ARTIFICIAL INTELLIGENCE IS WATCHING YOU AT WORK: DIGITAL SURVEILLANCE, EMPLOYEE MONITORING, AND REGULATORY ISSUES IN THE EU CONTEXT

Antonio Aloisi† & Elena Gramano††

I. INTRODUCTION

New technologies are reshaping work in an ever-growing number of fields. The current wave of industrial development is boosted by the proliferation of cyber-physical infrastructure and interconnected systems making possible new practices of profiling, organizing, and monitoring. The resulting gigantic datasets in turn lay the groundwork for the artificial intelligence (AI) boom. Only recently, however, have international, European, and domestic institutions started considering how to update existing regulation in order to tackle the complex and far-reaching challenges posed by ubiquitous tech devices and, more specifically, by AI,[1] a general-purpose application able to mimic *adaptive* and *predictive* "functions that humans associate with their own intelligence."[2] More concretely, several AI features are *embedded* as components of larger tech systems increasing their computational power, rather than stand-alone structures.[3] Despite that, there is still scant knowledge about the various impacts, not all of which are

† Assistant Professor of European and Comparative Labour Law at IE Law School, IE University, Madrid.

†† Postdoctoral Research Fellow at Goethe University of Frankfurt am Main, Institute for Labour and Civil Law. We are most grateful to the organizers and participants at the ILO-KU Leuven workshop for great discussion and feedback on earlier version of this work.

1. *See Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions*, COM SWD(2018) 237 final (Apr. 25, 2018). *See also* European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL) O.J. (C 252) 239 (2018). For a preliminary comment, see Aída Ponce Del Castillo, *A law on robotics and artificial intelligence in the EU?*, 2017 ETUI FORESIGHT BRIEFS 1.

2. Peter Cappelli, Prasanna Tambe, & Valery Yakubovich, *Artificial Intelligence in Human Resources Management: Challenges and a Path Forward* (Nov. 1, 2018), *available at* SSRN: https://ssrn.com/abstract=3263878.

3. Report by the High-Level Expert Group on Artificial Intelligence, *A definition of AI: Main capabilities and scientific disciplines*, at 1, COM (2019) (Apr. 8, 2019).

unprecedented,[4] of these powerful and multifarious innovations that, in the context of an employment relationship, can be considered as an effective combination of big data analytics[5] and algorithmic governance[6] in an optimized manner.

Technological advances ensure frictionless, accessible, and convenient information exchanges. More importantly, these devices are likely to deeply alter the relationship between employers and employees (or between clients and workers), given that hyperconnected equipment is responsible for a significant transformation of how work is rendered, both at the individual and the collective level. Concomitantly, on the part of the employer, day-to-day decisions can be more informed, property rights can be protected, productivity improved, loss of company property prevented, and waste production minimized.[7] In tandem with these changes, new working arrangements emerge, including the well-examined platform work and the relatively neglected extended family of "logged-in" jobs.[8] In this respect, the field of AI is experiencing a wave of rapid progress. The increasingly blurred boundaries between professional and private lives represent the lifeblood of the current remodeling, "creating significant challenges to privacy and data protection."[9] To make things worse, the cheap, massive and imperceptible production, capturing, collection and usage of data, in conjunction with effective cloud storage and computing, machine learning,[10] Internet of Things (IoT),[11] neuronal networks and mobile robotics enable new evidence-based human resources and intensive management practices. Instead of facilitating an emancipating new environment, the risk is that intrusive technology could be used to deepen hierarchy and control over work

4. ROGER BLANPAIN & MARC VAN GESTEL, USE AND MONITORING OF E-MAIL, INTRANET AND INTERNET FACILITIES AT WORK: LAW AND PRACTICE (2004).

5. *See* Matthew T. Bodie et al., *The Law and Policy of People Analytics*. 88 U. COLO. L. REV. 961 (2017); Marta Otto, *"Workforce Analytics" V Fundamental Rights Protection in the EU in the Age of Big Data*, 40 COMP LAB. L. & POL'Y J. 389 (2019); Vincenzo Zeno-Zencovich & Giorgio Giannone Codiglione, *Ten Legal Perspectives on the 'Big Data Revolution'*, 23 CONCORRENZA E MERCATO 29 (2016).

6. Mirela Ivanova et al., *The App as a Boss? Control and Autonomy in Application-Based Management*, 2 INTERDISZIPLINÄRER ARBEITSFORSCHUNG (2018). As explained by Ernst, "[a]n algorithm can be understood as an unambiguous, executable sequence of clearly defined instructions of finite length to solve a problem." Christian Ernst, *Algorithmische Entscheidungsfindung und personenbezogene Daten*, 72 JURISTENZEITUNG (2017).

7. Alessandro Mantelero, *Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection*, 32 COMPUTER L. & SEC. REV. 238 (2016). *See also* Alexandra Mateescu & Aiha Nguyen, *Workplace Monitoring & Surveillance*, DATA & SOCIETY (2019), *available at* https://goo.gl/Cv4EAi.

8. SARAH KESSLER, GIGGED: THE END OF THE JOB AND THE FUTURE OF WORK (2018).

9. *Opinion 2/2017 on data processing at work*, WP 249 (June 8 2017), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169.

10. Harry A. Surden, *Machine Learning and Law*, 89 WASH. L. REV. 87 (2014).

11. Derek Zimmer, *The Internet of Things is Surveillance*, PRIVATE INTERNET ACCESS, Nov. 21, 2018, https://www.privateinternetaccess.com/blog/2018/11/the-internet-of-things-is-surveillance/.

performance, team dynamics, usage habits, social media behavior, and even sensitive characteristics.[12]

We believe that the traditional legal arsenal regulating the monitoring power of the employer and the right to privacy of employees, compounded by the most recent interventions, such as the EU General Data Protection Regulation (GDPR),[13] represents a robust starting point. A question worth asking, however, is whether authority today is the same as authority in the past. Indeed, more often than not, the scope of application of certain provisions on data protection—based on an "analogue" understanding of ICT—in several civil law jurisdictions may fall short in providing an up-to-date model capable of addressing unforeseeable technological advances. In particular, this contribution aims to examine whether and to what extent the current legal framework—in the context of the European Union—is suited to regulate the "augmented" magnitude of managerial prerogatives and, in particular, control power.[14] Since technologies constitute a moving target as they change quickly and deeply, the issues that need to be considered are the following: how can competing interests (the employer's need for information and the employee's need for privacy) be reconciled in a constantly changing world of work? No less important, is there a need for new legislation or is a more effective enforcement of existing regulation enough?

The article is organized as follows. After describing the new arenas of workplace surveillance, we provide a comprehensive conceptualization of AI application. Section 2 explores the latest generation of digital devices, understood in their broadest definition encompassing both physical supports as well as intangible tools. Section 3 describes how the EU has set the tone globally in the regulation of privacy and data protection. Section 4 describes how some European civil law systems deal with the regulation of surveillance of workers. The cases of France, Germany and Italy are analyzed by stressing the common elements and loopholes. Section 5 assesses some conclusions by verifying whether the current regulations are suitable to cope with the adoption of AI-enabled technologies at work.

12. Phoebe Moore, *The Mirror for (Artificial) Intelligence: In Whose Reflection?*, 41 COMP. LAB. L. & POL'Y J PG# (2019)

13. 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), 2016 O.J. (L 119) 1.

14. Valerio De Stefano, *'Negotiating the Algorithm': Automation, Artificial Intelligence and Labour Protection*, 41 COMP. LAB. L. & POL'Y J PG# (2019)

II. "ALL AI ON YOU": THE SURVEILLANCE POTENTIAL OF NEW TECHNOLOGIES, AND WHY IT MATTERS

To begin with, human substitution is a recurring theme when it comes to analyzing the impact of AI[15]: several tasks or jobs can be performed by complex lines of code, which can be trained thanks to the huge amount of data collected. The narrative of a "workless future" seems to have prevailed in mainstream accounts of AI to the detriment of a deep understanding of its more mundane functions. Admittedly, the overstatement surrounding the advent of breakthrough technologies[16] has not done a great service to the cause of understanding the legal implications of digital transformation when it comes to surveillance and the balance that is to be struck between authentic organizational needs and workers' protection.[17] Thus, it is perhaps not the number of jobs lost through advanced automation that should worry public opinion most but rather the subtle potential of AI and algorithms,[18] leading to a model of control and appraisal without an intuitive link between what is done when "logged-in" and how it is assessed. Zuboff has for some years been describing the potential in terms of technology "informating" work[19]—a long-lasting process of datafication that is increasingly functional since, more than ever before,[20] we are witnessing a resurgence of highly standardized organizational patterns.

In a paper prepared by the International Labour Organization to support the Global Commission on the Future of Work,[21] three groups of tasks are indicated as the focus of AI applications: matching, classification, and process-management. In the first case, AI helps businesses identify matches in ride-hailing and accommodation services, retail, or human resource management, by "reducing costs on finding customers or suppliers and offering less expensive solutions to their growing customer base." The second area of application includes recognition techniques in relation to the

15. JERRY KAPLAN, HUMANS NEED NOT APPLY: A GUIDE TO WEALTH AND WORK IN THE AGE OF ARTIFICIAL INTELLIGENCE (2015).

16. CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY (2016).

17. For an overview, see Brishen Rogers, *Beyond Automation: The Law & Political Economy of Workplace Technological Change* 24 (Roosevelt Institute Working Paper, 2019), *available at* https://ssrn.com/abstract=3327608

18. John Danaher, *The Threat of Algocracy: Reality, Resistance and Accommodation,* 29 PHIL. & TECH. 245 (2016).

19. Shoshana Zuboff, *Big other: surveillance capitalism and the prospects of an information civilization*, 30 J. INFO. TECH. 75 (2015). For a critical comment, see Evgeny Morozov, *Capitalism's New Clothes*, THE BAFFLER (Feb. 4, 2019), https://thebaffler.com/latest/capitalisms-new-clothes-morozov.

20. Jose van Dijck, *Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology*, 12 SURVEILLANCE & SOC'Y 197 (2014).

21. Ekkehard Ernst et al., *The economics of artificial intelligence: Implications for the future of work*, 5 ILO FUTURE OF WORK RESEARCH PAPER SERIES 1 (ILO, 2018).

increase in surveillance. Lastly, AI makes it possible to "up-stream producers to integrate diversified supply chains through better information about product quality, certification schemes and market conditions." Far more problematic is that, while implementing these applications, artificial intelligence is writing a new chapter in the long history of ubiquitous worker surveillance, today based on time management, keystrokes, social media interactions, call logs, screenshots, search queries and even eye tracking, facial recognition software, smartphone sensors, and smart glasses.[22] However, the essential characteristic of AI, which makes it unique compared to other types of monitoring tools, resides in its "marriage of convenience" of already existing authoritative practices.[23]

Simple proxies or imperfect measures such as the number of emails sent, the list of websites visited, cookies, or documents and apps opened may offer indicators for seemingly "data-driven" or "evidence-based" personnel management decisions,[24] leading to new forms of anticipatory conformity,[25] both prior to and after hiring. Experts warn of the possible ways in which more and more processes and choices made by managers with regard to recruiting, remuneration and even dismissals are automated, too often giving free rein to discriminatory biases, perpetuating social segregation and impairing humanness and fairness.[26] Simply put, technologies in the field of AI increase the possibilities for hierarchical management and digital surveillance in a way that is unprecedented, tighter than before, and not even desired.[27] But the disastrous consequences do not stop there. What may begin as an online vetting for entry-level candidates "ends with the transformation of nearly every aspect of hiring, performance assessment and management."[28] All this may be done by means of systems that, once designed and calibrated, run automatically and gather enormous amounts of granular data about workers' behaviors from different sources, often far

22. Ifeoma Ajunwa, Kate Crawford & Jason Schultz, *Limitless worker surveillance*, 105 CAL. L. REV. 102 (2017). Ifeoma Ajunwa, *Algorithms at Work: Productivity Monitoring Platforms and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law*, ST. LOUIS U. L. J. 63 (2018).

23. *See* David Chandler, *Digital Governance in the Anthropocene: The Rise of the Correlational Machine*, *in* DIGITAL OBJECTS, DIGITAL SUBJECTS: INTERDISCIPLINARY PERSPECTIVES ON CAPITALISM, LABOUR AND POLITICS IN THE AGE OF BIG DATA (David Chandler & Christian Fuchs eds., 2019).

24. Olivia Solon, *Big Brother isn't just watching: workplace surveillance can track your every move*, GUARDIAN (Nov. 6, 2017), https://www.theguardian.com/world/2017/nov/06/workplace-surveillance-big-brother-technology.

25. Kirstie Ball, *Workplace surveillance: an overview*, 51 LAB. HIST. 87 (2010).

26. Claudia Schubert & Marc-Thorsten Hütt, *Economy-on-demand and the fairness of algorithms*, 10 EUR. LAB. L.J. 3 (2019).

27. Phoebe V. Moore, Martin Upchurch and Xanthe Whittaker, *Humans and Machines at Work: Monitoring, Surveillance and Automation in Contemporary Capitalism*, *in* HUMANS AND MACHINES AT WORK: MONITORING, SURVEILLANCE AND AUTOMATION IN CONTEMPORARY CAPITALISM (Phoebe V. Moore, Martin Upchurch & Xanthe Whittaker eds., 2018).

28. Don Peck, *They're Watching You at Work,* THE ATLANTIC (Dec. DATE 2013), https://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681/.

beyond what is necessary. In addition, by drawing "non-intuitive and unverifiable" inferences from data,[29] workforce analytics driven by AI may develop predictive capabilities.

As a result, AI has an impact on freedom, privacy, but also autonomy and moral reasoning, which is much more relevant in a society in which the traditionally strict separation between private life and professional life is dissolving. Algorithms can be trained to become increasingly efficient, with the risk of them spiraling out of control. Moreover, the lack of transparency may in turn result in workers' deviance and misconduct. More often than not, AI applications benefit from an ostensibly participatory character that encourages the seamless sharing of information in exchange for little rewards in terms of reputation or promotions. The underlying workplace culture also emphasizes individual measurement and self-tracking,[30] in relation to gamified internal programs. Concomitantly, while the perils of the "devil's bargain,"[31] which consumers must conclude in exchange for unfettered access to apparently free services based on a glittering promise of connectivity, convenience, personalization, and innovation, have largely been exposed and countered,[32] less investigated is the way feedback mechanisms, surveillance, and data—now perceived as essential organizational components—are altering the balance of power in the workplace.

III. THE EUROPEAN UNION TAKES THE LEAD: "GDPR" AND THE BALANCE BETWEEN COMPANIES' LEGITIMATE INTERESTS AND REASONABLE PRIVACY EXPECTATIONS OF EMPLOYEES

Personal data has progressively "become both the source and the target of AI applications."[33] Therefore, before exploring the selected national cases and the various approaches to monitoring devices and digital surveillance facilitated by AI, it is significant to scrutinize the multilevel legal framework

29. Sandra Wacther, *Data protection in the age of big data*, 2 *Nature Electronics* 6 (2019). For a broad definition of "sensitive data," see Case C-434/16, Peter Nowak v. Data Prot. Comm'r, 2017 E.C.R. (excluding inferences from the scope of data protection law); Case T-190/10 Kathleen Egan and Margaret Hackett v. European Parliament, 2012 E.C.R. (attributing the status of "personal data" to inferences).

30. Melanie Swan, *The quantified self: Fundamental disruption in big data science and biological discovery*, 1 BIG DATA 85 (2013).

31. Nathan J. Davis, *Presumed assent: The judicial acceptance of clickwrap*, 22 BERKELEY TECH. L.J. 577 (2007).

32. Sam Adler-Bell and Michelle Miller, *The Datafication of Employment. How Surveillance and Capitalism Are Shaping Workers' Futures without Their Knowledge,* THE CENTURY FOUNDATION (Dec. 19, 2018), https://tcf.org/content/report/datafication-employment-surveillance-capitalism-shaping-workers-futures-without-knowledge/?agreed=1.

33. Eur. Consult. Ass., *Consultative Comm. of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Convention 108, Doc. No. T-PD(2019)-01 (2019).

regulating data protection at work[34] or, according to a definition that has gone out of fashion, the right to privacy.[35] An examination of the labor regulation governing profiling practices and workplace monitoring, which are strictly entwined, must necessarily be compounded by an "integrated" study of the General Data Protection Regulation (GDPR).[36] In particular, the most recent initiative taken by the institutions of the European Union represents a remarkable step forward, leading to a homogenization of national models instead of promoting a mere harmonization. Indeed, the redraft of the Data Protection Directive, morphed into a new regulation, is in its entirety and directly applicable law in all EU Member States. However, this section will provide a partial overview of the GDPR by focusing on a limited number of strictly labor-related provisions.

Besides avoiding fragmentation,[37] the merits go even further. The GDPR has indeed been hailed as one of the best examples of the so-called "Brussels effect," namely the "global power that the European Union is exercising through its legal institutions and standards (and sanction mechanism), successfully export[ing] that influence to the rest of the world."[38] The model may inform similar intervention in the field of digital services. Remarkably, many international companies, after weighing the

34. Universal Declaration of Human Rights, G.A. Res. 217A (III), art. 12, U.N. Doc. A/810 at 71 (1948); Charter of Fundamental Rights of the European Union, art. 7 & 8, 2010 O.J. (C 364); Treaty on the Functioning of the European Union (TFEU), art. 16, 2012 O.J. (C 326). International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, 999 U.N.T.S. 171. Directive 95/46/EC, 1995 O.J. (L 281) 31 (EC) (also known as Data Protection Directive, "DPD"), adopted on the basis of Art. 95 TEC. In 2012 the Commission submitted two legal instruments: a European regulation project (Regulation 2016/679, 2016 O.J. (L 119) 1 [EU]) intended to replace Directive 95/46/EC and a new directive replacing Framework Decision 977/2008/EC (regarding data processing within the fight against crime and terrorism). For an overview, see Fabrizio Petrucco, *The right to privacy and new technologies: between evolution and decay* in *MediaLaws*, 1 RIVISTA DIR. MEDIA, 1 (2019). *See also* European Parliament Resolution of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement, Eur. Parl Doc. 2016/2225(INI) (2017).

35. See Colin J. Bennett, *The European General Data Protection Regulation: An instrument for the globalization of privacy standards?*, 23 INFO. POLITY 239 (2018). The Directive owes much to the prior agreement on data protection principles within the OECD and the Council of Europe, designed the framework of the personal data protection at a time when digital surveillance was still nascent. Convention of the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, CETS No. 108.; Recommendation No. R(89)2 of the Council of Europe on the protection of personal data used for employment purposes; *Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data*, COUNCIL OF EUROPE (Jan. 23, 2017), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001 6806ebe7a. Most data protection laws reflect principles established in the OECD Guidelines. The Guidelines were issued in 1980 and updated in 2013. *See* Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD Doc.[C(80)58/FINAL, as amended on Jul. 11, 2013 by C(2013)79] (2013). Colin J. Bennett & Charles D. Raab, *Revisiting the governance of privacy: Contemporary policy instruments in global perspective*, REGULATION & GOVERNANCE (2018).

36. ALESSANDRA INGRAO, IL CONTROLLO A DISTANZA SUI LAVORATORI E LA NUOVA DISCIPLINA PRIVACY: UNA LETTURA INTEGRATA (2018).

37. General Data Protection Regulation 2016/679, 2018 O.J. (L 127) Recital 9 (EU) [hereinafter GDPR].

38. Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1 (2012).

costs of compliance, decided to voluntarily implement the provisions of such a normative exemplar globally, rather than relying on different models around the world.[39] As a consequence, through the process of "unilateral regulatory globalization" even reluctant market participants have to adapt to this set of measures, resulting in international convergence (which has been identified as a part of a broader "Europeanization" process). What is more, the law extends its reach beyond the boundaries of the EU to any company processing the data of EU citizens. Whether the regulation will "revolutionize the data landscape" or "fizzle into a footnote in digital history"[40] remains to be seen and depends mainly on its implementation.

In order to cope with rapid technological shifts, the GDPR was adopted in April 2016 and entered into force in May 2018, establishing a renewed set of guarantees and increasing the standard of data protection.[41] Whilst promoting the free flow of personal data with a view to developing the internal (digital) market, Regulation (EU) 2016/679 no longer pursues primarily commercial interests. The GDPR aims to guarantee a "consistent" level of data protection to each and every European citizen ("natural persons"), regardless of their nationality or place of residence (Art. 3.1). However, it should not go unmentioned that its Recital 4 states that the right to the protection of personal data "is not an absolute right" and "must be . . . balanced against other fundamental rights, in accordance with the principle of proportionality."[42] In addition, Art. 88 of the GDPR specifies that 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. . . ."[43] This provision provides room for maneuver for the design of "integrative legislation designed to respond to the risk connected to big data analytics in

39. There have been calls for a "US version of GDPR." *See* Fahmida Y. Rashid, *Congress May Consider a U.S. Version of GDPR*, DECIPHER (Nov. 9, 2018), https://duo.com/decipher/congress-may-consider-a-us-version-of-gdpr.

40. Samuel Greengard, *Weighing the impact of GDPR*, 61 COMM. OF THE ACM 16-18 (2018).

41. ENRICO PELINO, CAMILLA BISTOLFI & LUCA BOLOGNINI, IL REGOLAMENTO PRIVACY EUROPEO. COMMENTARIO ALLA NUOVA DISCIPLINA SULLA PROTEZIONE DEI DATI PERSONALI (2016).

42. Note that Recitals are nonbinding provisions.

43. The article lists the following examples:

> recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organization 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.

The discretion left to the Member States as regards the rules to enact and the eventuality itself to implement such regulation may lead to an inhomogeneous framework of standards. *See* Julian Wagner & Alexander Benecke, *National Legislation within the Framework of the GDPR*, 2 EUR. DATA PROT. L. REV. 353 (2016).

the employment relationship,"[44] by devising procedural rules more incisively at a decentralized level.[45]

In line with the previous Data Protection Directive ("DPD"), the scope of application of the Regulation is rather broad and easily met[46]: "processing" is used to refer to "any operation . . . which is performed on personal data . . . whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (Art. 4, 1 and 2). Likewise, the concept of personal data is broad, but perhaps less easily met: "personal data" is defined as "any information relating to an identified or identifiable natural person ('data subject')." As a result, personal data containing "anonymous information, . . . which does not relate to an identified or identifiable natural person," and data that is solely about companies is excluded from the GDPR's scope.[47] Contentious though it is,[48] personal data, "which ha[s] undergone pseudonymisation, which could be attributed to a natural person by the use of additional information," should be considered as falling within its scope[49]—something that is very relevant for AI applications.

In this respect, GDPR should be read in conjunction with the documents issued by the Independent EU Advisory Body on Data Protection and Privacy (Art. 29 Working Party, "WP29"), comprised of the heads of the national data protection authorities, which anticipate the European Data Protection Board, in issuing guidelines, recommendations and best practices in order to foster a consistent application of the GDPR (Art. 70 (1)(e)).[50] Attention must

44. Annamaria Donini, *Employment Relationship and Big Data Analytics: Rules and Limits for Workers' Data-Driven Profiling*, *in* DIGITAL WORK AND PERSONAL DATA PROTECTION: KEY ISSUES FOR THE LABOUR OF THE 21ST CENTURY 397 (Nuno Cerejeira Namora et al. eds., 2018)

45. Whether or not social partners would seize this opportunity by imposing their agenda on the rule-makers still has to be determined. Indeed, when it comes to dealing with the technological transformation of work, the inherent flexibility of collective bargaining presents a unique opportunity, while new legislation might struggle to respond promptly to potential unforeseen developments. Jeremias Prassl, *Collective Voice in the Platform Economy: Challenges, Opportunities, Solutions*, REPORT TO THE ETUC (2018), https://goo.gl/n2yEMW. Todolí-Signes Adrian, *Algorithms, artificial intelligence and automated decisions about workers and the risks of discrimination: The necessary collective governance of data protection*, 25 Transfer (2019).

46. Manon Oostveen, *Identifiability and the applicability of data protection to big* data, 6 INT'L DATA PRIVACY L. 299 (2016).

47. GDPR, Recital 26.

48. Christopher Kuner et al., *Machine learning with personal data: is data protection law smart enough to meet the challenge?*, 7 INT'L DATA PRIVACY L. 1 (2017).

49. The GDPR also expands the definitions of personal data and sensitive data. It applies to data from which a living individual is identified or identifiable, whether directly or indirectly. *See* Viktor Mayer-Schonberger & Yann Padova, *Regime Change: Enabling Big Data through Europe's New Data Protection Regulation*, 17 COLUM. SCI. & TECH. L. REV. 315 (2015).

50. Set up under Article 29 of Directive 95/46/EC, the Art 29 Working Party, named after its establishing article in the DPD, is an independent European advisory body consisting of representatives from the national supervisory authorities/data protection authorities, the European Data Protection

be paid to the Opinion 2/2017 on data protection at work, adopted in June 2017, and aimed at complementing the Opinion 8/2001[51] and the 2002 Working Document.[52] Remarkably, the Opinion focuses on the impact of surveillance means on "all situations where there is an employment relationship, regardless of whether this relationship is based on an employment contract." At 6, the Opinion establishes a set of far-reaching principles, based on the equivalence of protection between new and "analogue communications." One of its merits is the attempt to outline the risk posed by new tech devices, as well as the "proportionality assessment" of a number of scenarios[53], including the recruitment process, in-employment screening, monitoring ICT usage both at and outside the workplace (e.g. home and remote working, "bring your own device" practices, wearable devices), monitoring of time and attendance, or through video systems, vehicle applications, and other operations.[54]

Art. 5(1)(a) of Reg. 2016/679 states that the data processing must respect the principles of lawfulness,[55] fairness and transparency. Moreover, other principles, belonging to the traditional arsenal of principles of data processing,[56] are incorporated in the GDPR such as purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality and accountability. Art. 6 lists a set of conditions of lawfulness according to which data can be processed: consent given by the data subject,[57] necessity

Supervisor and the European Commission. One of its tasks is to advise on data protection, which it does amongst others through issuing (non-binding) opinions, which are a source for the interpretation of EU data protection law.

51. Opinion 08/2001 on the processing of personal data in the employment context, Art. 29 – Data Protection WP [hereinafter WP 29], U.N. Doc. 5062/01/EN/Final WP 48 (Sep. 13, 2001, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf.

52. Working document on the surveillance of electronic communications in the workplace, WP 29, U.N. Doc. 5401/01/EN/Final WP 55 (May 29, 2002), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf.

53. Opinion 2/2017 on data processing at work, WP 29, U.N. Doc. 17/EN WP 249 (June 8, 2017), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169.

54. Eddie Keane, *The GDPR and Employee's Privacy: Much Ado but Nothing New*, 29 KING'S L.J. 359 (2018).

55. Employment contract is the legal basis for processing of data as long as this processing is necessary for the performance of the contract.

56. Pursuant to the case law on Article 8 of the European Convention on Human Rights (ECHR), the mere systematic collection and storage an individual's publicly available personal data can constitute an interference with the right to private life. The European Court of Human Rights (ECtHR) emphasized that an individual does not waive his or her rights by engaging in public activities that are subsequently documented European Court of Human Rights, *Rotaru v. Romania*, Application no. 28341/95, (2000). It held that it is irrelevant whether this systematic collection and storage of data inconveniences the applicant or whether the information concerned is sensitive or not. European Court of Human Rights, *Amann v. Switzerland*, Application no. 27798/95, 843 (2000). Orla Lynskey, *Grappling with "Data Power": Normative Nudges from Data Protection and Privacy*, 20 THEORETICAL INQUIRIES L. 189 (2019).

57. According to art. 4(11), "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." It cannot be "bundled" with other agreements and should also be revocable easily and at any time.

in the context of a contract, compliance with a legal obligation, protection of vital interest of the data subject, performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, legitimate interest, provided that the interests or fundamental rights and freedom of the data subject are not jeopardized. The purpose limitation principle, according to which processing requires a manifest purpose declared at the time of collection and not adjustable (especially for non-compatible uses[58]), has been defined as the "ground of the controller's powers."[59] As a consequence, greater weight must be given to initial choice concerning the aim of the processing (including an algorithmic one) that identifies and restricts the scope of operations.[60]

In the context of an employment relationship, according to Art. 7, "consent" can be necessary, but not in itself sufficient. The requirement has been reinforced by imposing obligations of intelligibility, clarity, and transparency with respect to the modalities of the request and by strengthening the right to withdraw consent. In order to assess the genuineness of such a consent, "utmost account shall be taken of whether, *inter alia*, the performance of a contract is conditional on consent." As stated in the WP29 Opinion 2/2017, "employees are seldom in a position to freely give, refuse or revoke consent" given the consequences they face in connection with their noncompliant conduct. Therefore, "unless in exceptional situations, employers will have to rely on another legal ground than consent." Regardless of the legal basis for processing, a proportionality test should be undertaken to consider whether it is necessary to achieve a legitimate purpose, whether it outweighs the data protection right, as well as the measures that have to be taken to ensure that infringements of the rights to private life and secrecy of communications are limited to a minimum. This can form part of a Data Protection Impact Assessment (DPIA).[61]

A. Automated Decision-Making Processes, the GDPR, and AI: Premises and Promises of a Complicated Relationship

As argued in the first section, once hired, employees are subject to (legitimate) surveillance and data extraction from their employers in a variety

58. GDPR, Art. 5(1)(b).

59. Federico Fusco, Employee Privacy in the Context of EU Regulation N.2016/679: Some Comparative Remarks, Presented at the XVI International Conference in Commemoration of Professor Marco Biagi in Modena, Italy (March 2018).

60. Art. 12, 13, 14 & 15 strengthen the right to transparent and adequate information and to access to data.

61. In addition, Art. 25 defines a system based on "data protection by design or by default," that is to say the implementation of the most privacy-friendly technical and organizational solutions to give effect to data-protection principles. Raphaël Gellert, *Data protection: a risk regulation? Between the risk management of everything and the precautionary alternativ*e, 5 INT'L DATA PRIVACY L. 3 (2015).

of ways.[62] By reason of the AI's characteristics, it is indeed in this context that its greatest potential is to be found and regulated accordingly. Serving as an impressive preliminary "experiment," the various experiences with gig platforms have lifted the veil momentarily by illustrating the harsh conditions of workers dispatched, organized, and controlled by algorithm-based decision-making processes.[63] Needless to say, opaque and insidious systems of both e-screening and performance appraisal are already in place "across a range of industries to manage wage-setting," in combination with the allocation of hours, and evaluation metrics related to hiring, promotions, and firing. Despite the collective attempts to decipher the internal logic of the metrics shaping the power relationships, the key operational components of systems such as people analytics and algorithmic governance constitute an unintelligible "black box," which is indented to keep most workers in the darkness as regards strategies, which, although partially autonomous, answer to specific organizational needs and reflect managerial choices.[64]

A positive development is that the GDPR is rather explicit in regulating the role of technologies substituting or integrating the prerogative of the employer.[65] Especially noteworthy for the purposes of this analysis is Art. 22 regulating "automated individual decision-making" processes.[66] In fact, the Regulation ought to be understood as precluding "a decision based solely on automated processing, . . . which produces legal effects concerning [the data subject] or similarly significantly affects him or her."[67] This is probably the most forward-looking chapter of the Regulation, aimed at providing a counterweight to the growth of automatization of organizational procedures.[68] The worker has the right not to be subject to decisions "based solely on automated processing, including profiling, which produces legal

62. Sandro Mezzadra & Brett Neilson, *On the multiple frontiers of extraction: excavating contemporary capitalism*, 31 CULTURAL STUD. 185 (2017).

63. Jeremias Prassl, *What if your boss was an algorithm? Economic incentives, legal challenges, and the rise of artificial intelligence at work*, 41 COMP. LAB. L. & POL'Y J PG # (2019).

64. FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015).

65. Emanuele Dagnino, *People Analytics: lavoro e tutele al tempo del management tramite big data*, 3 LAB. & L. ISSUES 1 (2017).

66. A version of this prohibition has already been part of the law in the European Union. According to Art. 15 of the European Directive 95/46/EC, there must be human review of any automated data-processing system that could have a substantial impact on an individual's life. *See* Lee A. Bygrave, *Automated Profiling, Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, 17 COMPUTER L. & SEC. REV. 17 (2001)

67. GDPR, art. 22.

68. The GDPR is inspired by the definition of profiling in the Council of Europe, *The protection of individuals with regard to automatic processing of personal data in the context of profiling*, Recommendation CM/Rec(2010)13 and explanatory memorandum (Nov. 23, 2010), https://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommendations/CMRec(2010)13E_Profiling.pdf. The Recommendation is a reference tool for its description of the three distinct stages of profiling: data collection, automated analysis to identify correlations, and applying the correlation to an individual to identify characteristics of present or future behavior.

effects," a formula well-suited to encompass most of the AI applications described in the introduction to this article. Interestingly, Art. 4(4) defines "profiling"—a relatively novel concept in European data protection law[69]—as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."

More precisely, the GDPR focuses on three main criteria: (1) decision making which is fully automated; even though, in a way paradoxically, it would be necessary to interpret the definition so as to encompass decisions made with some degree of authentic human involvement,[70] (2) personal data—but pseudonymized data easily pointing to specific data subjects may fall under this definition, and (3) aimed at implementing choices that have significant legal consequences or similar effects on the data subject.[71] The general prohibition[72] on solely automated individual decision making has a complementary set of exceptions requiring attention. It does not apply in the case when the automated process "(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller," (b) when authorized by Union or Member State, "(c) is based on the data subject's explicit consent." In the first and third case, the former clearly identifying a situation that would result from an employment relationship, the data controller "shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests." At the same time, the possibility of derogating from the prohibition by relying only on *explicit* consent seems unsuitable for AI-driven situations where "algorithms are inherently non-transparent in terms of their function and design or because even if they are transparent, they may not be intelligible to the data subject."[73]

69. A concrete example of this practice would be e-recruiting (Recital 71). See Mireille Hildebrandt, *Defining Profiling: A New Type of Knowledge?*, *in* PROFILING THE EUROPEAN CITIZEN (Mireille Hildebrandt and Serge Gutwirth eds., 2008).

70. *See* Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation, WP 29, U.N. Doc. 17/EN WP251rev.01, 1, 20 (Feb. 6, 2018): for instance, "[t]he controller cannot avoid the Article 22 provisions by fabricating human involvement." *See*, e.g., *Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR*, PRIVACY INT'L (2017), *available at* https://goo.gl/2X1isy.

71. See *Data is power*, *supra* note 71. The WP29 clarifies that "significant" decisions include those which nudge the individual thanks to behavioral tricks and incentives.

72. As confirmed in Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP29, U.N. Doc. 17/EN WP251rev.01 (Oct. 3, 2017), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053. In 2013, the Article 29 Working Party recommended the inclusion of "collection of data for the purpose of profiling and the creation of profiles as such" under the scope of art. 22. In line with a dynamic interpretation of data protection, the WP29 attempted to anticipate the operability of the GDPR.

73. Dimitra Kamarinou, Christopher Millard, & Jatinder Singh, *Machine Learning with Personal Data*, *in* DATA PROTECTION AND PRIVACY: THE AGE OF INTELLIGENT MACHINES, 89-114 (Ronald Leenes et al., 2017). If the decision is based on "special" categories of data (i.e. sensitive data), automated

It is worth emphasizing that, under Art. 22(3),[74] "the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision" is also established.[75] Since rights of subject access and rectification are similar to those in the DPD,[76] much of the attention given by scholars and commentators has been primarily focused on how to interpret and apply this provision. To provide but an example, in a machine learning or AI context,

> it is not clear who this 'human' should be and whether he / she will be able to review a process that may have been based on third party algorithms, pre-learned models or data sets including other individuals' personal data or on opaque machine learning models. Nor is it clear whether the human tasked with reviewing the decision could be the same person who made the decision in the first place, still potentially subject to the same conscious or subconscious biases and prejudices in respect of the data subject as before.[77]

In addition, explanation may not be feasible in situations where decisions are taken in response to data in real time or change accounting to "trees" involving the data subject's intervention. The question arises of how workers, "who have differing levels of comprehension and may find it challenging to understand the complex techniques,"[78] could access, understand and challenge the information requested.

When it comes to designing a sustainable environment for data protection in times of AI, the GDPR may *already* be obsolete. Sandra Wacther has leveled well-founded criticism at the GDPR, "focus[ing] too much on the input stage, meaning when data is collected, but not enough on how it is assessed." Once the data is lawfully obtained, very little control or understanding is reserved to inferential analytics, which remains a "no man's land."[79] Its key provisions could be circumvented simply by twisting the interpretation of the relevant exceptions, on the other, inferential analytics, one of the strongest AI applications aimed at deducing conducts by simply

decision-making processes are only allowed on the basis of explicit consent or substantial public interest. *See* Michael Veale & Lilian Edwards, *Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling*, 34 COMPUTER L. & SEC. REV. 398 (2018).

74. Lokke Moerel & Marijn Storm, *Law and Autonomous Systems Series: Automated Decisions Based on Profiling - Information, Explanation or Justification? That is the Question!*, OXFORD BUS. L. BLOG (April 27, 2018), https://www.law.ox.ac.uk/business-law-blog/blog/2018/04/law-and-autonomous-systems-series-automated-decisions-based-profiling.

75. On right to explanation, see Bryce Goodman & Seth Flaxman, *European Union regulations on algorithmic decision-making and a "right to explanation"*, 38 AI MAG. 50 (2016).

76. Art. 13.

77. Viktor Mayer-Schönberger & Yann Padova, *Regime Change? Enabling Big Data through Europe's New Data Protection Regulation*, 17 COLUM. SCI. & TECH. L. REV. 315 (2016)

78. WP 29.

79. *See* Sandra Wachter, Brent Mittelstadt and Chris Russell, *Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR*, 31 HARV. J. L. & TECH. (2018).

extrapolating patterns and recurrences from large amounts of data, seem largely unregulated. Moreover, a too narrow conceptualization of data may prevent the GDPR from fulfilling its protective goals. In addition, the mere focus on profiling may fail to grasp new market practices and face new challenges posed by AI and algorithms, as protection concerning inferences made through data is very limited.

IV. "YOU'LL NEVER WORK ALONE," INDIVIDUAL AND COLLECTIVE LIMITS TO THE MONITORING POWER: NATIONAL CASES

Employment law has been conceived as a set of rules aimed at rationalizing the managerial prerogative, including surveillance authority, since its emergence.[80] The employment relationship is an "organizational platform" aimed at reconciling conflicting interests, capable of adapting to the constantly changing nature of socioeconomic landscapes. On closer inspection, the issue of "humanizing" the bureaucratic and economical power of employers by means of mandatory provisions or collectively taken countermeasures, in an attempt to safeguard human dignity, is a defining feature of labor law in various legal systems all over Europe.[81]

Despite variation between legal traditions, the fact that one party, namely the employer, is entitled to exercise power over the other party, the employee, is at the core of the concept of subordination. Such exercise of powers is regulated differently from country to country, but it can go as far as to modify the content of the employee's obligations, to give orders and instructions on how the working obligation shall be fulfilled and to sanction the employee when such orders have not been punctually respected. The paradigm of *power*, as complex as it is, ultimately represents the rationale behind the regulation of the employment relationship; the need for a heteronomous intervention to restore a balance between the parties. This is not only to protect the employee from being subject to who fully controls the organization in which the employee is supposed to perform, but also to acknowledge and therefore legitimize such authority as long as it is exercised within the limits of the law.[82]

Among the powers the employer can exercise, we focus on the monitoring of the employee's working activity. The perspectives under

80. SIMON DEAKIN & FRANK WILKINSON, THE LAW OF THE LABOUR MARKET: INDUSTRIALIZATION, EMPLOYMENT, AND LEGAL EVOLUTION (2005); Simon Deakin S., *The comparative evolution of the employment relationship*, *in* BOUNDARIES AND FRONTIERS OF LABOUR LAW (Guy Davidov & Brian Langille eds., 2006)

81. Antonio Aloisi & Valerio De Stefano, *Regulation, flexibility and the future of work. The case for the employment relationship as innovation facilitator*, INT'L LAB. REV. (forthcoming).

82. *See* Adriana Topo & Orsola Razzolini, *The Boundaries of the Employer's Power to Control Employees in the ICTs Age*, 39 COMP. LAB. L. & POL'Y J. 389 (2017).

which such a prerogative is regulated can be very diverse. In order to provide an assessment by adopting a "civil law" perspective, we selected three national cases: France, Germany, and Italy. We do not expect this selection to describe and comprehend all possible shades in the regulation of the monitoring power in civil law systems. The goal is, instead, to provide the reader with some significant examples that might help us understand how the existing legal framework copes with surveillance and technology and what open issues might remain.

A. France

French labor scholars argue that, when it comes to "*surveillance*" and "*contrôle des salaries*,"[83] new technologies represent a true gamechanger, contributing to a decisive shift away from a direct and physical control by the employer or by middle management to a model based on various data collected through remote scrutiny.[84] Several provisions of the French Labor Code (LC) and of the Law "Technologies and Freedoms,"[85] the case law and the GDPR define a framework for conditions and restrictions on the use of technologies at the workplace.

It is legitimate for an employer to surveil employees' performance. The employer can vet employees with a view to assess their skills, interests, and competences in case of possible recruitment. Concomitantly, employers are responsible for compliance with health and safety measures, and liable for any tort committed at work by any employee under their direction. Art. L. 1121-1 of the LC provides that "no one shall limit the rights of the individual, or individual or collective freedoms, unless the limitations are justified by the task to be performed and are in proportion to the goal towards which they are aimed." The protection of the employee's personal life represents another limit to managerial authority: controls have to be carried out without prejudice to the human dignity of the employees.[86] French workers have a fundamental right to private life, encompassing the right to respect for privacy, as well as for public, political and collective activities. The Court of Cassation stated that that "the employee has the right, even at the time and place of work, to respect for her privacy, which implies in particular the

83. JEAN PELISSIER, GILLES AUZERO AND EMMANUEL DOCKES, DROIT DU TRAVAIL 637 (2012).

84. Bernard Bossu & Alexandre Barège, *Preuve et surveillance des salariés: regard français*, 54 LES CAHIERS DE DROIT 277 (2013).

85. Catherine Delbar, Marinette Mormont, & Marie Schots, New technology and respect for privacy at the workplace, *Institut des Sciences du Travail* (2003).

86. Gérard Lyon-Caen, *Les libertés publiques et l'emploi: rapport pour le ministre du Travail, de l'Emploi et de la Formation professionnelle*, 981 LA DOCUMENTATION FRANÇAISE (1992).

confidentiality of communication."[87] If the employer fails to comply, not only can she not use the evidence gathered, she may also face criminal conviction or administrative sanction by the "*Commission Nationale Informatiques et Libertés*" (CNIL). In particular, no system of surveillance or data collection may be installed without prior notice being given to employees and to employees' representatives.[88]

Three principles govern computer surveillance and collection of data on employees in the French Civil Code: the principles of transparency or loyalty; proportionality; and relevance. This means that employees must be informed about surveillance devices prior to installation. Any restrictions placed upon employees must be justified, proportionate to the aim pursued and relevant, namely, for the purpose of evaluating their professional abilities. Case law has developed a jurisprudential limit to the power of surveillance. First and foremost, one of the restrictions resides in the principle of loyalty—which is embedded in the employment relationship[89]—towards the workforce in the implementation of the system controlling their activity. In this respect, the principle is established that it is not permissible to trap the opponent.

There are two main ways of monitoring the employee. A "direct" control of action that is visible to the eye of management is admitted and licit.[90] However, if the employer wishes to install a specific surveillance device, a mandatory conciliation procedure laid down in Art. L. 1121-1 must be followed based on duplicated information, to both the individual[91] and the collective workforce. A number of formalities must be complied with prior to implementing any monitoring of employee emails. Amongst other things, the employee representatives (works council and health and safety committee) must be consulted before implementing any system that monitors employees' activities, and employees must be informed thereof.

Workers' representatives on the works council must be informed and consulted about the means or techniques governing control of the activity of employees before the decision to implement (Art. L. 2312-38 LC, Art. L. 2328-1 LC).[92] The "*Comité social et économique*" has to be informed about new techniques or automated systems of personnel management allowing for the control of employees' activities before their introduction and

87. Cour de Cassation, Chambre Sociale [Labor Division of the supreme court] October 2, 2001, No. 99-42.942 (Fr.). *See* Marie Morin and Francis Kessler, *Labor impact of technological devices in France*, 2 IUSLABOR 19-34 (2018).

88. CODE DU TRAVAIL [C. TRAV.], art. L. 1222-4 (Fr.). *See* Christophe Vigneau, *Information Technology and Workers' Privacy: The French Law*, 23 COMP. LAB. L. & POL'Y J. 351 (2002).

89. Bernard Bossu & Alexandre Barège, *Preuve et surveillance des salariés: regard français*, 54 LES CAHIERS DE DROIT 277, 279 (2013). Soc. 23 May 21012, J.C.P. S. 2012.1371

90. Soc. 26 April 2006, J.C.P. S. 2006. 1444, note Corrigna-Carsin. Soc. 26 Nov. 2002, Dr. soc. 2003.225, note Savatier.

91. CODE DU TRAVAIL [C. TRAV.], art. L. 1222-4.

92. CODE DU TRAVAIL [C. TRAV.], art. L. 2321-38.

implementation, as well as their modification, on penalty of inadmissibility of the collected evidence.[93] More generally, the employer is duty-bound to consult the works council over any introduction of new technology within the company if this might affect employees' working conditions, employment, pay, training, and qualifications.[94]

In addition, employees must be informed personally.[95] According to Art. L. 1224-4 LC, no information concerning an employee personally can be collected by a device that has not been previously disclosed to her. As established by the plenary session of the Court of Cassation, in accordance with Art. 6(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms (right to a fair trial), the employer cannot record a phone conversation, without the knowledge or consent of those involved. As a consequence, by interpreting Art. 9 of the Code of civil procedure in conjunction with Art. 6(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms and the principle of loyalty, evidence obtained without the knowledge or consent of those involved is illicit. If the process does not respect the duty of information, it is unlawful[96] and the evidence cannot be retained.

Tools performing or allowing personal data processing are no longer to be "declared" to the CNIL. Before 2018, According to Law 6 January 1978, amended by Law 6 August 2004, a simplified or normal declaration, or even a prior authorization scheme had to be carried out. In case of failure to comply with these provisions regulating surveillance, the employee could refuse to be monitored by devices. Today, instead, a compliance and self-control system apply.[97] The CNIL operates a compliance control *a posteriori*.[98]

B. Germany

In Germany, if employers wish to monitor the working activities and the conduct of their employees, a number of restrictions must be observed. In addition to data protection requirements and the participation rights of the works council, the protection of the general right of personality is an

93. CODE DU TRAVAIL [C. TRAV.], art. L. 2312-38. *See also* Cour de cassation [Cass.] [supreme court for judicial matters], June 7, 2006, No. 04- 43, 866.

94. Christophe Vigneau, *Information Technology and Workers' Privacy: The French Law*, 23 COMP. LAB. L. & POL'Y J. 351 (2002).

95. CODE DU TRAVAIL [C. TRAV.], art. 1222-4.

96. Evidence collected without informing employees is illicit, even when the employee could not be unaware of the presence of CCTV. See Cass. soc., 10 January 2012, No. 10-23 482.

97. Loi 2018-493 du 20 juin 2018 relative à la protection des données personnelles, [J.O.], June 21, 2018.

98. Arnaud De Senga, *Information, consultation et déclaration préalables obligatoires portant sur les mécanismes de contrôle de l'activité des salaries,* 699 *Droit ouvrier* 47 (2006). *See also* Hubert Boucher, *La cybersurveillance sur les lieux de travail,* Commission nationale de l'informatique et des libertés (2002).

important limit to be taken into account when it comes to answering the question of which surveillance measures are permitted and which are prohibited.

In the context of an employment relationship (as in any relationship under the law of obligations), each party is obliged to take account of the rights, legal interests and other interests of the counterparty (Section 214 (2) German Civil Code – BGB). These rights also include the general right of personality shaped by case law on the grounds of both a constitutional and a civil right of personality. In particular, the Federal Constitutional Court (BVerfG)[99] stated that the general right of personality is an expression of Art. 1 (1) German Constitution (GG) in conjunction with Art. 2 (1) GG. Art. 1 (1) GG protects human dignity (that shall be "inviolable"); art. 2 (1) GG. protects the right to the free development of personality. The objective scope of protection of the right of personality aims to defend against impairment of the narrower personal sphere of life, self-determination, and the basic conditions of personality development.[100] The BVerfG emphasizes the openness of the general right of personality to development, which is why a conclusive definition of the general right of personality has deliberately not yet been provided.[101] This makes it possible to adapt its scope of protection to current developments, such as the potential dangers of modern ICT and AI.[102]

For the comprehensive protection of the personality, the BVerfG has further specified the general right of personality and developed a fundamental right to guarantee the confidentiality and integrity of information technology systems.[103] This applies, for example, to not only the use of PCs, laptops,

99. Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Jan. 16, 1957, 1 BvR 253/56 (so-called Elfes-decision), 6 ENTSCHEIDUNGEN DER AMTLICHEN SAMMLUNG (hereinafter BVERFGE) 32, margin 15; *see also* Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] June 5, 1973, 1 BvR 536/72, NEUE JURISTISCHE WOCHENSCHRIFT 1226, 1973); Heinrich Lang, *GG, Article 2, margin 33, in* BECKOK GRUNDGESETZ (Volker Epping & Christian Hillgruber eds., 39th ed. 1999).

100. Udo Di Fabio, *GG, Article 2, margin 14,, in* GRUNDGESETZ-KOMMENTAR (Theodor Maunz & Gunter Dürig eds. 2018, 84th supplement August 2018).

101. For example, Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] June 3, 1980 1 BvR 185/77, 54 BVERFGE, ENTSCHEIDUNGEN DES BUNDESVERWALTUNGSGERICHTS 148, 153; Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] May 13, 1986 BvR 1542/84, 72 BVERFGE 155, 170; Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Jan. 31, 1989, 1 BvL 17/87, 79 BVERFGE, ENTSCHEIDUNGEN DES BUNDESVERWALTUNGSGERICHTS 256, 268; Udo Di Fabio, *GG, Article 2, margin 147, in* GRUNDGESETZ-KOMMENTAR (Theodor Maunz & Günter Dürig eds. 2018, 84th supplement August 2018).

102. Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Dec. 15, 1983, 1 BvR 209/83 and others, 65 BVERFGE, ENTSCHEIDUNGEN DES BUNDESVERWALTUNGSGERICHTS 1 et seqq.; Udo Di Fabio, *GG, Article 2, margin 147, in* GRUNDGESETZ-KOMMENTAR (Theodor Maunz & Gunter Dürig eds. 2018).

103. Ingrid Schmidt, *GG, Article 2, margin 43, in* ERFURTER KOMMENTAR ZUM ARBEITSRECHT (2019); *see also* Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Apr. 20, 2016, 1 BvR 966/09, 1 BvR 1140/09, NEUE JURISTISCHE WOCHENSCHRIFT 1781, margin 103, 2016 (Ger.).

mobile phones, navigation devices, but also voice telephony or e-mail.[104] Protection is afforded so that the data generated, processed, and stored by such a system remain confidential or are not secretly accessed or even manipulated.[105] Secret surveillance measures are limited to the protection of sufficiently important legal interests, where their endangerment is concretely foreseeable. In addition, the principle of proportionality calls for special safeguards to ensure transparency, individual legal protection, and prudent supervision.[106]

A large part of these requirements has been substantiated by data protection law. The permissibility of monitoring the work and conduct of the employee is governed by the Federal Data Protection Act (BDSG), insofar as personal data (as defined in Art. 4 No. 1 GDPR) are processed. Before 23 May 2018, the BDSG already contained specific rules for the handling of employee data. This legal situation continues after the fundamental revision of Section 26 BDSG, which came into force on 25 May 2018, with some modifications.[107] Section 26 provides for several reasons of justification for employee data processing.

Section 26 (2) BDSG lays down requirements for the employee's consent to the processing of personal data. The provision is linked to the definition of consent in Art. 4 No. 11 and Art. 7 GDPR. Section 26 (2) BDSG stipulates that, when assessing whether consent can be the legal basis for data processing, the assessment of the voluntary nature of the consent must be taken into account. In particular, the question of dependence of the person employed in the employment relationship, as well as the circumstances under which the consent was granted, have to be taken into account. Voluntariness may exist in particular if a legal or economic advantage is obtained for the employee or if the employer and the employee pursue similar interests.[108] Even though, in individual cases under the old law, case law assumed that the prerequisites under the old law existed,[109] is must be noted that Section

104. Ingrid Schmidt, *GG, Article 2, margin 43, in* ERFURTER KOMMENTAR ZUM ARBEITSRECHT (2019).

105. Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Feb. 27, 2008 1 BvR 370/07, 1 BvR 595/07, NEUE JURISTISCHE WOCHENSCHRIFT 822, 2008 (Ger.).

106. Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Apr. 20, 2016, 1 BvR 966/09, 1 BvR 1140/09, NEUE JURISTISCHE WOCHENSCHRIFT 1781, margin 103 et seqq., 2016 (Ger.).

107. Martin Franzen, *§ 26 BDSG, margin 2, in* ERFURTER KOMMENTAR ZUM ARBEITSRECHT (19th ed.) (2019); Peter Gola, *Der 'neue' Beschäftigtendatenschutz nach § 26 BDSG n. F.*, BETRIEBSBERATER 1462 (2017); Michael Kort, *Der Beschäftigtendatenschutz gem. § 26 BDSG-neu, Ist die Ausfüllung der Öffnungsklausel des Article 88 DS-GVO geglückt?*, ZEITSCHRIFT FÜR DATENSCHUTZ 319 (2017); Michael Kort, *Neuer Beschäftigtendatenschutz und Industrie 4.0, Grenzen einer „Rundumüberwachung" angesichts der Rechtsprechung, der DSGVO und des BDSG nF*, RECHT DER ARBEIT 24, 25 (2018).

108. Martin Franzen, *Datenschutz-Grundverordnung und Arbeitsrecht*, EUROPÄISCHE ZEITSCHRIFT FÜR ARBEITSRECHT 323 et seq (2017).

109. For example, in Bundesarbeitsgericht [BAG] [Federal Labor Court] Oct. 20, 2016, 2 AZR 395/15, NEUE ZEITSCHRIFT FÜR ARBEITSRECHT 443, margin 31, 2017 on the admissibility of CCTV surveillance to clarify the causes of stock shortages, the BAG considered the consent of two warehouse

26 (2) BDSG is based on the assumption that—as a rule of thumb—there will be no effective, voluntarily given consent in the employment relationship.[110] Even if a legal or economic advantage is achieved for the employee, or if the employer and the employee pursue similar interests, the law does not provide that voluntary consent is given, but only that it *may* be given.

Pursuant to Section 26 (1) sentence 1 BDSG, the personal data of employees may be processed for the purposes of the employment relationship if this is necessary: for the decision on the establishment of an employment relationship, or after the establishment of the employment relationship; for its execution or termination or for the exercise or fulfilment of the rights and obligations of the representation of the interests of the employees, resulting from a law or a collective bargaining agreement (*Tarifvertrag*), a works agreement (*Betriebsvereinbarung*) or a service agreement (*Dienstvereinbarung*).[111]

The term "necessary" must not be understood too narrowly.[112] There are hardly any personal data whose collection and processing are "necessary" in the sense of compelling necessity for the establishment, performance, or termination of an employment relationship.[113] The concept of necessity is not interpreted in the sense of an "absolute" necessity, but in the sense of a requirement to apply the principle of proportionality, balancing the employer's interests in data processing against those of the employee concerned.[114] If the prerequisites for proportionate data handling do not exist in the individual case, it is inadmissible. However, it should be mentioned that it does not necessarily follow from the violations that findings or

keepers to be effective; Karl Riesenhuber, *BDSG, § 26, margin 47, in* BECKOK/DATENSCHUTZRECHT (Heinrich A. Wolff & Stefan Brink eds., 2018); *see also* Frank Maschmann, *§ 26 Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses margin 62, in* DATENSCHUTZ-GRUNDVERORDNUNG, BUNDESDATENSCHUTZGESETZ: DS-GVO/BDSG (Kühling & Buchner eds., 2nd ed. 2018), with reference to Article 8 CFR.

110. Lena Rudkowski, *Predictive policing am Arbeitsplatz*, NEUE ZEITSCHRIFT FÜR ARBEITSRECHT, 72, 73 (2019); see Karl Riesenhuber, *BDSG, § 26, margin 43.1, in* BECKOK/DATENSCHUTZRECHT (Heinrich A. Wolff & Stefan Brink eds., 2018).

111. Parties to *Tarifverträge* are trade unions, individual employers, and employers' associations. In simple terms, *Betriebsvereinbarungen* are concluded between works councils (representatives elected by the employees of an establishment) and the employer. *Dienstvereinbarungen* are agreements comparable to *Betriebsvereinbarungen* in the public employment law.

112. Martin Franzen, *§ 26 BDSG, margin 9, in* ERFURTER KOMMENTAR ZUM ARBEITSRECHT (19th ed. 2019).

113. Michael Kort, *Der Beschäftigtendatenschutz gem. § 26 BDSG-neu, Ist die Ausfüllung der Öffnungsklausel des Article 88 DS-GVO geglückt?*, ZEITSCHRIFT FÜR DATENSCHUTZ 319, 320 (2017).

114. Bundesarbeitsgericht [BAG] [Federal Labor Court] Nov. 17, 2016, 2 AZR 730/15, NEUE ZEITSCHRIFT FÜR ARBEITSRECHT 394, 2017 (Ger.); Michael Kort, *Der Beschäftigtendatenschutz gem. § 26 BDSG-neu, Ist die Ausfüllung der Öffnungsklausel des Article 88 DS-GVO geglückt?*, ZEITSCHRIFT FÜR DATENSCHUTZ 319, 320 (2017); Achim Seifert, GDPR, *Article 88, margin 57, in* DATENSCHUTZRECHT (Simitis/Hornung/Spiecker gen. Döhmann eds., 1st ed. 2019).

evidence gained in this way cannot be taken into account in labor court proceedings.[115]

Section 26 (4) sentence 1 BDSG expressly permits the processing of employee data on the basis of "collective agreements,"[116] including works agreements,[117] as Art. 88 (1) GDPR and recital 155 GDPR clarify.[118] This means that under data protection law a works agreement can create not only employee rights that are relevant under data protection law, but also employee obligations that are relevant under data protection law.[119] However, although a works agreement can justify data processing within the framework of the BDSG, it cannot justify a violation of the fundamental general right of personality, since employers and works councils are not completely free to regulate data protection issues. Section 26 (4) sentence 2 BDSG makes it clear that the contracting parties of the collective agreement must comply with the provisions of Art. 88 (2) GDPR.[120] Furthermore, according to Section 75 (2) sentence 1 BetrVG, the employer and the works council have to protect and promote the free development of the personality of the employees of the enterprise. Section 75 (2) sentence 1 BetrVG contains a prohibition of "excessive measures" under works constitution law, which is intended to prevent unlawful violations of the general right of personality.[121] Interference with the right of personality must be justified by

115. Bundesarbeitsgericht [BAG] [Federal Labor Court] Oct. 20, 2016, 2 AZR 395/15, ZEITSCHRIFT FÜR DATENSCHUTZ 339, margin 17, 2017; Bundesarbeitsgericht [BAG] [Federal Labor Court] Jul. 27, 2017, 2 AZR 681/16, NEUE ZEITSCHRIFT FÜR ARBEITSRECHT 1327, margin 17, 2017 (Ger.); *see* Michael Kort, *Neuer Beschäftigtendatenschutz und Industrie 4.0, Grenzen einer "Rundumüberwachung" angesichts der Rechtsprechung, der DSGVO und des BDSG nF*, RECHT DER ARBEIT 33 (2018); Martin Franzen, *§ 26 BDSG, margin 47, in* ERFURTER KOMMENTAR ZUM ARBEITSRECHT (19th ed. 2019).

116. *Cf.* Bundesarbeitsgericht [BAG] [Federal Labor Court] June 25, 2002, 9 AZR 405/00, NEUE ZEITSCHRIFT FÜR ARBEITSRECHT 275, 2003; Bundesarbeitsgericht [BAG] [Federal Labor Court] Jul. 9, 2013, 1 ABR 2/13 (A), NEUE ZEITSCHRIFT FÜR ARBEITSRECHT 1433, margin 31, 2013; Bundesarbeitsgericht [BAG] [Federal Labor Court] Sept. 25, 2013, 10 AZR 270/12, NEUE ZEITSCHRIFT FÜR ARBEITSRECHT 41, margin 32, 2014 (Ger.); Martin Franzen, *§ 26 BDSG, margin 47, in* ERFURTER KOMMENTAR ZUM ARBEITSRECHT (19th ed. 2019); *see also* Tim Wybitul, *Neue Spielregeln bei Betriebsvereinbarungen und Datenschutz, BAG schafft Klarheit zu Anforderungen an Umgang mit Arbeitnehmerdaten*, NEUE ZEITSCHRIFT FÜR ARBEITSRECHT 225, 228 et seqq. (2014).

117. Only very few collective bargaining agreements regulate issues of employee data protection, cf. Martin Franzen, *§ 26 BDSG, margin 47, in* ERFURTER KOMMENTAR ZUM ARBEITSRECHT (19th ed.) (2019); Achim Seifert, GDPR, *Article 88, margin 30, in* DATENSCHUTZRECHT (Simitis/Hornung/Spiecker gen. Döhmann eds., 2019).

118. Martin Franzen, *§ 26 BDSG, margin 47, in* ERFURTER KOMMENTAR ZUM ARBEITSRECHT (19th ed.) (2019); Achim Seifert, GDPR, *Article 88, margin 26, in* DATENSCHUTZRECHT (Simitis/Hornung/Spiecker gen. Döhmann eds., 2019).

119. Michael Kort, *Neuer Beschäftigtendatenschutz und Industrie 4.0, Grenzen einer "Rundumüberwachung" angesichts der Rechtsprechung, der DSGVO und des BDSG nF*, RECHT DER ARBEIT 33 (2018).

120. Frank Maschmann, *§ 26 Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses margin 82, in* DATENSCHUTZ-GRUNDVERORDNUNG, BUNDESDATENSCHUTZGESETZ: DS-GVO/BDSG (Kühling & Buchner eds., 2nd ed. 2018).

121. Bundesarbeitsgericht [BAG] [Federal Labor Court] Aug. 26, 2008, 1 ABR 16/07, NEUE ZEITSCHRIFT FÜR ARBEITSRECHT 1187, 2008 (Ger.); Thomas Kania, *§ 75 BetrVG, margin 9, in* ERFURTER

the legitimate interests of the employer, other holders of fundamental rights or other important objectives.[122]

C. Italy

Title I of the Workers' Statute (Law No. 300 of 1970), entitled "On freedom and dignity of the worker," for the first time, regulated monitoring power of the employer.[123] In its original wording, Art. 4 of the Workers' Statute regulated remote controls, with the aim of protecting the dignity and confidentiality of the worker in the workplace, against the possibility of the employer putting in place any subtle control, potentially damaging to the person of the worker.[124] The provision prohibited the use of audiovisual and other equipment for the remote control of workers' activities (Section 1). Only in the case of organizational and production needs, or occupational safety requirements, could equipment offering the possibility of remote control of the workers' activities be installed, subject to prior agreement with the company's trade union representatives or subject to administrative authorization (Section 2).

Direct monitoring of work activities carried out remotely by means of installed devices was therefore always and without exception prohibited. On the other hand, controls—defined as "preter-intentional"[125]—aimed at pursuing different goals than the control of the working activity, were allowed under the condition that a specific collective agreement had been stipulated or an administrative authorization obtained.

Interestingly enough, the statutory provision limited itself to regulating the profile of the installation of the surveillance instruments, while it remained silent on the possibility of using—even in the presence of legitimately installed systems—the information gathered for disciplinary purposes. The tension between the regulatory vacuum regarding the usability of the data and the need to respond to the demands of the employer in the face of serious misconduct by the worker had prompted case law to forge the

KOMMENTAR ZUM ARBEITSRECHT (19th ed. 2019); KARL FITTING ET AL., BETRVG § 75, MARGIN 136 (2018).

122. As pointed out above, encroachments in the intimate sphere are forbbien, see also Frank Maschmann, *§ 26 Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses margin 84, in* DATENSCHUTZ-GRUNDVERORDNUNG, BUNDESDATENSCHUTZGESETZ: DS-GVO/BDSG (Kühling & Buchner eds., 2nd ed. 2018).

123. ALESSANDRO BELLAVISTA, IL CONTROLLO SUI LAVORATORI 102 (1995); Pietro Lambertucci, *La disciplina dei «controlli a distanza»*, GIUR. IT., 737 (2016); Matteo Dell'Olio, *Art. 4 Stat. lav. ed elaboratori elettronici*, DIR. LAV., 487 (1986); MARIAPAOLA AIMO, PRIVACY, LIBERTÀ DI ESPRESSIONE E RAPPORTO DI LAVORO 122 (2003).

124. Luigi Mengoni, *Le modificazioni del rapporto di lavoro alla luce dello Statuto dei lavoratori*, *in* L'APPLICAZIONE DELLO STATUTO DEI LAVORATORI (1973); BRUNO VENEZIANI, I CONTROLLI DELL'IMPRENDITORE E IL CONTRATTO DI LAVORO (1975).

125. Umberto Romagnoli, *Sub Art. 4*, *in* STATUTO DEI DIRITTI DEI LAVORATORI 29 (Giorgio Ghezzi et al. eds., 1979)

category of so-called *defensive controls*,[126] *alias* "controls aimed at ascertaining a conduct outside the employment relationship that is illicit or harmful to the company's assets and image and not aimed at ascertaining the breach of ordinary contractual obligations," excluded from the scope of application of Art. 4.[127] Conversely, controls aimed at ascertaining unlawful conduct that could be classified as a violation of contractual obligations were included among those controls to be conducted in compliance with the guarantees pursuant to Art. 4, paragraph 2.[128]

Case law on defensive controls was indeed controversial.[129] First, it imposed a new and complex distinction between controls aimed at ascertaining illicit acts completely unrelated to the employment relationship (legitimate) and controls aimed at ascertaining illicit acts internal to the employment relationship (forbidden).[130] Second, it took into account a good deal of change in the position of the judges, who often modulated their arguments according to the specific case, which did not guarantee a reasonable degree of certainty in such a complex matter. It was clear that the statute was in need of a thorough reassessment.[131]

Art. 23, par. 1, of Legislative Decree No. 151/2015 has completely replaced Art. 4 of the Workers' Statute. With regard to the installation of remote control instruments, the first paragraph of the provision provides that audiovisual equipment and other instruments—from which even the possibility of remote control of the activities of workers derives—can be used exclusively for organizational and production needs, for occupational safety and for the protection of the company's assets, and can be installed under the condition that a collective agreement has been signed or prior administrative authorization reached. The second paragraph excludes from the scope of the first paragraph the tools used to perform the working activity and to record the access and presence of the worker on the premises of the company. In order to use these tools for monitoring purposes, the employer is not bound by the conditions set forth in the first paragraph. Finally, the third paragraph provides for the usability of the data collected through instruments legitimately installed for all purposes related to the employment relationship,

126. Ilario Alvino, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*, 2 LAB. & L. ISSUES 1 (2016).

127. Cass. 23 Febbraio 2012, n. 2722, 2 RIV. IT. DIR. LAV. 113 (2013); Cass. 5 Ottobre 2016, n. 19922, MASS. GIUR. LAV. 37 (2017); Cass. 1 Ottobre 2012, n. 16622, LAV. GIUR. 383 (2013); Cass. 12 Ottobre 2015, n. 20440, 2 RIV. IT. DIR. LAV 249 (2016).

128. Cass. 19 Settembre 2016, n. 18302, GIUR. IT. 321 (2017); Trib. Napoli 29 Settembre 2010, 2 RIV. IT. DIR. LAV. 31 (2011).

129. For an overview, see Roberto Romei & Silvana Sciarra, The *Protection of Employees Privacy: a Survey on Italian Legislation and Case Law*, 17 COMP. LAB. L. & POL'Y J. 91, 96 (1995).

130. Ilario Alvino, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*, 2 LAB. & L. ISSUES 14 (2016).

131. Maria Teresa Carinci, *Il controllo a distanza dell'attività dei lavoratori dopo il "Jobs Act" (art. 23 D. lgs. 151/2015): spunti per un dibattito*, 2 LAB. & L. ISSUES 5 (2016).

provided that the worker is given adequate information on the methods of use of the instruments and the implementation of controls and in compliance with the provisions of Legislative Decree No. 196 of 30 June 2003 (so-called Privacy Code), which has been amended by Legislative Decree No. 101 of 10 August 2018 in order to integrate the new GDPR.

Needless to say, the new disposition triggered an intense debate among scholars.[132] First of all, it recognizes and regulates two distinct layers: the installation of the control instruments and the logical subsequent level of the usability of the information collected.[133] As for the first, there is a shared opinion that the prohibition of remote controls concerning work activity is intact, as it was prior to the latest reform.[134] However, it cannot be underestimated that paragraph 2 excludes the working tools from the limits set out in the first paragraph, the installation or—more generally—the adoption of which is not subject to any constraint. One of the most controversial issues is precisely the meaning of the expression "working instrument," in view of the plurality of functions that the same instrument can potentially perform. In a working context in which almost all of the working tools can also be used to collect data and to monitor employees, the distinction between "working tools" and "monitoring tools" is rather anachronistic and could allow gross interference in the employees' private sphere.

The second area, concerning the employability of the information collected through the remote-control tools, opens up new scenarios. In 2015 the legislator established the full usability of the data for all purposes related to the employment relationship, with three prerequisites: that paragraphs 1 and 2 of Art. 4 are complied with; that the employee is adequately informed; that the Privacy Code is complied with. Today, the new formulation of Art. 4 fully incorporates the entire Privacy Code through an express textual reference, making it clear that protection of privacy protection is fully guaranteed in the workplace.[135]

132. Alessandro Bellavista, *Il nuovo art. 4 dello Statuto dei* lavoratori, *in* COMMENTARIO BREVE ALLA RIFORMA DEL "JOBS ACT" 717 (Gaetano Zilio Grandi & Marco Biasi eds., 2016); Pietro Lambertucci, *La disciplina dei "controlli a distanza" dopo il Jobs Act: continuità e discontinuità con lo Statuto dei lavoratori*, *in* JOBS ACT: UN PRIMO BILANCIO ATTI DEL XI SEMINARIO DI BERTINORO-BOLOGNA DEL 22-23 OTTOBRE 2015 270 (Franco Carinci ed., 2016).

133. Marco Marazza, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, ARG. DIR. LAV. 487 (2016).

134. Riccardo Del Punta, *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, d.lgs. n. 151/2015)*, 1 RIV. IT. DIR. LAV. 82 (2016); Valerio Maio, *La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica*, ARG. DIR. LAV. 1190 (2015).

135. Alessandro Bellavista, *Dignità e riservatezza del lavoratore*, *in* DIRITTO DEL LAVORO, DIZIONARI DI DIRITTO PRIVATO PROMOSSI DA NATALINO IRTI 152 (Pietro Lambertucci ed., 2010); ANDREA SITZIA, IL DIRITTO ALLA "PRIVATEZZA" NEL RAPPORTO DI LAVORO TRA FONTI COMUNITARIE E NAZIONALI (2013); PATRIZIA TULLINI, TECNOLOGIE DELLA COMUNICAZIONE E RISERVATEZZA NEL RAPPORTO DI LAVORO. USO DEI MEZZI ELETTRONICI, POTERE DI CONTROLLO E TRATTAMENTO DEI DATI

V. "AI WIDE OPEN": SUMMARY AND ASSESSMENT

While AI may embody several benefits for workers "such as augmenting human capabilities and enhancing creativity, advancing inclusion of underrepresented populations, reducing economic, social, gender and other inequalities, and protecting natural environments, thus invigorating inclusive growth, sustainable development and well-being,"[136] it may also endanger lives as it increases authoritative attitudes. Even worse, it is difficult to say how monitoring, tracing, scoring,[137] incentivization through "nudges" and penalties,[138] rankings and all the resulting metrics generated by tech tools can be manipulated and repurposed to infer unspecified characteristics or to predict unknown behaviors.[139] Far from being neutral and unprejudiced,[140] such systems may perpetuate bias, promote discrimination, and exacerbate inequality, thus paving the way to social unrest and political turmoil. All in all, the prevailing approach towards new technologies is rather uncritical, and a considerable number of "users" seem ready to accept a renunciation of privacy (or, more in general, of their personal digital footprint) so as not to forego access to a set of services presented as sources of connection, optimization, convenience, and pleasure,[141] including in the "sensitive" context of an employment relationship.

The above analyzed national systems share an effective and adaptable arsenal in facing the challenges that AI poses in terms of interference with the employees' private sphere. In addition to the homogenization effect of the GDPR, there are some common positions. First, the recognition of human dignity as a fundamental right to be protected also within the workplace. Second, the involvement of the collective parties in the regulation or, sometimes, the authorization of technological installations that can be used as surveillance tools. More in general, the profound acknowledgement that the vulnerable position of the employees is even further compromised by the presence and usage of tools that interfere with their personal sphere, that overcome personal boundaries and that can challenge the respect of

PERSONALI (2010); Alessandra Ingrao, *Il controllo disciplinare e la privacy del lavoratore dopo il Jobs Act*, 1 RIV. IT. DIR. LAV. 46 (2017).

136. OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449 (May 12, 2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

137. Danielle Keats Citron & Frank Pasquale, *The scored society: Due process for automated predictions*, 89 WASH. L. REV. 1 (2014).

138. Graham Sewell, *Nice work? Rethinking managerial control in an era of knowledge work*, 12 ORG. 685 (2005).

139. Catherine Tucker, *Privacy, Algorithms, and Artificial Intelligence*, *in* THE ECONOMICS OF ARTIFICIAL INTELLIGENCE: AN AGENDA (Ajay Agrawal, Joshua Gans & Avi Goldfarb eds., 2017)

140. Gideon Mann & Cathy O'Neil, Hiring algorithms are not neutral, 9 HARV. BUS. REV. (2016).

141. Ian Bogost, *Welcome to the Age of Privacy Nihilism*, THE ATLANTIC (Aug. 23, 2018), https://www.theatlantic.com/technology/archive/2018/08/the-age-of-privacy-nihilism-is-here/568198/. For a comprehensive overview, see L. M. Sacasas, *Personal Panopticons*, REAL LIFE MAG (Nov. 5, 2018), https://reallifemag.com/personal-panopticons/.

fundamental limits when it comes to the separation between the private and professional sphere of a person. Furthermore, in all the jurisdictions taken into account, case law plays a relevant role in shaping the developmental interpretation of the law to keep it updated in relation to the latest technological innovations. We might conclude that there are positive indications about the effectiveness of the protection of the employees' dignity and privacy at work.

However, there is no reason to be too optimistic about the future developments of monitoring technologies. For instance, it must be said that, despite its systematic and comprehensive goals, the GDPR reveals a significant weakness in dealing with this sort of data-fueled and automatically-propelled decisions.[142] On the one hand, the GDPR extends protection against decisions based solely on automated processing, to cover not only profiling of data subjects but also any other form of automated processing,[143] on the other, it seems to be conceived on an old-fashioned understanding of how data is used, in turn based on a three-phase system (as classified by Oostveen,[144] acquisition, analysis, and application). Given the pace of change, employers may find themselves being able to make connections that they had not anticipated or disclosed. As noted in a thorough report by the advocacy group "Privacy International," "[t]hrough profiling, highly intimate information, including sensitive information, can be *inferred, derived or predicted* from personal and often non-sensitive data at varying degrees of accuracy. As a result, data about an individual's behavior can be used to generate unknown information about someone's likely identity, attributes, interests, or personality."[145]

Of course, AI can be beneficial in terms of security, productivity and efficiency. At the same time, however, AI might be imperceptible, even to those who are subject to the monitoring and involved in it. The concrete risk is that what was applied so far for traditional monitoring methods and what seems perfectly successful in the books of law, might face serious obstacles in chasing AI technologies that are far from being understood and co-determined by most of workers who rely heavily on digital gadgets.

142. Lilian Mitrou, *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?* (June 3, 2019), *available at SSRN*, https://ssrn.com/abstract=3386914.

143. Lee A. Bygrave, *Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, 17 COMPUTER L. & SEC. REV. 17 (2001)

144. Manon Oostveen, *Identifiability and the applicability of data protection to big* data, 6 INT'L DATA PRIVACY L., 299 (2016).

145. Emphasis added. This is problematic for two reasons. First, any de-identified data can theoretically be reverse engineered and linked back to an individual. Second, even truly anonymized data can be used to build user profiles and thus privacy and discrimination harms still occur, without the need to identify a particular individual. Paul Ohm, *Broken promises of privacy: responding to the surprising failure of anonymization*, 57 UCLA L. REV. 1701 (2009)