The Internet of Things and Artificial Intelligence as Workplace Supervisors

Molè, Michele

Published in:
Italian Labour Law e-Journal

DOI:
10.6092/issn.1561-8048/15598

Publication date:
2022

Italian Labour Law e-Journal
Issue 2, Vol. 15 (2022)
ISSN 1561-8048
https://doi.org/10.6092/issn.1561-8048/15598

The Internet of Things and Artificial Intelligence as Workplace Supervisors: Explaining and Understanding the New Surveillance to Employees Beyond Art. 8 ECHR

Michele Molè*

Abstract

The Internet of Things (IoT) and Artificial Intelligence (AI) are overexposing the employee under the employer scrutiny. Through a labour oriented approach to privacy and data protection, this contribution aims to detect principles of explainability and understanding of the new workplace surveillance under the ECHR. In fact, looking at the ECtHR's jurisprudence it is possible to theorise that the Court's margin of appreciation may be stricter in safeguarding employees' privacy and essential labour rights when the surveillance measure interferes with individual and collective autonomy of the workforce.

Keywords: Workplace Surveillance; Artificial Intelligence; Internet of Things; Privacy and Data Protection; Labour Rights.

* PhD researcher in Labour Law and Member of the Security Technology and ePrivacy Research Group (STeP) at the University of Groningen (The Netherlands). The PhD project is funded by the Cybersecurity Noord Nederland Project (CSNN). This essay has been submitted to a double-blind peer review.

1. The new workplace surveillance and the quest for a new symmetry of information and powers.

Workplace surveillance is undergoing a major paradigm shift in the times of Artificial Intelligence (AI) and the Internet of Things (IoT). Monitoring through software and extensive networks of devices and sensors opens up new opportunities for employers to control employees and working environments. Working tasks, in many sectors, can be performed remotely or in constant interaction with AI and IoT systems (such as laptops, smartphones and smart objects). Such systematic tracking of employees' activities provides for the increasingly common use of 'workforce analytics' as a means of organising and evaluating the workforce.[1] Employees surveillance is thus normalised in order to draw inferences or detect behavioural patterns useful for workforce management and business operations. (See Section 2).

Organising work activities efficiently and protecting the corporate assets against risks (accidents, damage, theft) are legal and legitimate interests of the employer pertaining to the employment contract.[2] However, the proportionality of the new paradigm of surveillance introduced by AI and the IoT is often questioned by scholars and Courts.[3] The systematic risk so far addressed is a more vigorous introduction of the 'function creep' of surveillance, i.e. a supervision able to reveal more information than expected or necessary to meet the employer's needs.[4] From these new technological premises, a 'genetic variation' in the distribution of power and information in employment is discussed in the labour law literature.[5] A structural overexposure of the workforce under employer scrutiny is thus interfering with individual and collective rights of employees and trade unions under a non-transparent and unaccountable supervision, as a result of AI and IoT's complex technicalities.[6]

Striking a new balance of power and information between the involved stakeholders is thus a priority. To reach a new symmetry, this article proposes an analysis of the Strasbourg Court's judgments (ECtHR) on privacy at work (art. 8 ECHR) and those that the ECtHR has developed on the effectiveness of fundamental rights at work. These two threads of jurisprudence will let me reason on the explainability and understanding of AI and IoT as

[1] Otto defines workforce analytics as the use of predictive data mining to establish recurrent patterns or 'profiles', aiming to the recruitment, organisation and management of the workforce. Otto M., '*Workforce Analytics' v Fundamental Rights Protection in the EU in the Age of Big Data,* in *Comparative Labor Law and Policy Journal*, 40, 3, 2019, 389.

[2] Ball K., *Workplace Surveillance: An Overview*, in *Labor History*, 51, 1, 2010, 87.

[3] Eurofound, *Employee Monitoring and Surveillance the Challenges of Digitalisation*, 2020; Levy K., Barocas S., *Privacy at the Margins | Refractive Surveillance: Monitoring Customers to Manage Workers*, in *International Journal of Communication*, 12, 2018, 23.

[4] Koops B. J., *The Concept of Function Creep*, in *Law, Innovation and Technology*, 13, 1, 2021, 29-56 https://www.tandfonline.com/doi/full/10.1080/17579961.2021.1898299.

[5] Aloisi A., De Stefano V., *Essential Jobs, Remote Work and Digital Surveillance: Addressing the COVID-19 Pandemic Panopticon*, in *International Labour Review*, 161, 2, 2022, 289-314, available at https://onlinelibrary.wiley.com/doi/10.1111/ilr.12219.

[6] Kim P. T., Bodie M. T., *Artificial Intelligence and the Challenges of Workplace Discrimination and Privacy,* in *Journal of Labor and Employment Law*, 35, 2, 2021, 289; Nguyen A., *The Constant Boss - Labor Under Digital Surveillance,* in *Data & Society Research Institute*, 2021, https://datasociety.net/library/the-constant-boss/.

workplace supervisors (Section 4). A comprehensive overview of privacy and labour rights might indeed foster a new margin of appreciation from the ECtHR in assessing the necessity and proportionality of a structurally invasive surveillance. The aim is to detect a 'minimum threshold of transparency and accountability' in the implementation of AI and IoT as workplace supervisors.[7] Therefore, supporting a labour-oriented reading of Article 8 ECHR[8]. Section 5, finally, addresses some concluding remarks on the intersection between the effectiveness of fundamental labour rights and Article 8 ECHR.

2. Surveilling through IoT and AI: an unprecedented technological scenario.

According to Article 3 § 1 of the European Commission proposal for an Artificial Intelligence Regulation, AI is:

"Software that is developed with [specific] techniques and approaches [listed in Annex 1] and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with."[9]

The notion offered by the proposal for a European regulation on AI, being free of technicalities, makes it possible to highlight the current stage of its evolution. The so-called Strong AIs are not available today; in other words, we are not able to fully replicate human intelligence. When we talk about AI, then, we are referring to Narrow AI, which, from a narrow range of parameters and contexts, achieves specific goals (e.g. measuring an employee's present and future productivity from various indexes and data). Artificial Intelligence today is not software endowed with free will, but software capable of achieving, improving over time, goals in specific contexts.[10]

The operation of AI requires a considerable volume of data, which are collected from the workforce and matched with indices and parameters to infer further information or identify discernible patterns.[11] AI's demand for employees' data, then, necessitates a complementation with a further technology, the Internet of Things (IoT). The IoT can be described as a network of objects and environments, each with its own processor and wireless connection, which can be recognised, located and controlled via the Internet. Hence, objects or spaces can communicate with each other independently of human intervention;

[7] The minimum threshold of transparency is a concept elaborated by Collins P., *The Right to Privacy, Surveillance-by-Software and the "Home-Workplace"*, in *UK Labour Law Blog*, 3 September 2020, https://uklabourlawblog.com/2020/09/03/the-right-to-privacy-surveillance-by-software-and-the-home-workplace-by-dr-philippa-collins/.

[8] Otto M., *The Right to Privacy in Employment: A Comparative Analysis,* Hart Publishing, Oxford, 2016, 195.

[9] Proposal For a Regulation of The European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) COM/2021/206 Final.

[10] OECD, *Algorithms and Collusion: Competition Policy in the Digital Age*, 2017: www.oecd.org/competition/algorithms-collusion-competition-policy-in-the-digital-age.htm.

[11] The programming phase of AI requires so-called training data; that is, an initial data set used to train machine learning algorithms. AI models learn to act to achieve the given goal from this training, i.e. data samples used to provide many examples so as to calibrate the parameters of a machine learning model. Janiesch, C., Zschech, P., Heinrich, K., *Machine learning and deep learning*, in *Electronic Markets* 31, 2021, 685–695.

each device connected to the network constantly collects data on a wide variety of elements.[12] IoT, thus, introduces for the first time both qualitative and quantitative tracking through non-human surveillance: objects and spaces can be used to monitor changes in the human body, physical states or inter-personal relationships, beyond a simple GPS geolocation technology.[13]

AI and IoT are thus jointly ushering unprecedented surveillance capabilities in favour of employers.[14] Networks of smart objects such laptops, smartphones, wearables (bracelets, suits), smart cameras and sensors are accelerating the volume, variety and velocity of data collection, beyond the understanding of human upstream programming;[15] whereas AI provides meaningfulness to this wide gathering of granular, specific and individually meaningless data.[16]

3. The employee overexposure and the new employer monitoring power.

The paradigm of surveillance at work by means of AI and IoT results in a constant observation by managers, establishing what I mentioned earlier as a structural overexposure of the employee under the managerial gaze.[17] The first aspect of structural overexposure relates to technology: AI and IoT can monitor with increasing precision, the exposure of the workforce in the eyes of companies is enhanced. Therefore, the diligent behaviour of the employee, who must perform the service agreed upon in the contract, increases in strictness proportionally to the strictness of the surveillance. A call centre employee will be obliged to keep a kinder voice on a steady basis, since the employer will not check occasionally but constantly through a sensor directed at the employee's tone of voice. If the electronic bracelet indicates a particular route in the meanders of the warehouse, the storekeeper will have to blindly follow that indication in the allotted time, otherwise might be considered as non-fulfilment of working tasks. And so on. Thus, increased surveillance inherently brings a decrease in intimacy, free will and employee autonomy.[18] The other fundamental aspect of

[12] Lupton D., *The Quantified Self: A Sociology of Self-Tracking,* Polity, Cambridge, 2016, 28–29.
[13] Wachter S., *The GDPR and the Internet of Things: A Three-Step Transparency Model*, in *Law, Innovation and Technology*, 10, 2, 2018, 266–267, https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1527479.
[14] Dick R. P., Shang L.; Wolf M., Yang S.., *Embedded Intelligence in the Internet-of-Things*', in *IEEE Design & Test*, 37, 1, 2020, 7.
[15] Upstream programming refers to source code that has been posted/hosted on/in the code repository by the programmer.
[16] Broeders D., Schrijvers E., van der Sloot B., van Brakel R., de Hoog J, Hirsch Ballin E., *Big Data and Security Policies: Towards a Framework for Regulating the Phases of Analytics and Use of Big Data*, in *Computer Law & Security Review*, 33, 3, 2017, 309, https://linkinghub.elsevier.com/retrieve/pii/S0267364917300675; Ghosh A., Chakraborty D., Law A., *Artificial Intelligence in Internet of Things*, in *CAAI Transactions on Intelligence Technology*, 3, 4, 2018, 208.
[17] On the design and diffusion of such organisational settings: Hansen E.B., Bøgh S., *Artificial Intelligence and Internet of Things in Small and Medium-Sized Enterprises: A Survey*, in *Journal of Manufacturing Systems*, 58, Part B, 2021, 362-372, https://linkinghub.elsevier.com/retrieve/pii/S0278612520301424.
[18] Delfanti A., *Machinic Dispossession and Augmented Despotism: Digital Work in an Amazon Warehouse*, in *New Media & Society*, 23, 1, 2021, 39, http://journals.sagepub.com/doi/10.1177/1461444819891613; De Stefano V., *"Masters and Servers": Collective Labour Rights and Private Government in the Contemporary World of Work,* in *International*

overexposure is its structural nature, i.e. its ability to reform organisational models. The permanent analysis of the workforce by means of data makes it possible to operate totally new corporate structures: an example is Amazon's warehouses where employees are completely dependent on wristbands tracking their movements and giving directions accordingly.[19] However, where the employer gets meaningful outputs from the surveillance systems, the employee results as an observed agent within a working environment.[20]

Increasing asymmetries of information and power are thus being channelled through organisational and efficiency needs; stemming from the employer's right to conduct and organise an economic activity and to protect private property.[21] The structural overexposure of employees is indeed substantially varying the employer control power, exceeding human capabilities in the amount of data collected and processed. The traditional management structures around which doctrine and jurisprudence have always analysed the employer's right to monitor the workforce are now reshaped by the current technological scenario. The new surveillance thus calls into question the traditional limits to the prerogatives of control normally accepted in subordinate employment: the proportionality and necessity of surveillance measures at work require a more careful assessment when it comes to intrusiveness in employees' lives and limits to their autonomy.[22] A fundamental rights approach to the employer monitoring prerogative must then consider a new context made of unprecedented technologies and a highly innovative market influencing the employer authority.

3.1. Diverse layers of asymmetry: introducing the surveillance provider.

A further element of the new technological scenario is the involvement of third parties within the employer's supervisory powers. Workforce surveillance systems, indeed, represent a large-scale market of private companies, start-ups, data brokers, and app developers.[23] An employer implementing such systems is often their customer. The employer acts thus as a user of an infrastructure developed and managed by an external provider.[24] AI and IoT as

Journal of Comparative Labour Law and Industrial Relations, 36, 4, 2020, 425, http://www.kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\IJCL\IJCL2020022.pdf.

[19] Delfanti A., *ibid*; Jarrahi M. H., Newlands G., Sutherland W., *Algorithmic Management in a Work Context*, in *Big Data & Society*, 8, 2, 2021, http://journals.sagepub.com/doi/10.1177/20539517211020332.

[20] Delfino G. F., Van Der Kolk B., *Remote Working, Management Control Changes and Employee Responses during the COVID-19 Crisis*, in *Accounting, Auditing & Accountability Journal*, 35, 6, 2021, https://www.emerald.com/insight/content/doi/10.1108/AAAJ-06-2020-4657/full/html.

[21] The Court of Strasbourg, in one of its most recent pronouncements on workplace surveillance, has elaborated on the essentiality of surveillance in ensuring safety and the protection of company assets. López Ribalda and Others v. Spain, App no 1874/13 and 8567/13 (ECtHR, 17 October 2019).

[22] Aloisi A., De Stefano V., nt. (5); Adams-Prassl J., *What If Your Boss Was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at* Work, in *Comparative Labor Law & Policy Journal,* 41, 1, 2019, 123 ff. https://ssrn.com/abstract=3661151.

[23] Negrón W., *Little Tech Is Coming for Workers. A Framework for Reclaiming and Building Worker Power*, CoWorker.org 2021, https://home.coworker.org/wp-content/uploads/2021/11/Little-Tech-Is-Coming-for-Workers.pdf.

[24] Negrón W., *Ibid. See* also: Köchling A., Wehner M. C., *Discriminated by an Algorithm: A Systematic Review of Discrimination and Fairness by Algorithmic Decision-Making in the Context of HR Recruitment and HR Development*, in

workplace supervisor then are embedding a third party in the corporate structure, often retaining knowledge of their operation. Due to excessive costs, it is less common for companies to develop in-house their original workplace surveillance systems, as in the case of Amazon.[25]

The inclusion of third parties in the employer's supervisory prerogatives has an effect that should be considered: they interfere with the *intuitu personae* nature of the contract.[26] In fact, the software might not entirely reflect the choice the employer would make. Or, the employer may be not able to explain why certain decisions have been taken by the AI. Taking the example of workforce forecasting software, the user-employer may not be aware of their discriminatory bias against people with health problems or disabilities; some software has been shown to favour healthy individuals over the "less optimal" ones.[27] Addressing the new surveillance requires taking into account these diverse layers of information and power asymmetry involving employees, unions, employers and providers with significant impacts on working conditions.[28]

4. Explaining and understanding the new surveillance under the ECHR.

This section investigates whether in the ECtHR's case law (and literature) a minimum threshold of transparency and accountability imposed on employers and providers is detectable for AI and IoT workplace surveillance. Such minimum threshold is addressed hereafter with the principles of explainability and understanding of workplace surveillance.

After providing definitions of explainability and understanding of workplace surveillance, the quest for these two principles will be unfolded between the ECtHR jurisprudence on Art. 8 ECHR on the right to private and family life, home and correspondence and the Court's rulings on the role of fundamental labour rights in curbing the employer authority.

4.1 Explaining and understanding: addressing contextual and universal approaches of transparency.

The strong intrusiveness in the workforce daily routine is calling for a stronger transparency in the designing and implementation of such surveillance systems, to safeguard individual and collective fundamental rights at work. Explaining and understanding the new

Business Research, 13, 2020, 795-848, http://link.springer.com/10.1007/s40685-020-00134-w; Kim M. T., Bodie M. T., nt. (6).

[25] Delfanti A., nt. (18).

[26] *Intuitu personae* is a legal term designating those transactions where the personal qualities of the contracting parties are considered to be of particular importance. Such contracts, being based on personal trust, are not transmissible. It refers to a bilateral relationship (there are rights and obligations on both sides).

[27] Kim M. T., Bodie M. T., nt. (6); Wachter S., Mittelstadt B., *A Right to Reasonable Inferences*, in *Columbia Business Law Review,* 2, 2019, 494, https://journals.library.columbia.edu/index.php/CBLR/article/view/3424.

[28] Jarrahi M. H., nt. (19).

surveillance, therefore, shall address the two main aspects: contextual and universal transparency of workplace surveillance.[29]

According to the mainstream debate on the explainability of the processing of personal data, explaining a surveillance measure is mainly described as providing specific and relevant information on the measure in relation to the context and the recipient. Thus, a principle of explainability does not address transferring information to the public, but rather, as Kaminski explains, establishing a system of targeted disclosure. Such purposefulness then leads to different depths and scope of explainability depending on the recipient. Hence, an employer or provider ought to explain to employees whether such a measure affects work settings, what business needs it is fulfilling, and whether it interferes with the confidentiality of communications and other essential freedoms; a conceptualisation that echoes many of the GDPR's provisions as far as the European context is concerned (EU Reg. 2016/679).[30]

Contrary to the conceptualisation of explainability as a context – and recipient – related principle, however, it is possible to map out in doctrine more universalistic approaches to the understanding of AI and IoT surveillance measures. The latter approach considers rebalancing the current asymmetries of power and information only possible with a comprehensive disclosure of the architecture of AI and IoT. In this way, the technicalities of AI and IoT are prevented from making their operation not clear and not comprehensible for non-experts; achieving a transparency that, in the case of workplaces, is not intermediated by the employer/provider of surveillance but codetermined.[31] Understanding of surveillance therefore addresses a universal perspective over transparency; including disclosures as regards the 'system functionality' of the AI and IoT implemented, such the decision trees, algorithm classification structures, the weighing of specific features and how these impacted the employee(s).[32] Such universal approach to transparency would fill the current gap of trade unions in exercising their collective rights, which have been proved to be crucial in curbing abuse of managerial prerogatives.[33] Unions are indeed increasingly updating their digital skills to gain involvement in codetermining the digital development of the contemporary workplace.[34] The European framework is clear in this regard: the General Data Protection

[29] Varošanec I., *On the Path to the Future: Mapping the Notion of Transparency in the EU Regulatory Framework for AI*, in *International Review of Law, Computers & Technology,* 36, 2, 2022, https://www.ssrn.com/abstract=4066020.

[30] Kaminski M. E., *The Right to Explanation, Explained,* in *Berkeley Technology Law Journal*, 34, 1, 2019, https://www.ssrn.com/abstract=3196985; Kaminski M. E., Malgieri G., *Algorithmic Impact Assessments under the GDPR: Producing Multi-Layered Explanations'*, in *International Data Privacy Law*, 11, 2, 2021, 125, https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipaa020/6024963; Hamon R., Junklewitz H., Sanchez I., Malgieri G., De Hert P., *Bridging the Gap Between AI and Explainability in the GDPR: Towards Trustworthiness-by-Design in Automated Decision-Making*, in *IEEE Computational Intelligence Magazine*, 17, 1, 2022, 72-85, https://ieeexplore.ieee.org/document/9679770/.

[31] Wachter S., Mittelstadt B., nt. (27).

[32] Wachter S., Mittelstadt B., Floridi L., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 7, 2, 2017, 76 https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipx005.

[33] Aloisi A., Gramano E., *Artificial Intelligence Is Watching You at Work. Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context,* in *Comparative Labor Law & Policy Journal,* 41, 1, 2019, 95-114 https://ssrn.com/abstract=3399548.

[34] Trade Union Congress, *Technology Managing People: The Worker Experience*, 2020, https://www.tuc.org.uk/research-analysis/reports/technology-managing-people-worker-experience; European Trade Union Confederation, *Commission's Proposal for a Regulation on Artificial Intelligence Fails to Address*

Regulation (GDPR, EU Reg. 2016/679), under art. 88, already provides that collective bargaining may introduce additional requirements concerning individual and collective rights when processing personal data, paving the way for the long-awaited negotiation of the algorithm.[35]

4.2. Ensuring the explainability and understanding of surveillance under art. 8 ECHR.

The literature on fundamental rights and the digitalisation of work often refers to privacy and data protection as 'the foundation from which all other human rights and freedoms flow'.[36] Hence, the role for privacy and data protection (Art. 7 and 8 CFREU, Art. 8 ECHR) takes on the proper function of explaining and understanding surveillance, as these fundamental rights guarantee the development of personal space and identity. In this perspective, providing relevant and adequate information and sharing the architecture of surveillance systems is a pertinent demand to protect the personal sphere of a working individual and his or her essential freedoms at work, such as trade union rights or freedom of expression.[37]

Providing explanation and understanding of surveillance on the basis of Article 8 ECHR has several jurisprudential references; among them, the case of Bărbulescu v Romania, submitted to the Strasbourg Court (ECtHR), is of particular interest. The Court in 2017 states that, without prejudice to an entrepreneur's right to freely organise his economic activity: "an employer's instructions may not reduce private social life in the workplace to zero. Respect for private life and the confidentiality of correspondence continues to exist, even if it can be limited to the necessary extent"[38].

Part of the literature read into these paragraphs the introduction of a right to a reasonable expectation of privacy for the employee. In essence, what the Court described was a duty on the part of the employer to inform the supervised employee regardless of the requirements of legality, lawfulness, necessity and proportionality.[39] The violation of Article 8 ECHR in this case is based on the failure to provide meaningful information to the employee about his or her e-mails being subject to surveillance by the employer.[40] According to the Court, regardless of compliance with the requirements of Article 8 ECHR, the employee must be put in a position to know about the existence of surveillance measures. Such an employer's

the Workplace Dimension, 28 May 2021, https://www.etuc.org/en/document/commissions-proposal-regulation-artificial-intelligence-fails-address-workplace-dimension.

35 De Stefano V., Taes S., *Algorithmic Management and Collective Bargaining*, in *European Trade Union Institute Policy Brief Series*, 10 May, 2021, https://www.etui.org/publications/algorithmic-management-and-collective-bargaining.

36 Hiranandani V., *Privacy and Security in the Digital Age: Contemporary Challenges and Future Directions, in The International Journal of Human Rights*, 15, 7, 2011, 1091-1092, http://www.tandfonline.com/doi/abs/10.1080/13642987.2010.493360.

37 Adams-Prassl J., nt. (22); Aloisi A., Gramano E., nt. (33); Otto M., nt. (1).

38 Bărbulescu v. Romania (2017) App no 61496/08 (ECtHR, 5 September 2017), para 80.

39 Collins P., nt. (7).

40 Bărbulescu v. Romania (2017) App no 61496/08 (ECtHR, 5 September 2017), paras 78, 80, 133, 140, 141.

duty (and the employee's right) was justified by the need to empower the employee (and unions) to comprehend the possible consequences of the new organisational and supervisory measures and thus, if necessary, change his or her behaviour, obtain explanations or even seek a new job. Under the lens of labour law, this stance is particularly valuable: such equality of information serves to correct the bargaining asymmetry typical of subordinate employment. An absolute minimum threshold of transparency would therefore protect not only the privacy of employees but also fundamental freedoms of the employee from opaque data processing.

However, taking a broader picture beyond the Bărbulescu case, the jurisprudence on surveillance and the protection of privacy returns conflicting pronouncements. The ECtHR spans from identifying a duty to adequately inform the employee under Art. 8 ECHR (Bărbulescu v. Romania) to challenging the existence of the same employer's duty as a necessary precondition for workplace surveillance (Lòpez Ribalda v. Spain). By looking in particular at the Lòpez Ribalda case, the Court could not supplant the manifest reasons of protection of company assets: the right to receive meaningful information was outweighed by security requirements (Art. 1 ECHR Protocol, right to property). The circumstances examined by the Court concerned a Spanish supermarket that had installed hidden cameras (some had been notified, some had not) to clarify who were the employees involved in thefts of goods from the store where they worked. The Court therefore concluded that a duty of explanation (Art. 8 ECHR) against the integrity of the company's assets shall not be placed outside the assessment of proportionality and necessity of the surveillance measure, in opposition to what was established in the Bărbulescu case.[41] The employer's interest in protecting the company's assets led the Court to conclude that the Spanish national authorities had not exceeded their margin of appreciation and thus had not failed in their positive obligation to protect the rights provided under Article 8 ECHR.

The significant discrepancy between the Bărbulescu and Lòpez Ribalda decisions makes it necessary, I argue, to carefully ponder the protection of labour rights only through Article 8 ECHR under the new surveillance. As a matter of fact, conceiving privacy and data protection as the 'foundation' of all other fundamental freedoms – operating information balances and power symmetries – encounters an increasingly impervious constraint: the complex technicalities of AI and IoT. The growing availability of precise surveillance tools transposes the balance between legitimate interest, necessity and proportionality to a new context, where greater surveillance capabilities require greater transparency and accountability. Article 8 ECHR, indeed, is consistently confronted with the limitations imposed by law, legitimate interest, necessity and proportionality principles.[42] The Court, therefore, applying Article 8 ECHR, may find itself denying the right to a meaningful explanation if a surveillance measure meets a 'pressing social need' or is proportionate to the

[41] Turanjanin V., *Video Surveillance of the Employees between the Right to Privacy and Right to Property after Lopez Ribalda and Others v. Spain Articles & Essays*, in *University of Bologna Law Review*, 5, 2, 2020, 268, https://heinonline.org/HOL/P?h=hein.journals/bologna5&i=288.

[42] Mifsud Bonnici J. P., *Exploring the Non-Absolute Nature of the Right to Data Protection*, in *International Review of Law, Computers & Technology,* 28, 2, 2014, 131, available at: http://www.tandfonline.com/doi/abs/10.1080/13600869.2013.801590.

legitimate aim pursued.[43] As, precisely, the case of Lòpez Ribalda demonstrates: faced with serious damage to property and compelling reasons to protect the employer's assets, the Court valued the right to protect the company's assets over the employee's essential right to be informed. The balance between the economic sphere and the protection of labour is correct according to the literature, which also underlines that this ruling will not necessarily pave the way to limitless workplace surveillance in the European Court of Human Rights' forthcoming jurisprudence.[44] In any case, the issue at stake remains; how to establish an absolute minimum threshold of explainability and understanding of workplace surveillance? Scrutinising the necessity and proportionality of surveillance measures in the times of AI and IoT must acknowledge that both individual and collective labour rights are being steadily curtailed: as often emphasised in the literature, the ECtHR itself and the European Data Protection Board.[45] The Court's scrutiny, then, cannot avoid a new technological contextualisation, given the structural shortcomings in the enjoyment of fundamental freedoms in the context of AI and IoT surveillance, as seen so far. An initial answer to the question posed here, however, can be found in the other branch of fundamental rights considered here: those of labour.

4.3. Explainability and understanding through the ECtHR's case law on fundamental labour rights.

The traditional function of labour regulation provides interesting elements in outlining principles of explainability and understanding of workplace surveillance. As a response to largely non-regulated labour markets in the 19th century, the regulation of labour sought to act on the laws of supply and demand to safeguard decent working conditions. Even today, according to part of the literature, labour regulation operates as a countervailing power to redress the inherent inequality in employment. Thus, fundamental labour rights in their various guises (equal treatment, trade union rights, prohibition of forced labour) have as their ultimate aim ensuring that subordination in employment expresses organisational settings and not personal subjugation.[46] To be a countervailing power is more than the most significant feature of fundamental rights at work, it also represents the most relevant application of those rights by the European Court of Human Rights (Art. 4, 9-11, 14 ECHR).

[43] *Gillow v. UK* (1986) App no 9063/80 (ECtHR 24 November 1986) para 55.
[44] Turanjanin V., nt. (41), 293.
[45] Article 29 Data Protection Working Party, *Opinion 02/2017 on Data Processing at Wor*k, 9, https://ec.europa.eu/newsroom/article29/items/610169/en.
[46] Bogg A., *Republican Non-Domination and Labour Law: New Normativity or Trojan Horse?*, in *International Journal of Comparative Labour Law and Industrial Relations*, 33, 3, 2017, 391; Collins H., *Is the Contract of Employment Illiberal?* in Collins H. (ed.), *Philosophical Foundations of Labour Law*, Oxford, Oxford University Press, 2018; Bueno N., *Freedom at, through and from Work: Rethinking Labour Rights*, in *International Labour Review*, 160, 2, 2021, 311, https://onlinelibrary.wiley.com/doi/10.1111/ilr.12192; Tapiola K., *What Happened to International Labour Standards and Human Rights at Work?* in Halonen T., Liukkunen U. (eds.), *International Labour Organization and Global Social Governance*, Springer International Publishing, Helsinki, 2021, https://doi.org/10.1007/978-3-030-55400-2_3.

Looking at a some of the landmark cases,[47] such as Demir and Baykara v. Turkey and Enervi Yapi-Yol Sen v. Turkey, the Strasbourg Court had precisely described fundamental labour rights as the channel to remedy the inherent inequalities of power in subordinate employment: the Court "does not accept restrictions that affect the essential elements of trade union freedom, without which that freedom would be devoid of substance"[48].

The European Court of Human Rights in this pronouncement (and others) has already expressly declared itself on the function of fundamental rights and their integration with further international sources to interpret the ECHR. Thus, the provisions of the ILO Conventions, the ESC (European Social Charter) and Article 28 of the CFREU[49] compose the overall function of labour rights under the ECHR.[50] From this composite framework, the Court extrapolated an underlying principle: the personal and collective autonomy of employees as the foundation of every fundamental right at work.[51] Equal treatment, freedom of expression, association, assembly, and the prohibition of forced labour thus channel a symmetry of information and power into industrial relations: by guaranteeing such symmetries, fundamental rights open the way to improved working, social and economic conditions.[52] The most inherent function of fundamental labour rights is thus to protect employees from non-decent working conditions and guarantee them sufficient independence to determine their interests and pursue them (individually or collectively) in a meaningful way.[53] Moreover, it is worth mentioning that the Strasbourg Court already recognises a negative and positive duty imposed on states[54] to ensure the enjoyment of fundamental freedoms at work, applicable also to third parties, i.e. employers; and today, as argued here, also to providers of surveillance services often embedded in the corporate structure.[55]

In the absence of any jurisprudence from Art. 4, 9-11, 14 ECHR on surveillance practices detrimental to fundamental freedoms at work, however, it is possible to reconstruct a clear orientation on the matter by the ECtHR. The result is significant and coincides offers a similar conceptualisation, albeit from different premises, to the one now widespread on Art. 8 ECHR. Article 8 ECHR would be the foundation from which all other fundamental freedoms derive in a digitised society (See supra par. 4.2); the ECtHR with regard to fundamental freedoms is however more specific: employees and unions, with regard to

[47] Demir and Baykara v Turkey (2008) App no 34503/97 (ECtHR 12 Novembre 2008); Enerji Yapi-Yol Sen v Turkey (2009) App no 68959/01 (ECtHR 21 April 2009). *See* also: Ognevenko v. Russia (2018) App no 44873/09 (ECtHR 20 November 2018); Hrvatski Lijecnicki Sindikat v. Croatia (2015) App no 36701/09 (ECtHR 25 February 2015); Sorensen and Rasmussen v. Denmark (2006) App no 52620/99 and 52562/99 (ECtHR 11 January 2006); Sigujonsson v. Iceland (1993) App no 16130/90 (ECtHR 20 June 1993).

[48] Demir and Baykara v Turkey para 144.

[49] Art. 28 CFREU: Workers and employers, or their respective organisations, have, in accordance with Union law and national laws and practices, the right to negotiate and conclude collective agreements at the appropriate levels and, in cases of conflicts of interest, to take collective action to defend their interests, including strike action.

[50] Demir and Baykara v Turkey para 85.

[51] Sorensen and Rasmussen para 54; Olafsson v. Iceland para 30-31.

[52] Mantouvalou V., *Are Labour Rights Human Rights?*, in *European Labour Law Journal,* 3, 2, 2021, 151, http://journals.sagepub.com/doi/10.1177/201395251200300204.

[53] National Union of Belgian Police para 39.

[54] Respectively, to refrain from interference and to promote fundamental labour rights.

[55] Wilson and Palmer v United Kingdom (2002) nos. 30668/96, 30671/96 and 30678/96 (ECtHR 30 January 2002).

workplace measures that may have a direct impact on their working conditions, must receive appropriate information from their employer or anyone involved (Wilson and Palmer v. United Kingdom) that allows them to act meaningfully – individually or collectively – to secure their interests.[56] The ECtHR therefore states, as a matter of principle, that due to the imbalance of power and information within an employment relationship, the parties who have fewer means to defend their interests must benefit from regulations that bridge that informational and power gap.[57] By looking beyond Art. 8 ECHR, the Court's positions on the purpose and effectiveness of fundamental rights at work may indeed provide us with further new 'foundations' for identifying principles of explainability and understanding of workplace surveillance under the ECHR.

4.4. Explainability and understanding the new surveillance beyond art. 8 ECHR: stressing the redistributive function of fundamental labour rights.

The search for principles of explainability and understanding of surveillance has so far collided with the relative nature of privacy and data protection rights. Article 8 ECHR, in fact, proves to be particularly sensitive to balances with spheres of economic and security needs. However, the ECtHR has elsewhere argued on the eminently redistributive nature of fundamental rights at work; hence further reasonings might be found on a minimum threshold of transparency and accountability of the new surveillance by AI and IoT involving employers, employees and third parties involved in the employment relationship (such as providers). The explainability and understanding of AI and IoT surveillance then emerge from a broader look rather than from watertight analyses focused either on privacy or fundamental labour rights. Assessing proportionality and necessity between the employee's right to privacy and the employer's right to security (and property) cannot be easily accomplished today. As the collection of data is standard in contemporary workplaces, it is increasingly difficult for a lawmaker or lawyer to discern between harmful and non-detrimental surveillance.[58] Focusing particularly on the Spanish case, the interference with Article 8 ECHR might not be disproportionate but the pattern of interferences might constitute a violation (the employer spied on employees in some of its premises). Using the words of Kaiser (2018):

The Courts are bound to study the legislation in isolation, and (…) only upon challenge from an individual (…). This absence of meaningful standards against the cumulative effect of intrusions into the right to privacy should be regarded as a grave threat to the fundamental rights of the individual.[59]

[56] National Union of Belgian Police para 39.
[57] Arabadjieva K., *Worker Empowerment, Collective Labour Rights and Article 11 of the European Convention on Human Rights*, in *Human Rights Law Review*, 22, 1, 2022, 2.
[58] Elrick L. E., *The Ecosystem Concept: A Holistic Approach to Privacy Protection,* in *International Review of Law*, in *Computers & Technology,* 35, 1, 2021, 24.
[59] Elrick L. E., nt. (58), 33.

Opinion 01/2014 of Article 29 WP echoes this position stressing the need for a harmonious and comprehensive application of fundamental rights, being "necessary to assess how the new measure would add to the existing ones and whether all of them taken together would still proportionately limit the fundamental rights of data protection and privacy"[60].

A new framework emerges from the intensified possibility of surveillance, the involvement of providers, the essential freedoms at work and the right to privacy and data protection. The Strasbourg Court from the new technological context ought to track the impact of the employees' new overexposure when assessing the necessity and proportionality of surveillance measures.[61] The human rights literature, in other terms, supports this need to update the Courts' margins of appreciation: the contextual and historical nature of fundamental rights is essential to extrapolate their overall function.[62] Thus, the redistributive function of fundamental labour rights as described by the Court should be evaluated as a crucial and complementary element in the assessment of transparency and accountability under Art. 8 ECHR: individual and collective labour rights effectively ensure that employees and trade unions are sufficiently independent to determine their own interests and pursue them in a meaningful way.[63] The explainability and understanding of a workplace surveillance measure may therefore be affirmed as embedded in the various positions taken by the Court, and as principles that would find fertile application in future jurisprudence addressing surveillance through AI and IoT and the effectiveness of fundamental labour rights. Thus, updating the assessment of the necessity and proportionality of a surveillance measure in a context where privacy and data protection as individual rights may recede into the background if not provided with a social protection function peculiar to labour regulation.

The redistributive function of explaining and understanding surveillance also calls into question the asymmetries of power and information from the outsourcing of surveillance. Similar to how states are bound to respect human rights, so should not only employers, but also companies that produce and operate surveillance software and hardware. The ECtHR has already proven to hold third parties liable for violating fundamental rights at work. Therefore, companies offering surveillance services are allegedly co-responsible for the restriction of fundamental freedoms at work, in the new surveillance-managed workplaces.[64] Despite being third parties to the employment contract, often they effectively define the working conditions, sometimes without the employer's being aware of it. Accordingly, a new

[60] Article 29 Data Protection Working Party, *Opinion 01/2014 on the Application of Necessity and Proportionality Concepts and Data Protection within the Law Enforcement Sector*, 2014, 21, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf.

[61] The first main conceptualisation of privacy as a liberal right complemented by the social nature of labour regulation was provided by Otto M., nt. (8) 171–199.

[62] Fields A. B., Narr W. D., *Human Rights as a Holistic Concept,* in *Human Rights Quarterly*, 14, 1, 1992, 3 https://www.jstor.org/stable/762549?origin=crossref.

[63] National Union of Belgian Police para 39.

[64] A preliminary analysis on technology's impact on fundamental rights is already a subject of debate in the literature on business and human rights, Ebert I., Wildhaber I., Adams-Prassl J., *Big Data in the Workplace: Privacy Due Diligence as a Human Rights-Based Approach to Employee Privacy Protection*, in *Big Data & Society*, 8, 1, 2021, http://journals.sagepub.com/doi/10.1177/20539517211013051.

technology, when entering the workplace surveillance market, can be evaluated with regard to the effects it might have upon fundamental rights at work.[65]

5. Conclusion: orienting the scope of art. 8 ECHR through labour rights.

Article 8 ECHR guarantees a right to private life often confronted with economic and organisational demands in employment contexts. However, the technological scenario is expanding surveillance capabilities, and such business needs risk encroaching on greater portions of the employee's privacy and autonomy and then curtailing fundamental freedoms at work. Identifying here principles of explainability and understanding of surveillance aims for a minimum threshold of transparency and accountability of surveillance. Such principles might arise from a joint reading of the case law on the right to private life and the redistributive nature of fundamental rights at work. Looking for such principles in the Strasbourg Court's approach allows for the substantiation of what Otto (2016) far-sightedly asserted: Article 8 ECHR cannot by itself rebalance the structurally asymmetries of information and power arising from an employment contract. Privacy and data protection must be read complementarily to fundamental labour rights: the lack of this complementarity risks to systematically let the economic and employer interest in surveillance prevail.[66] The purpose of labour rights can then provide the Strasbourg Court with a margin of appreciation that goes beyond the mere protection of individual spheres of intimacy, encroaching the protection of essential individual and collective freedoms, such as equal treatment, trade union freedoms, and the prohibition of forced labour. A fundamental right to receive explanations tailored to the recipient, together with a general disclosure of the functioning of surveillance systems to include social partners, would counterbalance a significant technological innovation which currently makes subordinate employment increasingly unbalanced in terms of information and power sharing. Detecting the explainability and understanding of surveillance in ECtHR case law would then round off the quest pursued all along: a (technologically) contextualised margin of appreciation from the ECtHR that values fundamental labour rights and curtails exorbitant surveillance capabilities arising from the AI and IoT-based landscape.

[65] Elrick L.E., nt. (58), 39–40; Couzigou I., T*owards a State-Private Actor Partnership in Securing Cyberspace,* in *Research Centre for Constitution and Public International Law Working Paper Series,* 2, 2019, https://www.law.ed.ac.uk/sites/default/files/2020-09/ECIGL%20Working%20Paper%20-%20I%20Couzigou_0%20-%20Acc.pdf.
[66] Otto M., nt. (8), 195.

Bibliography

Adams-Prassl J., *What If Your Boss Was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at* Work, in *Comparative Labor Law And Policy Journal,* 41, 1, 2019, 123 ff.;

Aloisi A., De Stefano V., *Essential Jobs, Remote Work and Digital Surveillance: Addressing the COVID-19 Pandemic Panopticon*, in *International Labour Review*, 161, 2, 2022, 289-314;

Aloisi A., Gramano E., *Artificial Intelligence Is Watching You at Work. Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context,* in *Comparative Labor Law And Policy Journal,* 41, 1, 2019, 95-114;

Arabadjieva K., *Worker Empowerment, Collective Labour Rights and Article 11 of the European Convention on Human Rights*, in *Human Rights Law Review*, 22, 1, 2022;

Ball K., *Workplace Surveillance: An Overview*, in *Labor History*, 51, 1, 2010, 87;

Bogg A., *Republican Non-Domination and Labour Law: New Normativity or Trojan Horse?*, in *International Journal of Comparative Labour Law and Industrial Relations*, 33, 3, 2017, 391-418;

Broeders D., Schrijvers E., van der Sloot B., van Brakel R., de Hoog J, Hirsch Ballin E., *Big Data and Security Policies: Towards a Framework for Regulating the Phases of Analytics and Use of Big Data*, in *Computer Law & Security Review*, 33, 3, 2017, 309;

Bueno N., *Freedom at, through and from Work: Rethinking Labour Rights*, in *International Labour Review*, 160, 2, 2021, 311-329;

Collins H., *Is the Contract of Employment Illiberal?* in Collins H. (ed.), *Philosophical Foundations of Labour Law*, Oxford, Oxford University Press, 2018;

Collins P., *The Right to Privacy, Surveillance-by-Software and the "Home-Workplace"*, in *UK Labour Law Blog*, 3 September 2020;

Couzigou I., T*owards a State-Private Actor Partnership in Securing Cyberspace,* in *Research Centre for Constitution and Public International Law Working Paper Series,* 2, 2019;

De Stefano V., *"Masters and Servers": Collective Labour Rights and Private Government in the Contemporary World of Work,* in *International Journal of Comparative Labour Law and Industrial Relations*, 36, 4, 2020, 425-444;

De Stefano V., Taes S., *Algorithmic Management and Collective Bargaining*, in *European Trade Union Institute Policy Brief Series*, 10 May, 2021;

Delfanti A., *Machinic Dispossession and Augmented Despotism: Digital Work in an Amazon Warehouse*, in *New Media & Society*, 23, 1, 2021, 39;

Delfino G. F., Van Der Kolk B., *Remote Working, Management Control Changes and Employee Responses during the COVID-19 Crisis*, in *Accounting, Auditing & Accountability Journal*, 35, 6, 2021;

Dick R. P., Shang L.; Wolf M., Yang S.., *Embedded Intelligence in the Internet-of-Things*', in *IEEE Design & Test*, 37, 1, 2020, 7;

Ebert I., Wildhaber I., Adams-Prassl J., *Big Data in the Workplace: Privacy Due Diligence as a Human Rights-Based Approach to Employee Privacy Protection*, in *Big Data & Society*, 8, 1, 2021;

Elrick L. E., *The Ecosystem Concept: A Holistic Approach to Privacy Protection,* in *International Review of Law*, in *Computers & Technology,* 35, 1, 2021, 24;

Eurofound, *Employee Monitor-45ing and Surveillance the Challenges of Digitalisation*, 2020;

European Trade Union Confederation, *Commission's Proposal for a Regulation on Artificial Intelligence Fails to Address the Workplace Dimension,* 28 May 2021;
Fields A. B., Narr W. D., *Human Rights as a Holistic Concept,* in *Human Rights Quarterly*, 14, 1, 1992, 3;
Ghosh A., Chakraborty D., Law A., *Artificial Intelligence in Internet of Things*, in *CAAI Transactions on Intelligence Technology*, 3, 4, 2018, 208-218;
Hamon R., Junklewitz H., Sanchez I., Malgieri G., De Hert P., *Bridging the Gap Between AI and Explainability in the GDPR: Towards Trustworthiness-by-Design in Automated Decision-Making*, in *IEEE Computational Intelligence Magazine*, 17, 1, 2022, 72-85;
Hansen E.B., Bøgh S., *Artificial Intelligence and Internet of Things in Small and Medium-Sized Enterprises: A Survey*, in *Journal of Manufacturing Systems*, 58, Part B, 2021, 362-372;
Hiranandani V., *Privacy and Security in the Digital Age: Contemporary Challenges and Future Directions, in The International Journal of Human Rights*, 15, 7, 2011, 1091-1106;
Janiesch, C., Zschech, P., Heinrich, K., *Machine learning and deep learning*, in *Electronic Markets* 31, 2021, 685–695;
Jarrahi M. H., Newlands G., Sutherland W., *Algorithmic Management in a Work Context*, in *Big Data & Society*, 8, 2, 2021;
Kaminski M. E., Malgieri G., *Algorithmic Impact Assessments under the GDPR: Producing Multi-Layered Explanations'*, in *International Data Privacy Law*, 11, 2, 2021, 125-144;
Kaminski M. E., *The Right to Explanation, Explained,* in *Berkeley Technology Law Journal*, 34, 1, 2019;
Kim P. T., Bodie M. T., *Artificial Intelligence and the Challenges of Workplace Discrimination and Privacy,* in *Journal of Labor and Employment Law*, 35, 2, 2021, 289-315;
Köchling A., Wehner M. C., *Discriminated by an Algorithm: A Systematic Review of Discrimination and Fairness by Algorithmic Decision-Making in the Context of HR Recruitment and HR Development*, in *Business Research,* 13, 2020, 795-848;
Koops B. J., *The Concept of Function Creep*, in *Law, Innovation and Technology*, 13, 1, 2021, 29-56;
Levy K., Barocas S., *Privacy at the Margins | Refractive Surveillance: Monitoring Customers to Manage Workers*, in *International Journal of Communication*, 12, 2018;
Lupton D., *The Quantified Self: A Sociology of Self-Tracking,* Polity, Cambridge, 2016;
Mantouvalou V., *Are Labour Rights Human Rights?*, in *European Labour Law Journal,* 3, 2, 2021, 151-172;
Mifsud Bonnici J. P., *Exploring the Non-Absolute Nature of the Right to Data Protection*, in *International Review of Law, Computers & Technology,* 28, 2, 2014, 131-143;
Negrón W., *Little Tech Is Coming for Workers. A Framework for Reclaiming and Building Worker Power*, CoWorker.org 2021;
Nguyen A., *The Constant Boss - Labor Under Digital Surveillance,* in *Data & Society Research Institute*, 2021;
OECD, *Algorithms and Collusion: Competition Policy in the Digital Age*, 2017;
Otto M., *The Right to Privacy in Employment: A Comparative Analysis,* Hart Publishing, Oxford, 2016;
Otto M., '*Workforce Analytics' v Fundamental Rights Protection in the EU in the Age of Big Data,* in *Comparative Labor Law and Policy Journal*, 40, 3, 2019, 389-404;

Tapiola K., *What Happened to International Labour Standards and Human Rights at Work?* in Halonen T., Liukkunen U. (eds.), *International Labour Organization and Global Social Governance*, Springer International Publishing, Helsinki, 2021;
Trade Union Congress, *Technology Managing People: The Worker Experience*, 2020;
Turanjanin V., *Video Surveillance of the Employees between the Right to Privacy and Right to Property after Lopez Ribalda and Others v. Spain Articles & Essays*, in *University of Bologna Law Review*, 5, 2, 2020, 268;
Varošanec I., *On the Path to the Future: Mapping the Notion of Transparency in the EU Regulatory Framework for AI*, in *International Review of Law, Computers & Technology,* 36, 2, 2022;
Wachter S., Mittelstadt B., *A Right to Reasonable Inferences*, in *Columbia Business Law Review,* 2, 2019, 494-620.
Wachter S., Mittelstadt B., Floridi L., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 7, 2, 2017, 76-99;
Wachter S., *The GDPR and the Internet of Things: A Three-Step Transparency Model*, in *Law, Innovation and Technology*, 10, 2, 2018, 266–267;