. On many occasions, such regulations have set new standards and provided a reference point for national legislators. Therefore, even when analysing national models of workplace monitoring, it is still desirable to refer to the provisions addressing this issue in the international dimension.

The main emphasis of the article will be primarily on European regulations operating within the framework of the Council of Europe (CoE) and the European Union (EU), as they are of fundamental relevance to the European states' national workplace monitoring and employees' personal data protection systems.

As the topic of workplace monitoring from a human rights perspective is extremely broad and given that the purpose of this article is to provide a comprehensive overview of the European regulations governing the issue of surveillance within the employment sphere, the discussion on European human rights protection mechanisms will be limited to a brief outline.

2. European Regulations Covering Workplace Monitoring

When approaching the issue of workplace monitoring from the perspective of European regulations, two legal orders must be taken into account: the first, set by the CoE, and the second, operating within the EU. The two legal orders permeate each other, and within them we can distinguish legal instruments of different significance in terms of their legal binding force and area of application, such as: conventions, acts with the rank of treaty, regulations, as well as recommendations and opinions of working groups.[2]

2.1. Human Rights Perspective

The analysis should begin with European mechanisms for the protection of human rights. Within the CoE, the legal instrument underpinning the protection of human rights is the European Convention on Human Rights (ECHR), which has an international character. In turn, in the EU, such a basis is the Charter of Fundamental Rights of the EU (CFREU), which is of a supranational nature.[3]

2 Otto, *The Right to Privacy in Employment – A Comparative Analysis*, 115.

3 Fabbrini, "The European Multilevel System for the Protection of Fundamental Rights", 9.

The ECHR does not directly address the issue of privacy in employment, including monitoring, but guarantees in Article 8 the general right to respect for private and family life. The explicit articulation of this right in the Convention provided a new direction for national privacy laws in Member States.[4]

Paragraph 1 of Article 8 of the ECHR states that 'Everyone has the right to respect for his private and family life, his home and his correspondence.' However, the second paragraph of the article indicates the possibility of certain derogations, as it provides that,

> [t]here shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[5]

The general concept of the right to privacy under Article 8 of the ECHR has gradually evolved, under the influence of the ECtHR jurisprudence, covering also the right to personal data protection[6] and the right to privacy in the employment context.[7] In addition, over time, increasingly more cases concerning workplace monitoring and the surveillance of employees in the context of alleged violations of Article 8 of the ECHR have started to be

4 Rustad and Paulsson, "Monitoring Employee E-Mail and Internet Usage: Avoiding the Omniscient Electronic Sweatshop: Insights from Europe", 870-871.

5 Article 8 of the European Convention on Human Rights.

6 The Grand Chamber in the case *S. and Marper v. the United Kingdom* adjudicated that 'The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention.' See: *S. and Marper v. the United Kingdom*, nos. 30562/04 and 30566/04), judgment of 4 December 2008, para. 103.

7 In the case *Niemietz v. Germany*, the Court stated that '(...) it would be too restrictive to limit the notion (of 'private life') to an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of 'private life' should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world.' See: *Niemietz v. Germany*, no. 13710/88, judgment of 16 December 1992, para. 29.

brought before the ECtHR.[8] This, in turn, led the Strasbourg Court to develop appropriate criteria to assess the proportionality of the interference with the right to privacy caused by surveillance measures in the workplace and acknowledge whether the monitoring was legal.[9] It should be noted that, in accordance with the Court's judgement, these criteria are addressed to the domestic authorities in the first instance.[10]

Similarly to the ECHR, the CFREU does not explicitly address the right to privacy in the context of employment. However, Article 7 of the Charter sets out the right to privacy in general terms, closely mirroring Article 8 of the ECHR. Indeed, it can be stated that Article 7 of the Charter 'substantially reproduces' Article 8 of the ECHR.[11]

Article 7 of the Charter reads as follows: 'Everyone has the right to respect for his or her private and family life, home and communications.'[12] The only difference between this provision and Article 8 of the ECHR is the use of wording. The EU legislator, instead of 'correspondence' used the word 'communications.' This move reflects a desire to give the Charter a timeless character, which takes into account technological changes.[13] However, the difference tends to be rather illusory since, as the ECtHR has pointed out on several occasions in its judgments, the term 'correspondence' covers all forms of communications regardless of their content.[14] This includes all 'traditional' paper and 'modern' electronic communications. Furthermore, the catalogue of means of correspondence is also open to new communications, which will be developed in the future due to technological

8 See e.g. *Halford v. the United Kingdom*; *Copland v. the United Kingdom*; *Köpke v. Germany*; *Bărbulescu v. Romania*; *Antović and Mirković v. Montenegro*; *López Ribalda and Others v. Spain*; *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*.

9 Barański, "Ukryty monitoring w miejscu pracy", 31.

10 The criteria were mentioned by the Court in the judgment of Grand Chamber in the case *Bărbulescu v. Romania* See: *Bărbulescu v. Romania*, no. 61496/08, judgement of 21 September 2017, para. 121.

11 C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU*, ECLI:EU:C:2008:54, para. 64.

12 Article 7 of the Charter of Fundamental Rights of the European Union (200/C 364/01).

13 Explanations relating to the Charter of Fundamental Rights (2007/C 303/02), Explanation on Article 7 – Respect for private and family life.

14 *Michaud v. France*, no. 12323/11, judgment of 6 March 2013, para. 90.

changes.[15] Additionally, it should be indicated that the 'correspondence' is not limited only to private correspondence but also to professional one.[16]

The similarity between Article 7 of the Charter and Article 8 of the Convention and their frequent simultaneous reference in the literature is not coincidental. According to Article 52(3) of the CFREU, 'the meaning and scope' of the right to privacy stated in the Charter should coincide with that indicated in the ECHR.[17] Therefore, when examining what is the scope of the right to privacy guaranteed by the Charter, and in particular what is the exact meaning of 'private life,' it should be assumed that it is determined by the interpretation provided by the ECtHR. Thus, the concept of 'private life' under the Charter must be interpreted broadly, which means that it also applies to matters relating to the employment relationship, including the issue of employee privacy in the context of workplace monitoring.[18] Nevertheless, the requirement of a compatible interpretation of Article 7 of the Charter with Article 8 of the ECHR and jurisprudence of the ECtHR constitutes merely a 'minimum standard clause,'[19] which does not deter the EU from developing more complex protection of the rights guaranteed by the Charter.[20]

In addition, when analysing Article 7 of the Charter in the context of employee privacy, it is important to recall the interpretative concept outlined by Otto based on the so-called 'integrated approach' developed by the case law of the ECtHR. Otto points out that the CFREU, through its catalogue of social rights, offers a framework for strengthening the protection of employees' privacy. Using an integrated approach in order to link civil and social rights, the Charter allows for a broader interpretation of privacy at work. Rights such as the right to freely choose an occupation and to engage

15 Lafferty, "Article 8: The Right to Respect for Private and Family Life, home and Correspondence", 530.

16 *Niemietz v. Germany,* no. 13710/88, judgment of 16 December 1992, para. 32.

17 The first sentence of Article 52 (3) of the CFREU states that 'the Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention.'

18 As Kokott and Sobotta points out 'According to both Courts (*ECtHR and CJEU*), the term 'private life' must not be interpreted restrictively.' See Kokott and Sobotta, "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR", 223.

19 Otto, *The Right to Privacy in Employment – A Comparative Analysis*, 109.

20 The second sentence of Article 52(3) of the CFREU reads as follows: 'This provision shall not prevent Union law providing more extensive protection.'

in work,[21] protection against unjustified dismissal,[22] and the right to fair and just working conditions[23] may contribute to the clarification of the legal boundaries of permissible employer interference in employees' private lives, e.g. by means of workplace monitoring.[24]

Considering the privacy of employees, this concept should definitely be appreciated as it encourages a more comprehensive understanding of privacy in employment within EU law.

Under the CFREU, a distinctive element, especially with regard to the ECHR, is Article 8. It guarantees the protection of personal data. However, it should be noted that the above considerations regarding Article 7 of the Charter also apply to Article 8 of the Charter since, although the right to the protection of personal data is not explicitly mentioned in the ECHR, it is included within the scope of the right to respect for private life, as has already been pointed out above.

The provision states that:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.[25]

The main basis for the Article was Article 286 of the Treaty establishing the European Community and Directive 95/46/EC,[26] which was sort of a clarification of the principles and conditions of data processing in the context of Article 8.[27] Over time, Article 286 of the Treaty establishing the European Community was replaced by Article 16 of the Treaty on the Functioning of the EU and Article 39 of the Treaty on EU; in turn, Directive 95/46/EC was succeeded by Regulation 2016/679 (GDPR). The GDPR,

21 Article 15 of the CFREU.
22 Article 30 of the CFREU.
23 Article 31 of the CFREU.
24 Otto, *The Right to Privacy in Employment – A Comparative Analysis*, 109.
25 Article 8 of the CFREU.
26 Lock, "Commentary on Article 8 CFR", 2122.
27 Explanations relating to the Charter of Fundamental Rights (2007/C 303/02), Explanation on Article 8 – Protection of personal data.

as a regulation, is of general application, binding in its entirety and directly applicable in all EU Member States, although, due to Article 23 and, above all, Article 88, as will be elaborated later in the paper, it does not provide a uniform regulation of the protection of personal data in employment.[28]

The explicit inclusion of the right to the protection of personal data in the CFREU should be considered a breakthrough, as it has granted it the status of a fundamental right.[29]

In addition, it should be pointed out that the issue of protection of personal data in the context of employment has been addressed on several occasions by the Court of Justice of the EU (CJEU), which oversees the application of EU law and its compliance by Member States.[30] The Court ruled on this in: *Rechnungshof v. Österreichischer Rundfunk*, case[31] the *Bodil Lindqvist* case,[32] and the *V and European Data Protection Supervisor v. European Parliament* case.[33] These cases concerned actions that had the potential to violate an employee's private life and right to protection of personal data, but in none of them was this action employee monitoring.

2.2. Council of Europe's Regulatory Framework

Gradually moving away from the sphere of human rights, although not entirely, it is worth mentioning the CoE's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (so-called Convention 108),[34] which was the first legally binding document regulating the processing of personal data of an international nature.[35] The aim of the Convention 108 was to bring greater uniformity to the protection of personal data systems expressed in national laws and protect human

28 Barański, "Ochrona danych osobowych pracowników w orzecznictwie Trybunału Konstytucyjnego oraz Trybunału Sprawiedliwości", 56.

29 Hendrickx, "Privacy@work: A Systemic Introduction", 2.

30 Lukács, *Employees' Right to Privacy and Right to Data Protection on Social Network Sites with Special Regard to France and Hungary,* 99-100.

31 Joint Cases: C-465/00 *Österreichischer Rundfunk and Others*, C-138/01 *Christa Neukomm* and C-139/01 *Joseph Lauermann*, ECLI: ECLI:EU:C:2003:294.

32 Case C-101/01 *Lindqvist*, ECLI:EU:C:2003:596.

33 Judgement of the Civil Service Tribunal, Case F-46/09 *V v Parliament*, 2011/C 282/92.

34 The Convention was adopted on 28 January 1981.

35 Lukács, *Employees' Right to Privacy and Right to Data Protection on Social Network Sites with Special Regard to France and Hungary*, 61.

rights[36] owing to the risks imposed by the increasing cross-border flow of personal data and its automated processing.[37] Although this convention was adopted by the CoE, it was not limited solely to its Member States; rather, it might be said that it aspired to become the Convention of global reach.[38] [39]

The Convention advocated for a fair and lawful model of the collection and automated processing of data and established a number of principles and requirements that such a model should incorporate. According to the Convention, such data should be retained solely for clearly defined and legitimate purposes and not used in ways that are incompatible with those purposes. Data must be adequate, relevant, and not disproportionate to the objective for which it is retained, and it should be accurate and, where necessary, kept up to date. Furthermore, it must be stored in a form permitting the identification of data subjects only for as long as is necessary to achieve the purposes for which the data are held.[40]

In 2018, the CoE decided to modernise the Convention. This decision was justified by the Council's desire to better address emerging privacy challenges resulting from the increasing use of new information and communication technologies (IT), the globalisation of processing operations and the ever-greater flows of personal data, and, at the same time, to strengthen the Convention's evaluation and follow-up mechanism.[41]

The modernised Convention is currently referred to as 'Convention 108+' and its major difference from the previous version of the act is that it adds transparency as a core principle of data processing[42] and dispels

36 Preamble of Convention 108 from 28 January 1981. See also Hendrickx, "Privacy@work: A Systemic Introduction", 150.

37 Preamble of Convention 108 from 28 January 1981.

38 Convention 108 has been signed and ratified by some non-members of Council of Europe. See https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108. See also Hendrickx, "Privacy@work: A Systemic Introduction", 3-4.

39 However, the outcome of such efforts has been rather poor as by 1992 only ten countries had ratified the convention – Austria, Denmark, France, Germany, Ireland, Luxembourg, Norway, Spain, Sweden and the United Kingdom, while eight countries – Belgium, Cyprus, Greece, Iceland, Italy, Netherlands, Portugal and Turkey – had signed it without ratification. See Cate, *Privacy in the Information Age*, 35.

40 Article 5 of Convention 108 form 28 January 1981.

41 Council of Europe, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 10 October 2018, 1.

42 Article 5 (4) a of Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data from 18 May 2018 (Convention 108+).

doubts about the inclusion of manual data processing within the scope of the Convention by pointing out that,

> data processing' starts from the collection of personal data and covers all operations performed on personal data, whether partially or totally automated. Where automated processing is not used, data processing means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria, allowing the controller or any other person to search, combine or correlate the data related to a specific data subject.[43]

Additionally, it should be noted that after the adaptation of the original version of the Convention 108, many declarations, resolutions and recommendations were published by different bodies of the CoE, among which were documents of particular relevance to the employment field, including the question of workplace monitoring.

The first such document, which also illustrated the CoE's policy shift towards sectoral regulations, was the Recommendation of the Committee of Ministers to Member States on the Protection of Personal Data Used for Employment Purposes, adopted on 18 January 1989.[44] The important feature of the Recommendation No. (89) 2 is that its scope covers the collection and processing of personal data for employment purposes in the public and private sectors.[45] The framework of the Recommendation can be reduced to five core principles. Firstly, employers should, as a general rule, obtain personal data directly from the job applicant or the employee concerned. Secondly, such data should be collected and processed solely for employment-related purposes (i.e. recruitment of employees; fulfilment of the contract of employment; management, including discharge of obligations laid down by law or laid down in collective agreements; and planning and organisation of work)[46] corresponding to the specific type of employment in question. Thirdly, employees must be regularly informed about the nature of the data held, the purposes of its processing, the recipients to whom it is routinely

43 Council of Europe, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 10 October 2018, 21. See also Article 2 (a) and (c) of Convention 108+.

44 Hereinafter: Recommendation No. (89) 2.

45 Recommendation No. (89) 2, 1.1.

46 Recommendation No. (89) 2, 1.3.

disclosed, and the legal grounds for such disclosures. Fourthly, employees should have the right to access all personal data relating to them, as well as the right to request the rectification or deletion of any data processed in violation of the Recommendation's principles. Finally, personal data should be retained only for as long as is necessary to fulfil the purposes for which it was collected. In particular, this entails an obligation to erase applicants' data promptly once it becomes clear that they will not be offered the position for which they applied.[47] The recommendation also draws attention to particular categories of employee data,[48] the processing of which should be limited and in compliance with the appropriate safeguards indicated by national laws. In the absence of such safeguards, particular categories of employee data may be processed and stored with the express and informed consent of the employees.[49]

However, considering the changes taking place in employment, triggered by, among other things, the globalisation of work and services, the increasing use by employers of information and communication technologies that enable the collection of broader sets of employees' data, the need to review the Recommendation No. (89) 2 has arisen.[50] Following this demand, on 1 April 2015, the Committee of Ministers of Member States adopted the Recommendation CM/Rec(2015)5 on the processing of personal data in the context of employment.[51]

The Recommendation CM/Rec(2015)5 is significant in the context of workplace monitoring as it addresses the use of modern technologies in the workplace and contains explicit provisions on employee monitoring.

The document emphasises that employers should avoid unjustifiable or unreasonable interference with employees' private life when using the Internet and electronic communications at work. This principle extends to all ICT[52] devices used by employees. According to the Recommendation,

47 Simitis, "From the General Rules on Data Protection to a Specific Regulation of the Use of Employee Data: Policies and Constraints of the European Union", 362.

48 Such data are personal data relating to racial origin, political opinions, religious or other beliefs, sexual life or criminal convictions, referred to in Article 6 of the Convention 108. See Recommendation No. (89) 2, 10.1.

49 Recommendation No. (89) 2, 10.1.

50 See Explanatory Memorandum to Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment, 2; Preamble of the Recommendation CM/Rec(2015)5 of the Committee of Ministers to Member States on the processing of personal data in the context of employment, 1 April 2015.

51 Hereinafter: Recommendation CM/Rec(2015)5.

52 ICT states for 'Information and Communication Technology'.

employers should be obliged to implement and regularly update a privacy policy detailing the purpose of processing, retention periods, and the handling of professional communications. Preventive measures, such as filtering or anonymous random checks, are preferred over intrusive monitoring of employees' web activity. Moreover, access to professional communications is permissible only if it is necessary for legitimate purposes, it should be conducted in the least intrusive manner possible and only after informing the concerned employee.[53]

Touching upon the broader monitoring systems, including video surveillance, the Recommendation expresses the prohibition of the use of information systems and technologies for the sole purpose of directly tracking employees' activity and behaviour. When such monitoring occurs indirectly, for instance, owing to the systems aimed at protecting production, health and safety, or organisational efficiency, it should comply with strict safeguards such as informing employees before introducing monitoring means; taking proper internal measures connected to the processing of personal data and notification of employees about this in advance; consulting employees' representatives and national personal data supervisory authority.[54] Particularly sensitive areas of employees' personal life, such as, e.g. rest areas, toilets, showers, and cloakrooms, are strictly off-limits for video surveillance. Additionally, employees should be granted access to any recorded materials in the context of disputes or legal proceedings, and such recordings must be stored only for a limited period.[55]

The document also addresses location-tracking equipment, which may only be introduced when necessary for legitimate purposes, which do not include monitoring *per se*, and should never serve as a tool for continuous monitoring. Employers are required to uphold proportionality and data minimisation principles and to adopt additional safeguards[56] to protect employees' privacy and personal data protection. In addition, while introducing appropriate internal procedures regulating the processing of data on employees' location, employers should, in advance, notify the concerned persons about such procedures.[57]

53 Recommendation CM/Rec(2015)5, 14.
54 Recommendation CM/Rec(2015)5, 21.
55 Recommendation CM/Rec(2015)5, 15.
56 These safeguards are expressed in the principle 21 of the Recommendation CM/Rec(2015)5.
57 Recommendation CM/Rec(2015)5, 16.

What emerges from the indicated provisions is a model for regulating workplace monitoring that limits monitoring to specific purposes and only allows it when other, less intrusive measures would not achieve such aims. Furthermore, it stipulates that once monitoring measures are applied in the workplace, they must be proportionate, transparent and respectful towards the fundamental rights of employees.

Another outstanding feature of this document is that, as the first CoE document touching upon employee data protection, it addresses the issue of monitoring employees and job applicants via social media platforms.[58]

The Recommendation CM/Rec(2015)5 clearly indicates that employers should not request or require that employees or job applicants grant access to information they share with others online, particularly on social networking platforms.[59] Moreover, the explanatory memorandum provides us with more information on this subject, stating that employers should abstain from using intermediaries, alternative names or pseudonyms to get access to the personal data of an employee or a work candidate without their consent.[60] Employers are also prohibited from requesting the login details of employees and candidates to access their social media accounts.[61]

In view of the above, the interpretation that emerges on the ground of the principle expressed in paragraph 5.3 of the Recommendation CM/Rec(2015)5, is that an employer should refrain from any attempt to access information shared by an employee online, to which his or her access has been restricted due to the employee's privacy settings. On the other hand, if the data shared online is available to the public, there is no obstacle to it becoming the object of processing by an employer. Naturally, such processing must comply with the principles of lawful personal data processing.[62]

Despite being more than a decade old, the Recommendation, to a certain extent, demonstrated remarkable foresight. Most of its principles

58 Lukács, *Employees' Right to Privacy and Right to Data Protection on Social Network Sites with Special Regard to France and Hungary*, 97.

59 Recommendation CM/Rec(2015)5, 5.3.

60 Explanatory Memorandum to Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment, para. 45.

61 Explanatory Memorandum to Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment, para. 46.

62 Lukács, *Employees' Right to Privacy and Right to Data Protection on Social Network Sites with Special Regard to France and Hungary*, 97.

concerning the processing of employees' personal data, particularly those addressing workplace monitoring and the processing of employees' data shared online, e.g. via social media, are gaining increasing relevance in light of current developments. For example, in the labour market of Central European countries, it is increasingly becoming noticeable that employers are starting to use sophisticated techniques to monitor employees, including monitoring via social media.[63] Cases of employees being dismissed due to criticism of the employer or social media activity potentially undermining the employer's interest are gaining prominence. Štefko refers to such employees as 'Facebook fired.'[64] As an example of such cases, it is worth mentioning, for example, a case decided by the Hungarian Supreme Court, in which an employee was disciplinarily dismissed for posting insulting remarks and threats against his employer on Facebook and calling on employees to organise themselves. In that case, the Curia (Hungarian Supreme Court) ruled in favour of the employer, that the dismissal was lawful.[65] Another similar case also originates from Hungary and concerns a prosecutor who was disciplinarily dismissed because he published posts of a political nature on his Facebook profile. However, in this case, the courts of both instances ruled that the dismissal was excessive. Instead of dismissal, the prosecutor's salary was reduced.[66] There have also been similar cases in other Central European countries, like Poland and the Czech Republic. In Poland, strong emotions were aroused by the case of a post office employee dismissed for comments on social media supporting the actions of the Russian army in the war against Ukraine,[67] and by the case of an employee of the Ministry of Foreign Affairs who was dismissed for posting comments on his private social media profile that referred to political and social reality. In the present case, the Warsaw Regional Court found the termination of the employment contract without notice to be unjustified.[68] In turn, in the Czech Republic,

63 Štefko, "Social Media in the Workplace in the Czech Republic, Poland and Slovakia", 11-17.

64 Štefko, "Privacy at Work in the Czech Republic", 138; See also: Štefko, "Social Media in the Workplace (Bărbulescu v. Romania, ECHR, 61496/08)", 156.

65 Judgement of Kúria (Supreme Court of Hungary) Mfv. 10.469/2013/4.

66 https://index.hu/belfold/2019/05/10/facebook_per_ugyesz_ugyeszseg_kirugas_itelet/?token=ec537fc4771e0f1a5fac51a7cefc3b19 (Accessed 14 August 2025).

67 https://www.gazetaprawna.pl/praca/artykuly/8386055,poczta-polska-zwolnienie-dyscyplinarne-media-spolecznosciowe-wpis-wojna-w-ukrainie.html (Accessed 15 August 2025). See also the statement of the Polish Post regarding that case – https://media.poczta-polska.pl/releases/oswiadczenie-2022-03-17 (Accessed 14 August 2025).

68 https://www.prawo.pl/kadry/pracownik-zwolniony-za-wpisy-w-mediach-spolecznosciowych-jaki,508257.html (Accessed 15 August 2025).

a high-profile case involving the issue of 'Facebook fired' employees is that of an editor and reporter who, in an online article, criticised his employer – TV Barrandov – comparing relations within its structures to a totalitarian regime, claiming that the plans of reportages must be approved in advance by supervisors, which leads to top-down censorship. Nevertheless, the Czech Supreme Court, adjudicating on the case, found that the employee's criticism was subjective and unjustified, and objectively capable of endangering the employer's good reputation. Therefore, the disciplinary dismissal was justified.[69]

The momentous nature of these cases lies in the fact that the monitoring of employees via their social media does not only and exclusively affect employees' privacy, but also their freedom of expression, which can certainly be included in the sphere of privacy, but which also constitutes a separate fundamental right under the ECHR and the CFREU.[70]

When analysing Recommendations of the Committee of Ministers to Member States, it should be remembered that they are only soft law instruments; they have no legal force and rules stated in their provisions cannot be enforced in any way. Nevertheless, they are of great doctrinal importance, and often even the postulates included in them are reflected in binding legal acts.

The last piece of legislation that should be mentioned in the context of workplace monitoring and employee privacy in the realm of the CoE is the European Social Charter (ESC), which constitutes a pillar of social and economic rights in Europe.[71] The ESC, in its regulations, does not explicitly address either employees' right to privacy or the right to personal data protection.

Nevertheless, on the basis of Article 1(2), which states that '[w]ith a view to ensuring the effective exercise of the right to work, the Parties undertake: to protect effectively the right of the worker to earn his living in an occupation freely entered upon,' the European Committee of Social Right (ECSR) pointed out that the freedom to engage in work inherently encompasses protection against infringements of the right to privacy. Accordingly, it is

69 The Czech Republic Supreme Court judgement of 20 March 2017, 21 Cdo 1043/206.

70 This issue has been addressed in the ECtHR judgment in case *Herbai v. Hungary,* no. 11608/15, judgment of 5 February 2020. See also: Koltay, "Social Media and Freedom of Speech in Employment: Limitations on Employees' Right to Self Expression", 331-345.

71 Lukács, *Employees' Right to Privacy and Right to Data Protection on Social Network Sites with Special Regard to France and Hungary,* 98.

essential that workers' fundamental rights to privacy be recognised and safeguarded within the framework of the employment relationship, ensuring its effective protection.[72] In addition, an interesting and pertinent position was expressed by the committee, justifying the derivation of the right to privacy from the right to take up an occupation freely. Namely, the Committee notes that the advent of new communication technologies has enabled employers to maintain continuous supervision over employees, while also making it possible for employees to perform work for their employers at any time and in any location, including their homes. This development has blurred the boundaries between professional and private life, increasing the risk of work encroaching upon all spheres of private life, even beyond working hours and outside the workplace.[73]

Therefore, it can be concluded that the Committee's interpretation was directly influenced by the phenomenon of employee monitoring and especially its increasingly severe forms, which result in the fading of the boundary between work and private life. In 2016, the ECSR directly pointed out that Article 1(2) of the ESC also concerns the right to privacy at work.[74]

2.3. European Union Regulatory Framework

At the central point of the EU's framework of personal data protection lies the General Data Protection Regulation,[75] which, to a certain extent, originated from the previous Directive 95/46/EC of 24 October 1995.[76] The desire to change the previous model of personal data protection in the EU has been driven by the accelerating pace of technological development, coupled with the effects of globalisation, which fundamentally altered the ways in which vast quantities of personal data are collected, accessed, utilised, and transferred. Moreover, personal data has acquired significant economic value, with many businesses relying on its collection, aggregation,

72 European Committee of Social Rights, *Activity Report 2012*, Council of Europe, 2013, 26.
73 European Committee of Social Rights, *Activity Report 2012*, Council of Europe, 2013, 26.
74 European Committee of Social Rights, *Activity Report 2016*, Council of Europe, 2017, 32.
75 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
76 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281.

and analysis as a core element of their commercial activities. That is why it has become essential to ensure that individuals can exercise effective control over their personal information.[77] This pushed the EU to reform in order to build a modern, strong, consistent and comprehensive data protection framework.[78]

The GDPR regulation is based on a technology-neutral approach, originally expressed in Directive 95/46/EC.[79] Moreover, the Regulation establishes key principles according to which data are to be collected and processed. These principles are: 1. lawfulness, fairness and transparency; 2. purpose limitation; 3. data minimisation; 4. accuracy; 5. storage limitation; 6. integrity and confidentiality.[80] It also sets out specific categories of data, the processing of which should be, in principle, prohibited,[81] and introduces rules on accountability of organisations.[82]

The GDPR is of universal scope, binding in its entirety and directly applicable to all EU Member States.[83] Its general regime of data protection law also applies to the employment sphere. Nevertheless, as Hendrickx points out, this presents a significant challenge from a labour law perspective, as the GDPR's provisions are highly detailed and drafted in a technical manner, yet not specifically with labour law in mind. Labour law is a specific field of law with sets of its own rules, catalogues of notions and traditions; therefore, its intersection with privacy law creates a very complex relationship.[84]

However, in an attempt to allow the principles expressed in the GDPR to be adapted to the employment sphere, the EU legislator has included it

77 European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Safeguarding Privacy in a Connected World a European Data Protection Framework for the 21st Century*, COM(2012) 9 final, 2012, 2.

78 COM(2012) 9 final, 12.

79 European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A comprehensive approach on personal data protection in the European Union*, COM(2010) 609 final, 2010, 3.

80 Article 5 of the GDPR.

81 Article 9 of the GDPR.

82 Article 5(2) and Article 24 of the GDPR. See also: Hijmans, "Data Protection and Surveillance: The Perspective of EU Law", 244-246.

83 Barański, "Ochrona danych osobowych pracowników w orzecznictwie Trybunału Konstytucyjnego oraz Trybunału Sprawiedliwości", 56.

84 Hendrickx, "Privacy@work: A Systemic Introduction", 3.

in the Regulation Article 88, which gives Member States a certain degree of discretion in setting up personal data protection systems within the employment context. Article 88 of the GDPR states that:

1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.
2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the workplace.

The implementation of the aforementioned article resulted in the creation of specific national models for data processing in the sphere of employment, which in turn led to different regulations in the sphere of workplace monitoring.

Article 88 is also of great importance for European and national social partners, primarily because of its component of collective agreements. European social partners in the 2020 Autonomous Framework Agreement on Digitalisation, which is the soft law instrument, evoke Article 88 of the GDPR pointing out that it opens the way for the social partners to establish 'more specific rules to ensure the protection of the rights and freedom with regards to the processing of personal data of employees in the context of employment relationships,' through collective agreements.[85] Moreover, the Framework Agreement explicitly affirms that AI deployment at work must follow a 'human-in-control' principle and remain under human oversight. It also warns that pervasive digital surveillance risks 'compromising the dignity

85 European social partners framework agreement on digitalisation of 2020, 12.

of the human being, particularly in cases of personal monitoring.'[86] Thus, the document enshrines a rights-based framework for balancing technological innovation with fundamental labour rights and the preservation of human dignity in the digital transformation of work.[87]

When describing the EU data protection system, especially in relation to employment, it is important not to forget about the Article 29 Data Protection Working Party (WP), which was an independent European advisory body on data protection and privacy, established by Directive 95/46/EC and, after the entry into force of the GDPR, replaced by the European Data Protection Board.[88] The WP participated in the creation of the EU data protection system, playing a huge role in employees' data protection, and although the documents it issued were not legally binding, they are still relevant and of great importance for labour law doctrine. From the perspective of the issue of workplace monitoring, three of the most important documents issued by the WP are Opinion 8/2001 on the processing of personal data in the employment context,[89] Working document on the surveillance of electronic communications in the workplace[90] and Opinion 2/2017 on data processing at work.[91] Opinion 8/2011 addresses the processing of personal data in the employment context in broad terms, without specifying how the general principles should be applied to particular instances of employee monitoring. The accompanying Working Document narrows its focus to the monitoring of electronic communications, with particular emphasis on e-mail monitoring and Internet access. On the other hand, Opinion 2/2017 builds upon and complements both Opinion 8/2001 and the Working document, taking into account subsequent societal, technological and legal developments and offering guidance on various forms of data processing and monitoring, including screening of employees, monitoring of ICT usage at and outside the workplace; monitoring

86 European social partners framework agreement on digitalisation of 2020, 12.

87 European social partners framework agreement on digitalisation of 2020.

88 European Data Protection Board, Legacy: Art. 29 Working Party, https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_en (Accessed 15 August 2025).

89 Opinion 8/2001 on the processing of personal data in the employment context, 13 September 2001, 5062/01/EN/Final WP 48.

90 Working document on the surveillance of electronic communications in the workplace, 29 May 2002, 5401/01/EN/Final WP 55.

91 Opinion 2/2017 on data processing at work, 8 June 2017, 17/EN WP 249.

systems used to check the time and attendance; video monitoring; and geolocation monitoring.[92] [93]

3. Conclusion

The issue of workplace surveillance in Europe is regulated through a multilayered framework combining CoE standards, EU primary and secondary law, and soft law instruments. While both legal orders emphasise the protection of employees' privacy and personal data, they also provide a sort of flexibility for Member States to adapt rules to the specific character of national labour relations.

Recent developments, such as the modernisation of Convention 108 and the adoption of the General Data Protection Regulation alongside Article 88, reflect a growing recognition of the unique challenges posed by new technologies, AI, digitalisation of labour, and pervasive monitoring. These instruments, reinforced by recommendations and European social partners' agreements, aim to balance employers' interests with fundamental rights of employees, underlining transparency, proportionality and respect for human dignity as key guiding principles.

The framework is robust in principle; however, its effectiveness depends on coherent implementation at the national level, the adaptability of legal standards to emerging technologies, and the ability of social dialogue parties to address sector and workplace specific realities. As digitalisation continues to blur the boundaries between work and private life, the challenge for European legislators will be to ensure that technological progress enhances rather than undermines the rights of employees, and that employee monitoring, where it occurs, remains a proportionate and accountable tool rather than an instrument of severe control.

92 Opinion 2/2017 on data processing at work, 8 June 2017, 17/EN WP 249, 12-21.

93 Lukács, *Employees' Right to Privacy and Right to Data Protection on Social Network Sites with Special Regard to France and Hungary*, 101.

Bibliography

1. Barański, Michał. "Ochrona danych osobowych pracowników w orzecznictwie Trybunału Konstytucyjnego oraz Trybunału Sprawiedliwości." *Państwo i Prawo* 1/2022 (2022): 46-65.
2. Barański, Michał. "Ukryty monitoring w miejscu pracy." *Monitor Prawa Pracy,* no. 3 (2020): 26-32.
3. Cate, Fred H. *Privacy in the Information Age*. The Brookings Institution, 1997.
4. European Committee of Social Rights. *Activity Report 2012*. Council of Europe, 2013.
5. European Committee of Social Rights. *Activity Report 2016*. Council of Europe, 2017.
6. European Social Partners, *Framework Agreement on Digitalisation*, 2020.
7. Fabbrini, Federico. "The European Multilevel System for the Protection of Fundamental Rights: A 'Neo-Federalist' Perspective." *Jean Monnet Working Paper 15/10* (2010): 7-60.
8. Hendrickx, Frank. "Privacy 4.0 at Work: Regulating Employment, Technology and Automation." *Comparative Labor Law & Policy Journal* 41, iss. 1 (2019): 147-172.
9. Hendrickx, Frank. "Privacy@work: A Systemic Introduction." In *Privacy@work – A European and Comparative Perspective*, edited by Frank Hendrickx, David Mangan, Elena Gramano. Kluwer Law International, 2023.
10. Hijmans, Hielke. "Data Protection and Surveillance: The Perspective of EU Law." In *Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives*, edited by Valsamis Mitsilegas and Niovi Vavoula. Hart, 2021.
11. Kokott, Juliane and Sobotta, Christoph. "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR." *International Data Privacy Law* 3, no. 4 (2013): 222-228.
12. Koltay, András. "Social Media and Freedom of Speech in Employment: Limitations on Employees' Right to Self Expression." In *Decent Work in the Digital Age: European and Comparative Perspectives,* edited by Tamás Gyulavári and Emanuel Menegatti. Hart, 2022.
13. Lafferty, Michelle. "Article 8: The Right to Respect for Private and Family Life, Home and Correspondence." In *Harris, O'Boyle & Warbrick: Law of the European Convention on Human Rights*, edited by David Harris, Michael O'Boyle, Ed Bates, and Carla Buckley. Oxford University Press, 2014.
14. Lock, Tobias. "Commentary on Article 8 CFR." In *Commentary on the EU Treaties and the Charter of Fundamental Rights,* edited by Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin. Oxford: Oxford University Press, 2019.
15. Lukács, Adrienn. *Employees' Right to Privacy and Right to Data Protection on Social Network Sites with Special Regard to France and Hungary*. Iurisperitus Publishers, 2021.
16. Otto, Marta. *The Right to Privacy in Employment – A Comparative Analysis*. Hart Publishing, 2016.
17. Rustad, Michael. L., and Paulsson, Sandra. R., "Monitoring Employee E-Mail and Internet Usage: Avoiding the Omniscient Electronic Sweatshop: Insights

from Europe." *University of Pennsylvania Journal of Business Law* 7, iss. 4 (2005): 829–904

18. Simitis, Spiros. "From the General Rules on Data Protection to a Specific Regulation of the Use of Employee Data: Policies and Constraints of the European Union." *Comparative Labor Law and Policy Journal*, vol. 19, no. 3 (1998): 351-371.
19. Štefko, Martin. "Privacy at Work in the Czech Republic." In *Privacy@work – A European and Comparative Perspective*, edited by Frank Hendrickx, David Mangan, Elena Gramano. Kluwer Law International, 2023.
20. Štefko, Martin. "Social Media in the Workplace (Bărbulescu v. Romania, ECHR, 61496/08)." In *Labour Law and Social Rights in Europe: The Jurisprudence of International Courts – Selected Judgements*, edited by Stefano Bellomo, Nicola Gundt, Maciej Łaga, and José M.M. Boto. Gdańsk University Press, 2018.
21. Štefko, Martin. "Social Media in the Workplace in the Czech Republic, Poland and Slovakia." *The Lawyer Quarterly*, vol. 6, no. 1 (2016): 11-17.