DISSERTATIONES
IURIDICAE
UNIVERSITATIS
TARTUENSIS
83

SEILI SUDER

Protection of employee privacy in the digital workplace

DISSERTATIONES IURIDICAE UNIVERSITATIS TARTUENSIS
83

DISSERTATIONES IURIDICAE UNIVERSITATIS TARTUENSIS
83

SEILI SUDER

Protection of employee privacy in the digital workplace

UNIVERSITY OF TARTU
Press
1632

School of Law, University of Tartu, Estonia

The dissertation has been accepted for the commencement of the degree of Doctor of Philosophy (PhD) in law by a resolution of the Council of the School of Law of 27 September 2021.

Supervisors: Prof. Merle Erikson (University of Tartu, School of Law)
Prof. Andra Siibak (University of Tartu, Institute of Social Studies)

Opponent: Assistant Prof. Dr. Marta Otto (Faculty of Law and Administration, University of Lodz, Poland)

The commencement will take place on 6 December 2021 at 11:00 a.m in the School of Law, Näituse 20, room K-03 and via video bridge.

The research leading to this dissertation was supported by the research project 'Conceptualisations and experiences with public and private in technologically saturated society' PUT44, funded by the Estonian Research Council.

Publication of this dissertation is supported by the School of Law, University of Tartu.

ISSN 1406-6394
ISBN 978-9949-03-738-4 (print)
ISBN 978-9949-03-739-1 (pdf)

University of Tartu Press
www.tyk.ee

TABLE OF CONTENTS

LIST OF ORIGINAL PUBLICATIONS

Publication I Suder, S. Pre-Employment Background Checks on Social Networking Sites – May Your Boss Be Watching? – Masaryk University Journal of Law and Technology 2014/8 (1).

Publication II Suder, S., Siibak, A. Employers as Nightmare Readers: An Analysis of Ethical and Legal Concerns Regarding Employer-Employee Practices on SNS – Baltic Journal of Law & Politics 2017/10 (2).

Publication III Suder, S., Erikson, M. Microchipping Employees – Unlawful Monitoring Practice or a New Trend in the Workplace? In Ebers, M.; Cantero Gamito, M. (Eds.). Algorithmic Governance and Governance of Algorithms. Legal and Ethical Challenges. Springer International Publishing. Data Science, Machine Intelligence, and Law 1 2020.

Publication IV Suder, S. Processing employees' personal data during the Covid-19 pandemic. – European Labour Law Journal 2021/12 (3). DOI: 10.1177/2031952520978994.

Publication V Suder, S., Siibak, A. Proportionate response to a COVID-19 threat? Use of apps and other technologies for monitoring employees under the EU data protection framework. – Special issue 'COVID-19 and the world of work'. – International Labour Review 2021.

Author's contribution

The author of the dissertation was the sole author of two of the publications (publications I and IV), she was responsible for legislative discussion in publication II, where the co-author was responsible for the discussion concerning empirical material gathered during qualitative case studies; she was mainly responsible for writing publication III as the co-author corrected and complemented the article and she was mainly responsible for writing publication V and in particular legislative discussions related to applicability, legal bases and principles enacted in the GDPR.

ANALYTICAL COMPENDIUM TO A CUMULATIVE DISSERTATION

1. Introduction

1.1 Digital monitoring technologies at work

Today's workplaces are becoming increasingly digitalized.[1] Digitalization has created many economic and societal benefits and advantages to employers and employees, such as increased flexibility and autonomy, the potential to improve work-life balance, etc., but has also triggered a number of ethical, legal and employment related challenges.[2] One of these challenges is the increasing use of technology to monitor applicants and employees, which is accompanied by intensification of the processing of their personal data and possible intrusions to privacy.[3] Still, employers' quest for knowledge about employees and thus employer surveillance of employees is nothing new. Supervision and monitoring[4] have long been assumed as necessary to ensure managerial goals; for example, to protect an

[1] The concept of the digital workplace originates from 1990s. In recent years, in response to rapid technological developments and as part of wider concerns surrounding the future of work and organizations, the term digital workplace has gained renewed attention. Williams, S. P. and Schubert, P. argue that the digital workplace is being conceived as: an integrated technology platform that provides all the tools and services to enable employees to effectively undertake their work, both alone and with others, regardless of location and is strategically coordinated and managed through digital workplace designs that are agile and capable of being adapted to meet future organizational requirements and technologies. Williams, S. P., Schubert, P. Designs for the Digital Workplace. – Procedia Computer Science 2018/138. See also: Köffer S. Designing the digital workplace of the future – what scholars recommend to practitioners. International Conference on Information Systems 2015.; Marks, A., Briken, K., Chillas, S., Krzywdzinski, M. The New Digial Workplace: How New Technologies Revolutionise Work. Macmillan Publishers Limited 2017.

[2] European Parliament resolution of 21 January 2021 with recommendations to the Commission on the right to disconnect 2019/2181(INL).

[3] See for example: Simits, S. Reconsidering the Premises of labour Law. – European Law Journal 1999/5 (1); Ajunwa, I., Crawford, K., Schultz, J. Limitless worker surveillance. – California Law Review 2017/105 (3); Moore, P., Upchurch, M., Whittaker, X. (Eds.) Humans and Machines at Work. Monitoring, Surveillance and Automation in Contemporary Capitalism. Palgrave Macmillan 2018.

[4] This dissertation uses monitoring as an all-embracing concept that covers all kinds of activities with employee data. However, it is worth noting that some researchers differentiate monitoring from surveillance. They confine monitoring to capturing work-related activities and consider surveillance as more intrusive form of monitoring, as it employs technologies that cover a broader range of information, such as both work- and non-work related activities. See for example, McNall, L. A., Stanton, J. M. Private eyes are watching you: Reactions to location sensing technologies. – Journal of Business and Psychology 2011/26; Sadeghian, P., Abdollahian, F., Hamidi, K. Workplace surveillance: review of surveillance and control of workplace. – Advanced Social Humanities and Mangement 2017/4 (1).

organization's assets and property rights, track performance and optimize processes, ensure occupational safety and compliance with legal requirements and prevent criminal or fraudulent activities. However, today, managing employees is becoming data-driven[5] as advances in technology allow for constant electronic monitoring and data gathering. New applications and smart devices enable employers to collect enormous quantities of employees' personal data from a vast array of sources, all of which can be done within a reasonable time and by inexpensive means.[6]

In the employment context, data collection can be done in a variety of ways[7], such as through interviews, games, digitized tests, internet searches, e-mail monitoring, phone tapping, tracking computer content and usage times, video monitoring, global positioning system (GPS)[8] tracking, and biometric[9] monitoring. Employers with an interest in monitoring employees may use different digital monitoring technologies, such as wearable technology (bracelets, wristbands, high-tech caps, helmets or vests and bionic suits or exoskeletons)[10], or request employees to install applications on devices such as computers or mobile phones[11]. In the context of the present dissertation, 'digital monitoring technologies' is used as a common denominator, covering all possible technologies – both existing and emerging – that leave digital trails that can be collected and mined for insights into how employees work.

Digital monitoring technologies collect different data, such as location information, usage information, vitals data and other information relating to the user,

---

5 Patil D., Mason, H. Data Driven. Creating a Data Culture. O'Reilly Media 2015; There will be little privacy in the Workplace of the Future. – The Economist 28.03.2018.

6 Article 29 Data Protection Working Party. Opinion 2/2017 on data processing at work. 2017 WP 249; Valerio, De S. Negotiating the algorithm. Automation, Artificial Intelligence and Labor Protection. – Comparative Labor Law & Policy Journal 2019/41 (1).

7 Bodie, M. T., Cherry, M. A., McCormic, M. L., Tang, J. The Law and Policy of Big Data and People Analytics, University of Colorado Law Review 2016.; *op cit* Ajunwa, I., Crawford, K., Schultz, J.; *op cit* Moore, P., Upchurch, M., Whittaker, X.

8 GPS is a global navigation satellite system whereby data are transmitted from satellites in space to earth-bound receivers to notify them of their location. GPS can localise and trace goods and people when used in combination with mobile systems such as geography information systems and advanced internet applications. Kanngieser, A. Tracking and tracing: geographies of logistical governance and labouring bodies. – Environment and Planning D: Society and Space 2013/31.

9 Biometric technologies refer to all processes used to recognize, authenticate and identify persons based on physical and/or behavioural characteristics. European Commission. Biometrics technologies: A key enabler for future digital services 2018.

10 See for example: Greenbaum, D. Ethical, Legal and Social Concerns Relating to Exoskeletons. – CM SIGCAS Computers and Society 2015/45 (3); Rogers, A. We Try a New Exoskeleton for Construction Workers. – WIRED 28.04.2015; Ajunwa, I. Algorithms at Work: Productivity Monitoring Applications and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law. – Saint Louis University Law Journal 2018/63 (1).

11 *op cit* Ajunwa, I., Crawford, K., Schultz, J.

so that the data can be used to automatically track employees and measure their speed and efficiency, give insight into the employee's work patterns or indicate medical necessity.[12] These technologies are increasingly ubiquitous and allow for connectivity anytime and anywhere. For example, location-sensing technologies relying on radio frequency identification (RFID)[13] devices can be used to provide always-on-time and real-time location tracking of the whereabouts of employees. With emotion-sensing technologies, employee monitoring can go beyond monitoring productivity to detecting employees' emotions.[14] Sometimes these technologies also allow employers to easily monitor employees' activities outside of work hours or place of work.[15] For example, health and workout apps promoted among employees may lead employers to consider sleep patterns or dietary habits for the purpose of determining employee benefits or compensation.[16]

In addition, as researchers point out, data collected through digital monitoring technologies is often analysed using artificial intelligence (AI)[17], allowing

---

[12] *op cit* Greenbaum, D.; *op cit* Moore, P., Upchurch, M., Whittaker, X.; *op cit* Valerio, De S.

[13] RFID devices are known as a technology for the remote identification. RFID uses tags (or transponders) in a microchip to locate, identify and transmit information on items (or people) carrying the chip. RFID does not require contact or line-of-sight for data capture. The RFID system consists of three components: a chip (which can be implanted into the employee), the reader (which is used to read chip's data without contact) and the backend database (to manage the data from the chip). The role of the reader is to interrogate the chip and retrieve its stored data. To do this the reader broadcasts an electromagnetic signal that any RFID chip within range and operating on the same frequency will respond to. Drawing its power from this signal, the RFID chip will respond with an encrypted signal. The RFID reader will decode this and pass the resulting information to the backend system. The backend system is where data is manipulated and stored, and forms the data resource for the system users. See for example: Gille, D., Wohlgemuth, S., Strüker, J. RFID in Germany in A Structured Collection on Information and Literature on Technological and Usability Aspects of Radio Frequency Identification. Future of Identity in the Information Society 2007; *op cit* Kanngieser, A.; Graveling, R., Winski, T., Dixon, K. The Use of Chip Implants for Workers. European Parliament 2018; MHI. Automatic Identification and Data Collection. – https://www.mhi.org/ fundamentals/automatic-identification (30.07.2021).

[14] Kinni, T. Monitoring Your Employees' Every Emotion. – MITSloan 15.09.2016.; Whelan, E., McDuff, D., Gleasure, R., Brocke, J. How Emotion-Sensing Technology Can Reshape the Workplace. – MITSloan 05.02.2018.

[15] Vatcha, A. Workplace Surveillance Outside the Workplace: An Analysis of E-Monitoring Remote Employees. – iSCHANNEL 2020/15 (1).

[16] Tran, A. H. The Internet of Things and Potential Remedies in Privacy Tort Law. – Columbia Journal of Law and Social Problems 2017/50 (2).

[17] The definition adopted by the European Commission refers to AI, which uses machine learning and deep learning tools to extract information from an enormous number of data and to generate new value based on models built with those data. AI system can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with. European Commission. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts. – COM/2021/206 final. See also: Brynjolfsson, E., Rock, D., Syverson, C. Artificial

employers to monitor employees' activities to an extent unthinkable in the past, as well as to process enormous amount of data about employees.[18] A range of AI-enabled applications enable employers to assign work tasks, predict employees' behaviour and guide day-to-day decision-making in the workplace.[19] This developing field of people analytics involves injecting data mining[20] into human resource management, aiming to use systemic and supposedly scientific data analysis as a tool to guide hiring, promotion, demotion, scheduling, wages, and discharge determinations.[21] Hence, algorithms control various aspect of work, from sorting through job applications[22] to continuous tracking of employees' behaviour to performance evaluations.[23] From the vast quantity of information, and the predictive analysis associated with it, employers are encouraged to gain managerial tools.[24] Thus, algorithmic predictive analysis that is based on large quantities of data and digital monitoring technologies are becoming instrumental in how employment is managed.[25] The drawback, as argued by researchers, is that big data analytics and AI draw on highly diverse and feature-rich data of

intelligence and the modern productivity paradox: A clash of expectations and statistics. Working Paper No. 24001, National Bureau of Economic Research, Cambridge 2017; Organization 2019. – https://www.ilo.org (30.07.2021); Eurofound. Game-changing technologies: Transforming production and employment in Europe. Luxembourg: Publications Office of the European Union 2020.

[18] *op cit* Moore, P., Upchurch, M., Whittaker, X.; *op cit* Valerio, De S.; Prassl, J. What If Your Boss Was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work. – Comparative Labor Law & Policy Journal 2019/41 (1).

[19] Algorithmic Management – A Trade Union Guide. UNI Global Union 2020. – https://www.uniglobalunion.org (30.07.2021).

[20] Data mining is an automated analysis of data, using mathematical algorithms, in order to find new patterns and relations in data. Custers, B. Data Dilemmas in the Information Society: Introduction and Overview. In Custers, B., Calders, T., Schermer, B., Zarsky, T. (Eds.) Discrimination and Privacy in the Information Society. Springer International Publishing 2013.

[21] See for example: *op cit* Custers, B.; *op cit* Bodie, M. T. *et al*.; *op cit* Ajunwa, I., Crawford, K., Schultz, J.; Digitalization and decent work implications for Pacific Island Countries. International Labour Organization 2019. – https://www.ilo.org (30.07.2021); Aloisi, A., Gramano, E. Artificial Intelligence is Watching You at Work: Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context – Comparative Labor Law & Policy Journal 2019/41 (1).

[22] Non-tech businesses are beginning to use artificial intelligence at scale. – The Economist 28.03.2018.; Managing human resources is about to become easier. – The Economist 28.03.2018.

[23] Berg, J., Furrer, M., Harmon, E., Rani, U., Silberman, M. S. Digital labour platforms and the future of work. International Labour Organization 2018. – www.ilo.org (30.07.2021).

[24] Barzilay, A. R. Data Analytics at Work: A View From Israel on Employee Privacy and Equality in the Age of Data-Driven Employment Management. – Comparative Labor Law & Policy Journal 2019/40.

[25] See for example: Adams, A. Technology and the Labour Market: the Assessment. – Oxford Review of Economic Policy 2018/34 (3).

unpredictable value, and create new opportunities for discriminatory, biased, and invasive decision-making.[26]

While digital monitoring technologies can help to ensure compliance with rules on working time, trace employer's assets and enhance workplace safety, they have raised further concerns about poor working conditions, such as increased work intensity and higher levels of stress and anxiety, erosion of the demarcation between work and personal life, reduced work autonomy and diminished trust towards management.[27] According to research, employees who are aware of the monitoring most or all of the time are bound to adjust their behaviour accordingly, suggesting that monitoring violates an individual's autonomy in a way that is often associated with dystopian characteristics.[28] As these technologies enable more intrusive employee monitoring, they raise concerns about the ability of employers to control employees in insidious new ways and further enhance power imbalances between employees and employers.[29] Digital monitoring technologies may also have an effect on the fundamental rights of employees to organize, set up employee meetings and communicate confidentially.[30] If misused, digital monitoring technologies can present a serious threat to employees' freedom of association and potentially weaken employees' negotiating power.[31]

Furthermore, technological advances in monitoring allow employers to utilize information about their employees; oftentimes personal data, raising serious concerns about the lack of employees' privacy in regard to controlling information about themselves and determining how it will be used, and keeping personal facts and feelings to themselves.[32] These possibilities and functions of digital monitoring technologies have highlighted privacy concerns related to workplace monitoring and given both European and national legislators new and ever-evolving sets of issues arising from technological change in the area of employee monitoring. As digital monitoring technologies are in constant

---

[26] Wachter, S., Mittelstadt, B. D. A right to reasonable inferences: Re-thinking data protection law in the age of Big Data and AI. – Columbia Business Law Review 2019/1.; *op cit* Barzilay, A. R.

[27] Sprague, R. Survey of (Mostly Outdated and Often Ineffective) Laws Affecting Work-Related Monitoring: The Piper Lecture. – Chicago-Kent College of Law Review 2018/93; Eurofound. Employee monitoring and surveillance: The challenges of digitalisation. Luxembourg: Publications Office of the European Union 2020.

[28] Torpey, J. Through thick and thin: Surveillance after 9/11. – Contemporary Sociology 2007/36 (2); Ball, K. Workplace surveillance: An overview. – Labour History 2010/51 (1); Zuboff, S. The age of surveillance capitalism: The fight for a human future at the new frontier of power. New York: PublicAffairs 2019.

[29] *op cit* Ajunwa, I., Crawford, K., Schultz, J.; Hirsch, J. M. Future Work. – University of Illinois Law Review 2020.

[30] *op cit* Article 29 Data Protection Working Party. Opinion 2/2017.

[31] *op cit* Eurofound. Employee monitoring and surveillance.

[32] *op cit* Barzilay, A. R.

development and becoming more sophisticated and increasingly affordable, enabling intrusive employee monitoring, regulatory provisions at the EU level and individual member states are often out of step with technological developments.[33] Hence my publications (publications I, II, III, IV, V) and the present dissertation examine how the current privacy and data protection framework in the EU is equipped to protect employees from privacy-invasive monitoring practices.

1.2 Setting the problem

1.2.1 Privacy concerns in a digital workplace

The dissertation contributes to the discussion of privacy and data protection by exploring the possible ways employers could make use of and rely upon different digital monitoring technologies. The choice to focus both on privacy and data protection is inevitable because the discussion concerning digital monitoring technology should be based on both topics – it can be argued that the distinction between privacy and data protection is made not to separate these rights but to provide more specific norms governing privacy protection.[34] Although sometimes data protection is regarded as detached from privacy,[35] researchers mostly contend that data protection rules are intended to ensure privacy as they help to protect fundamental values of human dignity and individual autonomy.[36] As Poullet noted, 'privacy, now protected through personal data protection legislation, thus becomes the fundamental freedom, and the necessary condition for all other freedoms'.[37] Overall, data protection is said to be founded on our existing ideas of privacy and seen as a tool of transparency[38] – setting terms under which it is possible to collect and use personal data. Therefore, data protection should

---

[33] *op cit* Eurofound. Employee monitoring and surveillance.

[34] Purtova, N. Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver in European Data Protection Rights. – Netherlands Quarterly of Human Rights 2010/28 (2).

[35] De Hert, P., Gutwirth, S. Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. In Claes, E., Duff A., Gutwirth, S. (Eds.) Privacy and the criminal law. Antwerp/Oxford: Intersentia, 2006.; Lynskey, O. The Foundations of EU Data Protection Law. Oxford University Press 2015.

[36] Bygrave, L. A. The Place of Privacy in Data Protection Law. – University of New South Wales Law Journal 2001/24 (1); Rouvroy., A., Poullet, Y. The right to informational self-determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In Gutwirth S., Poullet Y., De Hert P., de Terwangne C., Nouwt S. (Eds.) Reinventing Data Protection? Springer 2009.

[37] Poullet, Y. Data protection legislation: What is at stake for our society and democracy? – Computer Law & Security Review 2009/25 (3).

[38] *op cit* Poullet, Y.; Andrade, N. Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights. In Fischer-Hübner, S., *et al*. (Eds.) Privacy and Identity Management for Life: 6th IFIP WG PrimeLife International Summer School. Springer 2011.

not be built or discussed separate from privacy. On the basis of the above explanations, both privacy and data protection issues are tackled in the present dissertation in the context of digital monitoring technologies. More specifically, data protection is considered as a part of privacy.

In addition, it is important to clarify, that my publications concentrate on privacy and data protection issues concerning three specific digital monitoring technologies – social media monitoring (publication I and II), monitoring microchipped employees (publication III) and digital monitoring technologies used during COVID-19, such as contact tracing technologies (publication IV and V). Two of the publications (publication IV and V) discuss workplace monitoring during the spread of COVID-19 as employers who needed to respond to the threat posed by the virus had to implement measures to protect their employees' health and safety. In many workplaces, the need for a safe working environment resulted in deepening control over employees (e.g. monitoring of teleworkers)[39] and rise of new monitoring practices[40]. My publications cover these specific digital monitoring technologies (social media, microchips and contact tracing applications) due to their newness and their possibility to reveal vast amounts of data in a covert manner concerning employees. They also allow increased access to the employee's personal sphere and undeniably add an additional dimension to the employment relationship highlighting contradictory interests, namely employers' power of control and employee's privacy and data protection rights. Furthermore, in the shift towards greater sophistication of the new 'dataveillance'[41] technologies and their acceptance in the workplace, employee's privacy and data protection are challenged by evolving capabilities of these technologies and increasing data processing. Taking the above into consideration, the next sections give an overview of digital monitoring technologies analysed in my publications, provide insight about the potential privacy problems related to their adoption in the workplace and refer to current research on this topic.

[39] Hodder, A. New Technology, Work and Employment in the era of COVID-19: reflecting on legacies of research. – New Technology, Work and Employment 2020/35 (3).

[40] See for example: Chesler, C. Coronavirus will turn your office into a surveillance state. – Wired Daily. 04.05.2020; As employees return to the office, banks explore surveillance tech. – Reuters. 21.05.2021; Watkins, K. Security and Privacy of COVID-19 Contact-Tracing Apps. Symantec Enterprise Blogs 2021. – https://symantec-enterprise-blogs.security.com (30.07.2021); Fragala, M. S., Goldberg, Z. N., Goldberg, S. E. Return to Work: Managing Employee Population Health During the COVID-19 Pandemic. – Population Health Management 2021/24 (1).

[41] Dataveillance is a form of continuous surveillance through the use of (meta)data. Raley, R. Dataveillance and Countervailance. In Gitelman, L. (Ed) 'Raw Data' is an Oxymoron. Cambridge, MA: MIT Press 2013; van Dijck, J. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. – Surveillance & Society 2014/12 (2).

1.2.2 Social media

First, let us look at social media[42] as a possible source of applicants' and employees' data. The widespread use of social media has led employers in Estonia and all over the world to routinely use information found on social networking sites (e.g. Facebook) to employ and manage their workforce.[43] Various studies and court cases indicate that processing of employee data on social media may have a considerable effect on human resource decisions, including hiring, training, promotion and termination.[44] The growing popularity of using social networking sites is usually justified by the fact that such an approach is quick and inexpensive and enables conclusions to be drawn about the applicant's and employee's character.[45] This approach has been considered promising by various human resources and popular media accounts which highlight the importance and benefits of managers' use of big data[46] analysis, noting for example that recruitment is superior when based on data collated from numerous social media sources (e.g. Facebook, LinkedIn), together with other sources such as CV databases.[47] This is because the use of social media enables employers to obtain

---

[42] Social media is defined as the Internet-based platforms based upon Web 2.0 that allow users to generate and exchange their own content. Kaplan, A. M., Haenlein, M. Users of the world, unite! The challenges and opportunities of Social Media. – Business Horizons 2010/53 (1).

[43] boyd, d.n., Ellison, N. B. Social Network Sites: Definition, History, and Scholarship. – Journal of Computer Mediated Education 2007/13 (1); Visamaa, K. Veebipõhiste sotsiaalvõrgustike kasutamine töötajate värbamisel [The use of social networking sites in recruitment], Bachelor thesis. University of Tartu 2011; Ivask, E.-L. The Use of Facebook as Evaluation Method for Job Candidates in Service Sector Organizations. Bachelor Thesis. University of Tartu 2013.

[44] Brown, V. R., Vaughn, E. D. The Writing on the (Facebook) Wall: The Use of Social Networking Sites in Hiring Decision. – Journal of Business and Psychology 2011/26 (2); Abril, P. S., Levin, A., Del Riego, A. Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee. – American Business Law Journal 2012/49 (1); Landers, R. N., Schmidt, G. B. Social Media in Employee Selection and Recruitment: An Overview. In Landers, R. N., Schmidt, G. B. (Eds.) Social Media in Employee Selection and Recruitment. Theory, Practice, and Current Challenges. Springer International Publishing Switzerland 2016.

[45] Clark, L. A., Roberts, S. J. Employer's use of social networking sites: A socially irresponsible practice. – Journal of Business Ethics 2010/95 (4); Guilfoyle, S., Bergman, S. M., Hartwell C., Powers, J. Social Media, Big Data, and Employment Decisions: Mo' Data, Mo' Problems? In Landers, R. N., Schmidt, G. B. (Eds.) Social Media in Employee Selection and Recruitment. Theory, Practice, and Current Challenges. Springer International Publishing Switzerland 2016.

[46] Big data refers to large amounts of data produced very quickly by a high number of diverse sources. Data can either be created by people or generated by machines, such as sensors gathering climate information, satellite imagery, digital pictures and videos, purchase transaction records, GPS signals, etc. European Commission. Big data. – https://ec.europa.eu/ digital-single-market/en/big-data (30.07.2021).

[47] Barzilay, A. Data Analytics at Work: A View From Israel on Employee Privacy and Equality in the Age of Data-Driven Employment Management. – Comparative Labor Law & Policy Journal 2019/40.

information to predict an individual's potential to perform job-related tasks, complement the social structure of the organization[48] and help to predicting employees' behaviour (e.g. who is likely to quit work)[49]. An employer may also gather and assess behavioural metadata, such as 'likes', shares, retweets, and follows, using big data techniques to infer psychological traits that are traditionally assessed during the selection process.[50]

The use of social media as a monitoring tool has led to the blurring of boundaries between the personal and professional lives of employees and applicants and has started to create both legal and ethical challenges for employers.[51] Scholars have indicated two main legal and ethical issues surrounding these practices – the right of the employer to access an employee's or applicant's online information, and the permissibility of basing hiring, promotion or dismissal decisions on the discovered information.[52] These issues indicate that although social media monitoring may prove to be a potentially promising source of data on applicants or employee data, it is also fraught with potential risks for the employee.

As discussed in publication I, studies carried out among employees show that employees consider background checks conducted by employers on social media profiles unacceptable as compromising employees' privacy on social media may result in various types of harm. Social media monitoring may reveal job-irrelevant information[53], lead to premature conclusions about employees' personality and skills and result in the loss of employment opportunities as information presented in one context is used in another (also referred as information injustice[54]). Due the possible harm that may arise from social media monitoring, the widespread use of this practice and employees' hesitations concerning the monitoring, the questions of privacy and data protection are imminent.

---

48 Carr, C. T. An Uncertainty Reduction Approach to Applicant Information-Seeking in Social Media: Effects on Attributions and Hiring. In Landers, R. N., Schmidt, G. B. (Eds.) Social Media in Employee Selection and Recruitment. Theory, Practice, and Current Challenges. Springer International Publishing Switzerland 2016.

49 *op cit* Barzilay, A.

50 Youyou, W., Kosinski, M., Stillwell, D. Computer-based personality judgments are more accurate than those made by humans. Proceedings of the National Academy of Sciences 2015/112 (4).

51 Vinson, K. E. The blurred boundaries of Social Networking in the Legal Field: Just 'Face' it. – University of Memphis Law Review 2010/41.

52 *op cit* Abril, P. S., Levin, A., Del Riego, A.

53 Davison, H. K., Bing, M. N., Kluemper, D. H., Roth, P. L. Social Media as a Personnel Selection and Hiring Resource: Reservations and Recommendations. In Landers, R. N., Schmidt, G. B. (Eds.) Social Media in Employee Selection and Recruitment. Theory, Practice, and Current Challenges. Springer International Publishing Switzerland 2016.

54 van den Joven, M. J., Weckert, J. Information Technology and Moral Philosophy. Cambridge University Press 2008.

1.2.3 Microchips

Unlike social media monitoring, the use of microchips implanted under an employee's skin is still in its infancy, however, the practice has become a reality in many workplaces. There are various examples of microchips being implanted into employees in different parts of the world (US, Mexico, Sweden, Belgium).[55] This rising new trend is also apparent in Estonia where a few companies have taken the lead in microchipping their employees.[56] The reason for the escalating use of microchips lies primarily in advanced miniaturization and continuously falling prices, which makes the use of chips economically viable.[57] Also, preliminary findings indicate that our technology saturated society is becoming increasingly accepting of *insideable technologies* (e.g. subcutaneous technologies)[58] and the practice of microchipping employees may become even more common through commercialization of these chips.[59] At the same time, in some countries, the trend of microchipping employees has also been met with raised concerns. For example, in Britain, trade unions have expressed reluctance about the prospects of British companies implanting staff with microchips.[60]

In the majority of occasions, microchip implants are currently used to replace artefacts such as credit cards, keys, passwords and bracelets that allow users to automatically open doors, trigger computers or printers and pay for purchases.[61] Chips are therefore linked to convenience in everyday activities, but as the cost of implementing RFID systems drops and the functionality of chips grows, organizations may choose to use this technology to track employee productivity, improve security and reduce theft[62] as microchips may make it possible to log

---

55 Esfola, J. P. M. Bar Coded at Work. LL.M. Law & Technology. Tilburg Institute of Law, Technology and Society (TILT). – http://arno.uvt.nl/show.cgi?fid=146486 (30.07.2021); Yeginsu, C. If Workers Slack Off, the Wristband Will Know. (And Amazon Has A Patent For It.). – The New York Times 01.02.2018; Miller, A. More Companies Are Using Technology to Monitor Employees, Sparking Privacy Concerns. – ABCNEWS 10.03.2018.

56 Kanarbik, L. Võtmed naha all ehk Miks Ülemiste linnaku töötajad end kiibistada lasevad [The keys under the skin, i.e. Why the employees of Ülemiste City let themselves be implanted with a microchip]. – Eesti Päevaleht 11.10.2018.

57 Thiesse, F. RFID, privacy and the perception of risk:A strategic framework. – The Journal of Strategic Information Systems 2007/16 (2).

58 Gauttier, S. I've got you under my skin' – The role of ethical consideration in the (non-) acceptance of insideables in the workplace. – Technology in Society 2019/56.

59 Roosendaal A. P. C., Kosta, E. A study on ICT implants. FIDIS Deliverables; No. D12.6). FIDIS 2008. – http://www.fidis.net (30.07.2021).

60 Kollewe, J. Alarm over talks to implant UK employees with microchips. – The Guardian 11.11.2018.

61 *Op cit* Gauttier, S.

62 Scassa, T., Chiasson, T., Deturbide, M., Uteck, A. An Analysis of Legal and Technological Privacy Implications of Radio Frequency Identification Technologies. Report Prepared under the Contributions Program of the Office of the Privacy Commissioner of Canada 2005. – https://libraries.dal.ca (30.07.2021).

employees' movements and location and to measure their working time and pace. In addition to these functions, chips can also be characterized by their continuous presence and lack of control by the employee. As discussed in my publication III, the use of microchips may raise several data protection concerns, such as the possibility of covert and constant surveillance, profiling and digital discrimination.[63] Due to their features and concerns they reveal, the use of microchips in a manner that is respectful of privacy is crucial to maintaining human dignity in the employment context.[64] Again this technology challenges the privacy and data protection framework enacted in the EU. The European Parliament has also acknowledged data protection concerns microchips could mean for the employee and published a study on possible issues arising from microchipping in the workplace.[65] As discussed in publication III, analysis in that report is too generic and the issue needs further examination.

1.2.4 Contact tracing apps and health monitoring technologies

As discussed in my publications IV and V, not only technology but also critical situations may lead to new monitoring practices that have an impact to employees' privacy and data protection rights. This has been evident during the COVID-19 crisis. According to the International Labour Organization, 94% of the world's employees lived in countries with some sort of workplace closure as a health and safety measure in 2020[66], indicating that workplace lockdowns affected a large proportion of the workforce. Thus, all EU member states and organizations alike are trying hectically to find solutions for slowing the spread of the disease to enable employees to return to work safely. In the case of infectious diseases such as COVID-19, workplaces are effective focal points for the dissemination of information and activation of occupational health and safety measures,[67] and different data collection and monitoring technologies can potentially be introduced in order to ensure a safe working environment. As discussed in my publication IV, this has forced EU and national data protection authorities in Europe to address questions concerning privacy and data protection to determine what personal information employers need to, or can, collect about

---

[63] e.g. more prejudiced treatment of employees without chips which may lead to their exclusion from different possibilities such as better working conditions.

[64] Office of the Privacy Commissioner of Canada. Radio Frequency Identification (RFID) in the Workplace: Recommendations for Good Practices 2008. – https://www.priv.gc.ca/en (30.07.2021).

[65] *op cit.* Graveling, R., Winski, T., Dixon, K.

[66] ILO Monitor: COVID-19 and the world of work. Sixth edition. International Labour Organization 2020. – https://www.ilo.org/ (31.07.2021).

[67] COVID-19 and the world of work: Impact and policy responses. International Labour Organization 2020. – https://www.ilo.org/ (31.07.2021).

employees to limit the spread of the virus.[68] Furthermore, several researchers have indicated possible deficiencies concerning privacy and data protection in employment in the context of COVID-19. For example, both Mangan, Gramano et al.[69] and Hendrickx, Taes et al.[70] have discussed employers' obligations concerning data processing to ensure health and safety in the workplace and have raised questions about the extension of the employee's duties to cooperate with employers to limit the spread of the virus.

Considering that employers must maintain safe workplaces and prevent work-related injuries and illnesses[71] means that employers are also required to limit and, if necessary, track cases of COVID-19 caused in work settings. As COVID-19 is a contagious disease that spreads through close social interaction between humans, contact tracing, i.e. the practice of identifying persons who are in close contact with the infected person so that exposed individuals can be informed to self-isolate and go into quarantine, has become one of the most important mechanisms for containing the spread of the virus.[72] Although no evidence has been currently found on the effectiveness of automated contact tracing apps to reduce infected cases or the number of infected contacts identified[73], many different app providers e.g. various health protection agencies; non-health agencies within a federal government or local government; health insurers; employers; non-profit organizations; and universities; have developed new kinds of COVID-19 response technologies.[74] Therefore, in deciding how to manage COVID-19 detection and control in a workplace, employers have a number of different options.

As discussed in my publication V, employers may use contact tracing apps developed at the national level or use solutions generated for mitigating the spread of COVID-19 at an organizational level. One of the easiest options for the employer would be to make use of the contact tracing apps initiated on the state

---

[68] The European Data Protection Board and several national data protection authorities have issued specific guidance to employers on dealing with COVID-19 and data protection issues in the workplace. COVID-19 Resources Library. Global Privacy Assembly. – https://globalprivacyassembly.org (31.07.2021).

[69] Mangan, D., Gramano, E., Kullmann, M. An unprecedented social solidarity stress test. – European Labour Law Journal 2020/11 (3).

[70] Hendrickx, F., Taes, S., Wouters, M. Covid-19 and labour law in Belgium. – European Labour Law Journal 2020/11 (3).

[71] European Commission. EU strategic framework on health and safety at work 2021–2027 Occupational safety and health in a changing world of work. – COM(2021) 323 final.

[72] World Health Organization. Contact tracing in the context of COVID-19: interim guidance. 2020. – https://apps.who.int (31.07.2021).

[73] Jeffrey, B., Ludlow, K., Testa, L., Herkes, J., Augustsson, H., Lamprell, G., McPherson, E., Zurynsk, Y. Built to last? The sustainability of healthcare system improvements, programmes and interventions: a systematic integrative review. – BMJ Open 2020/10 (6).

[74] See for example: McKinsey & Company. How COVID-19 has pushed companies over the technology tipping point – and transformed business forever. Survey 2020. – https://www. mckinsey.com (31.07.2021).

level as these are free and widely available almost in every EU member state.[75] Employers may also use custom-built solutions to monitor employees during COVID-19, i.e., employers have the option of building their own contact tracing apps, sourcing one from app developers, or subscribing to workplace contact tracing systems offered by private companies. Whether government owned or developed by a private company, each of these technologies brings forth the inevitable rise of surveillance in a workplace and presents different challenges from a privacy and data protection perspective. As discussed in my publication V, recent analyses provide insights about the potential problems related to the adoption of digital contact tracing. Many authors writing on this topic have addressed various concerns related to privacy, including security and risks associated with the use of data[76] and data privacy in particular[77] as well as ethical challenges of using public health surveillance technologies[78]. Although scholars have voiced their concerns about governments offering surveillance solutions[79], and app users have brought actions against app developers and health departments after COVID-19 contact tracing apps have exposed sensitive data of individuals who used the platform[80], less attention has been paid to employer-employee power relationships and ubiquitous surveillance in the

[75] European Commission. Mobile applications to support contact tracing in the EU's fight against COVID-19. 2020. – https://ec.europa.eu (31.07.2021).

[76] See for example: Spears, J. L., Padyab, A. Privacy risk in contact tracing systems – Behaviour & Information Technology 2021; *op cit* Watkins, K.; Boudreaux, B., DeNardo, M. A., Denton, S. W., Sanchez, R., Feistel, K., Dayalani, H. Data Privacy During Pandemics: A Scorecard Approach for Evaluating the Privacy Implications of COVID-19 Mobile Phone Surveillance Programs. Santa Monica, Calif.: RAND Corporation 2020; van Kolfschooten, H., de Ruijter, A. COVID-19 and privacy in the European Union: A legal perspective on contact-tracing". – Contemporary Security Policy 2020/41 (3); Kitchin, R. Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of COVID-19. – Space & Polity 2020/24 (3); Raskar, R. *et al*. Apps Gone Rogue: Maintaining Personal Privacy in an Epidemic. 2020. – arXiv:2003.08567 [cs.CR].

[77] Newlands, G., Lutz, C., Tamo'-Larrieux, A. Villaronga, E. F., Harasgama, R., Scheitlin, G. Innovation under pressure: Implications for data privacy during the Covid-19 pandemic. – Big Data & Society 2020/7 (2); Galloway, K. The COVID cyborg: protecting data status. – Alternative Law Journal 2020/45 (3); Bradford, L., Aboy, M., Liddell, K. COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR and Data Protection Regimes. – Journal of Law and the Biosciences 2020/7 (1).

[78] Floridi, L. Mind the App – Considerations on the Ethical Risks of COVID-19 Apps. – Philosophy & Technology 2020/33; Lo, B., Sim, I. Ethical Framework for Assessing Manual and Digital Contact Tracing for COVID-19. – Annals of Internal Medicine 2021/174 (3).

[79] *Op cit* van Kolfschooten, H., de Ruijter, A.; Riemer, K., Ciriello, R., Peter, S., Schlag-wein, D. Digital contact-tracing adoption in the COVID-19 pandemic: IT governance for collective action at the societal level. – European Journal of Information Systems 2020/29 (6).

[80] Davis, J. PA Health Dept Sued; Investigation Looms, After Contact Tracing Breach. – Health IT Security 10.05.2020; Davis, J. Google Sued, Lawsuit Claims COVID-19 Contact Tracing Tool Exposes Data. – Health IT Security 30.04.2021.

workplace in this context[81]. The issue of privacy and data protection in the EU is even more relevant as the advice given by the European Data Protection Board (EDPB)[82] concerning contact tracing in the workplace has been generic,[83] and during the COVID-19 outbreak, EU data protection rules enacted in the General Data Protection Regulation (GDPR)[84] have been both praised and criticized in the context of contact tracing apps. For example, Labour MP and chair of the Joint Committee on Human Rights Harriet Harman has said that the GDPR is totally inadequate for ensuring the security and privacy of data collected by the government's COVID-19 contact tracing app[85]. Scholars, however, have stated that the EU data protection legal framework was designed to be sufficiently flexible and as such, is able to allow for both an efficient response in limiting the pandemic and for protecting fundamental human rights and freedoms.[86]

1.3 The research problem

Today, work technology advancements, have given rise to new organizational behaviour regarding the management of employees and prompted new legal questions regarding the protection of employees' rights.[87] The invasive nature of digital monitoring technologies makes it of utmost importance to question how an employee's right to privacy and the protection of their personal data can be safeguarded against possible privacy-invasive monitoring practices. The issue is particularly relevant as scholars argue that increasing technology innovation

---

[81] Bodie, M. T., McMahon, M. Employee Testing, Testing, Tracing, and Disclosure as a Response to the Coronavirus Pandemic. – Washington University Journal of Law and Policy 2020/64; Yang, X. Workforce Survival: Tracking Potential COVID-19 Exposure Amid Socioeconomic Activities Using Automatic Log-Keeping Apps. – Population Health Management 05.04.2020; Scassa, T. COVID-19 Contact Tracing: From Local to Global and Back Again. – International Journal of E-Planning Research, IGI Global 2021/10 (2).

[82] The EDPB is an independent European body, which contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the EU's data protection authorities. The EDPB is established by the General Data Protection Regulation and composed of representatives of the EU national data protection authorities. https://edpb.europa.eu/about-edpb (31.07.2021).

[83] European Data Protection Board. Statement on the processing of personal data in the context of the COVID-19 outbreak. 19.03.2020.; See also European Data Protection Supervisor. Orientations from the EDPS. Reactions of EU institutions as employers to the COVID-19 crisis. 15.07.2020.

[84] 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). – OJ L 119 4.5.2016, p. 1.

[85] Scroxton, A. GDPR wholly inappropriate to govern contact-tracing data. – ComputerWeekly 19.05.2020.

[86] Kędzior, M. The right to data protection and the COVID-19 pandemic: the European approach. – ERA Forum 2021/21.; *op cit* Bradford, L., Aboy, M., Liddell, K.

[87] *op cit* Ajunwa, I., Crawford, K., Schultz, J.

appears destined to further challenge regulatory frameworks as digital monitoring technologies can be expected to develop in the future.[88] However, regardless of increasing monitoring practices and public concern[89], academic discussion of emerging technologies and the legal and ethical aspects of employees' rights vis-a-vis workplace monitoring, is still growing and has mainly been carried out in the US. This is understandable, as scholars argue that there are no real federal laws in the US limiting the collection of data received from digital monitoring technologies and the applicability of various federal statutes in the context of surveillance is extremely narrow.[90] This gives US employers broad licence to monitor employees. However, in recent years scholars, legislators, experts and employee representatives in the EU have also started to discuss possible concerns related to digital monitoring technologies on a greater scale.[91] For example, the European Trade Union Confederation has called for an EU directive on privacy at work[92] and the European Trade Union Institute has highlighted the need for the development of a governance framework in relation to the use of AI (along with other new technologies).[93] The pressure of new technologies has led EU institutions to initiate possible legislative initiatives. Firstly, the European Commission has launched a legislative proposal for an Artificial Intelligence Act that provides a legal framework for the use of AI.[94] Secondly, due to the widespread increase in telework and taking into consideration that technological advances have added a new layer of complexity to monitoring in the workplace, in 2021 European Parliament called on the European Commission to come up with a law allowing employees to disconnect from work during non-work hours without consequences and setting minimum standards for remote work.[95] In the course of this initiative, the Parliament also acknowledged that the use of intrusive digital monitoring technologies in the workplace is to some extent addressed and regulated only in some member states.[96]

In the EU, employee monitoring is not explicitly regulated, but privacy and data protection rights that may be violated by employee monitoring are regulated. The normative basis for privacy in the EU derives from the provisions of privacy

---

88 Tikkinen-Piri, C EU General Data Protection Regulation: Changes and implications for personal data collecting companies. – Computer law & security review 2017/34 (1).

89 See for example: Carpenter, D., McLeod, A., Hicks, C., Maasberg, M. Privacy and Biometrics: An Empirical Examination of Employee Concerns. – Information Systems Frontiers 2018/20.

90 *op cit* Ajunwa, I., Crawford, K., Schultz, J.

91 *op cit* Eurofound. Employee monitoring and surveillance.

92 European Trade Union Confederation. ETUC resolution on digitalisation: Towards fair digital work. 2016. – https://www.etuc.org (31.07.2021).

93 European Trade Union Institute. Labour in the age of AI: Why regulation is needed to protect workers. 2020. – https://www.etui.org (31.07.2021).

94 *op cit* European Commission. COM/2021/206 final.

95 *op cit* European Parliament resolution of 21 January 2021.

96 *Ibidem.*

and data protection regulated in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)[97], Article 7 and 8 of the Charter of Fundamental Rights of the European Union and the GDPR. Without underestimating the important value added by the Charter to privacy and data protection in the European Union, this dissertation focuses on the ECHR and the GDPR. The Charter is left out from the analysis for several reasons: 1) the wordings in Article 8(1) of the ECHR and in Article 7 of the Charter concerning private life are almost identical; 2) the right to private life regulated in the Charter should be given the same meaning and scope as in the ECHR[98]; 3) the protection afforded to privacy by the Charter may not lower the level of protection provided for in the ECHR[99]; 4) the concept of privacy regarding monitoring in the workplace has had a long time to develop under the rulings of the European Court of Human Rights (hereinafter 'ECtHR') and 5) the right to data protection established in the Charter is further materialized in the GDPR, which in 2018, replaced Data Protection Directive[100] with the intent of strengthening and unifying data protection for all individuals with EU and setting forth rules to make sure people's right to personal data protection remains effective in the digital age.[101]

Employers must therefore rely on the legislation cited above when they keep track of their employees using digital monitoring technologies. As discussed in publications I–V, in the case of workplace monitoring, both employers and employees must navigate complex topics regarding data protection and privacy as both the ECHR and the GDPR do not specifically address employee's rights in the employment context and therefore fail to give a set of uniform rules that regulate workplace monitoring. The struggles that parties to employment contracts face indicate possible challenges for the legal clarity of the existing privacy and data protection framework. Also, it can be argued that neither the ECHR nor the GDPR offers specific guidelines for the implementation of its provisions with respect to employee monitoring. EDBP and its predecessor, the Article 29 Working Party,[102] have given various guidance concerning collection of data

---

[97] Article 6(2) Treaty on European Union provides that the EU shall accede to the European Convention on Human Rights. Its aim is to ensure in the long-term comprehensive and stable consistency between EU law and the Convention. See for example: Callewaert, J. Do we still need Article 6(2) TEU? Considerations on the absence of EU accession to the ECHR and its consequences. – Common Market Law Review 2018/55 (6).

[98] Charter art 52(3)

[99] Charter article 53

[100] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Union. – L 281, 23.11.1995, 31–50.

[101] European Commission. Questions and Answers – Data protection reform. 21.12.2015) – http://europa.eu (31.07.2021).

[102] Article 29 Working Party was an independent European working party that served as an advisory body dealing with issues relating to the protection of privacy and personal data until 25 May 2018. It has been replaced by the European Data Protection Board under the GDPR.

under the GDPR. However, these guidelines often do not address specific monitoring activities at all or do so in a generic manner. Also, the Court of Justice of the European Union has only handed down limited case law on the use of digital monitoring technologies at work. Due to the general guidance and lack of jurisprudence at EU level, national data protection authorities play an important role in clarifying the relevant rules and have issued opinions and guidance on employee monitoring in general, as well as on specific forms of monitoring in the workplace. However, as discussed in publication V, their guidance is often country-specific and varies in the case of digital monitoring technologies.

Today, specific rules at the national level are allowed by laws or collective agreements under Article 88(1) of the GDPR. Member states may therefore introduce specific provisions with regard to the processing of employee data for a variety of purposes, from recruitment to health and safety, under this article. For these reasons, it can be argued that it is in the remit of the member state or social partners to rectify possible concerns related to employee monitoring. However, according to the research carried out by Eurofound, national legislation struggles to keep pace with technological advances and often does not account, sufficiently or at all, for employers' use of state-of-the-art technologies for monitoring purposes.[103] In many countries (especially in eastern EU member states), the topic of employee monitoring is not high on the policy agenda of the government or social partners.[104] These member states (e.g. Estonia) have no specific rules concerning data collection in employment and therefore apply the rules enacted in the GDPR. In other countries, a wide range of different practices is available as several member states have enacted laws or allowed derogations under collective agreements concerning data collection in employment and employee monitoring (e.g. Finland) and others rely on individual provisions in data protection laws that address the same issues (e.g. Germany).[105] In most member states, legislation follows a technologically neutral approach (as also used in the GDPR), setting general rules of wide applicability that in principle cover all types of monitoring and data processing.[106] Still, a handful of countries in the EU have also regulated the use of some intrusive digital monitoring technologies in the workplace, such as biometric monitoring.[107] Similarities can be cited with the US, where some states have responded to the growth potential of microchipping, increased use of social media and biometric monitoring by proactively adopting legislation that

---

[103] *op cit* Eurofound. Employee monitoring and surveillance.

[104] *Ibidem.*

[105] *Ibidem.*

[106] GDPR recital 6; *op cit* Eurofound. Employee monitoring and surveillance.

[107] France (Data Protection Act, Law 2018–493 of 20 June 2018) and Portugal (Law 58 of 8 August 2019). See for example: Rodrigues, M. G., Bairrão, I. New Portuguese Data Protection Act. Garriues – Lexology 13.08.2019; French Implementation of the GDPR. Ahmed Baladi, Gibson, Dunna & Chrutcher. Thomson Reuter 2019. – https://www.gibsondunn.com (31.07.2021).

addresses specific technologies to contain the threat posed to employees.[108] Also, the framework agreement on digitalization adopted by the European social partners in 2020 is reminiscent of Article 88 of the GDPR and the possibilities to establish more specific rules in collective agreements on the protection of the rights and freedoms in relation to the processing of personal data in the context of the employment relationship.[109] The reasoning in the agreement states that the use of digital technologies and AI surveillance systems poses new risks, potentially compromising human dignity and contributing to a deterioration of working conditions. In summary, different legal approaches in EU member states, the agreement of the European social partners and the evolving technological landscape all continue to widen the differences between countries and open the door for various and contradicting practices concerning the use of digital monitoring technologies.

To conclude, EU has one of the recent and most substantial data protection frameworks in the world; however, employee monitoring is not explicitly regulated, which spawns a wide range of national practices. The main problem analysed in the present dissertation is that privacy and data protection regulation in the ECHR and in the GDPR lack clarity and specificity with regard to the use of digital monitoring technologies at work. The problem is not specific to digital monitoring technologies referred in subchapters 1.2.2–1.2.4, as the use of existing technologies or uptake of any new technology might lead to the same problem with existing regulation. However, it can be argued that the problem has emerged critically due to digital monitoring technologies that enable constant and covert monitoring of employees and has escalated during the COVID-19 pandemic when employers had to limit the spread of the disease and used different methods of monitoring to do so. The problem is escalated further still by the rise of AI and its use in the workplace. If the problem is ignored, it might lead to further deterioration of employees' rights, increase the discretionary power of employers and therefore lead to invasive monitoring practices.

1.4 The aim and research questions

In the context of digital monitoring technologies, it is important to discuss whether the rules enacted in the ECHR and the GDPR create a framework that enables employers to monitor employees so that employees' rights concerning their privacy are not unjustifiably hindered, and consider whether there is a necessity for additional protection of employees. For this reason, the aim of the dissertation is to ascertain whether there is a need for specific rules at the EU

[108] Schmidt, G., O'Connor, K. W. Social Media, Data Privacy, and the Internet of People, Things, and Services in the Workplace: A Legal and Organizational Perspective. In Simmers, C., Anandarajan, M. (Eds.) The Internet of People, Things and Services. Workplace Transformations. Routledge 2018.

[109] European social partners framework agreement on digitalisation. ETUC, BusinessEurope, CEEP and SMEUnited. Brussels (2020). – https://www.etuc.org (31.07.2021).

level that regulate privacy and data protection in case an employer uses digital monitoring technologies at work and on what conditions employee monitoring using these technologies should be allowed. More specifically, the dissertation contains critical analysis of employee privacy and data protection rights enacted in the ECHR and the GDPR in the context of digital monitoring technologies to determine whether the EU legislature should enact a directive or regulation that deals with employee's privacy rights. If the analysis indicates that EU legislation is needed to protect employees, the dissertation proposes to supplement EU legislation.

The dissertation outlines the current privacy framework under the ECHR and the GDPR to determine under what conditions employers can monitor employees and what the possible challenges are related to employee's privacy when using digital monitoring technologies. Since assessment of the entire GDPR would be superfluous, the analysis in the present dissertation is limited in scope and I concentrate on the applicability of data protection rules under the GDPR, compare different legal bases that employers may use for workplace monitoring and discuss issues concerning data protection principles to draw conclusions whether the EU needs a set of specific rules concerning workplace monitoring. Although all data protection principles must be followed for data processing, the dissertation concentrates on the principles of lawfulness, purpose limitation, fairness and transparency that raise the most questions in the context of digital monitoring technologies.

To achieve the research aim laid out above, the main research questions addressed in the context of digital workplace monitoring practices are as follows:

1) How does the ECHR protect employees if digital monitoring technologies are used by the employer in the digital workplace?
2) Under which conditions does the GDPR apply if the employer uses digital monitoring technologies? Which monitoring practices used by employers in the digital workplace under the GDPR could potentially invade the privacy and data protection rights of employees? Which monitoring practices used by employers in the digital workplace do not fall under the scope of the GDPR but should be regulated to protect employees' privacy?
3) Which legal bases used by employers in the digital workplace to monitor employees under the GDPR could potentially invade the privacy and data protection rights of employees?
4) What protection do the data protection principles offer to employees if the employer monitors employees in the digital workplace?

The dissertation is organized so that each research question is addressed in a separate chapter: the first research question is discussed in the second chapter, the second research question is analysed in the third chapter, and the third and fourth research questions are covered in the fourth and fifth chapter.

1.5 Methods and sources

I used doctrinal research[110] to discuss application and interpretation of Article 8 of the ECHR and rules in the GDPR to ascertain whether there is a need for specific rules at the EU level to regulate privacy and data protection in case employer uses digital monitoring technologies at work and on what conditions employee monitoring using these technologies be allowed. As appropriate to this traditional research method, I aimed to systematize, rectify and clarify the law[111] on employee monitoring by analysing texts that consist of primary and secondary sources. Therefore, a systemic analysis of relevant rules in the ECHR and the GDPR was carried out as well as analysis of additional sources, including legislation, preparatory works, scholarly writings, jurisprudence, studies and guidelines. More specifically, I examined the scholarly writings concerning the legal regulation of digital monitoring technologies and their different aspects and possible concerns related to privacy, security and ethics. Also, more voluminous literature on privacy and data protection has been referred and discussed. Additionally, as the topic of digital monitoring technologies is novel, empirical studies and popular science articles from private and public sources were occasionally relied upon. I used these sources to get a better understanding of different digital monitoring technologies, their features, privacy and security risks and advantages. Furthermore, different guidelines and studies by several institutions, for example, research from the European Commission, European Parliament and International Labour Organization and guidance from the Article 29 Working Party (later EDPB) and national data protection authorities has been analysed.

However, it needs to be acknowledged that the traditional method of doctrinal research does not fully allow to experience the law in action as argued by scholars, and the method focuses on rules of law and does not permit systematic and regular reference to the context of the problems the laws were supposed to resolve, the purpose they were to serve and the effect they in fact have.[112] Therefore, as the pure doctrinal analysis has been criticized for its 'intellectually rigid,

[110] The doctrinal research involves the identification and interpretation of legal texts. (Hutchinson, T., Duncan, N. Defining and describing what we do: doctrinal legal research. – Deakin Law Review 2012/17 (1)). According to van Hoecke, the doctrinal research includes two parts. Firstly, it is necessary to collect all relevant materials, including normative cases, legislation, treaties, authoritative non-binding cases and scholarly writings and, secondly, the research involves creating a hypothesis as to the validity and precise meaning of the legal texts, combining 'specific interpretations of legal principles, rules and concepts in a (newly) systematized whole'. van Hoecke, M. Legal doctrine: which method(s) for what kind of discipline? In van Hoecke M. (Ed.) Methodologies of legal research: what kind of method for what kind of discipline? Oxford: Hart Publications 2011.

[111] McConville, M., Chui, W. H. Introduction and Overview. In McConville, M., Chui, W. H. (Eds.) Research Methods for Law. UK: Edinburgh University Press 2017.

[112] Singhal, A. K., Malik. I. Doctrinal and socio-legal methods of research: merits and demerits. – Educational Research Journal 2012/2 (7).

inflexible and inward-looking approach'[113] I did not limit myself only to normative comparisons and also paid attention to the context around the topic of digital monitoring technologies. In publication II, written together with supervisor Andra Siibak, we also used non-doctrinal research, known as socio-legal research, to better understand the possible consequences of digital monitoring technologies on employee expectations and behaviours.[114] The aim of publication II, which uses the socio-legal approach, was to study the social reality surrounding the data processing practices employers and employees engage in on social networking sites. The publication makes use of the data collected during semi-structured individual interviews with Estonian employers and employees in order to study whether there is a mismatch between the social reality of data subjects and the data protection principles. The analysis in publication II demonstrated that this mismatch applies regardless of which sector employers and employees' work in. Furthermore, the mismatch was apparent even if the employers involved in the study had not encountered any actual (e.g. reputational) problems due to their employees' social media posts, and despite the fact that there were specific social media guidelines issued by the organization.

I also used international and comparative legal research so as to acknowledge certain trends and developments and to forecast future developments[115]. The aim of this research is to facilitate our understanding of the operation of international law and legal systems.[116] Comparative research can be used to enrich the imagination and increase the set of alternatives[117] to be taken into account when drafting possible future rules concerning data protection and privacy at work. Unfortunately, the possible deficits of this method also need to be considered as the differences of EU legislation and national legal systems of different member states is not simply a question of differences of doctrine. Problems may be far more fundamental and complicated and may have their roots in the legal system as a whole and in society as whole.[118] In publication I, taking these concerns into account, I compare the privacy approaches in the US and Europe to investigate whether a job applicant actually has a right to privacy if they have a profile on a social networking site, and then examine the practices in a set of European

---

[113] Vick, D. W. Interdisciplinary and the Discipline of Law. – Journal of Law and Society 2004/31.

[114] Socio-legal research is a legal research that employs methods taken from other disciplines to generate empirical data to answer research questions. It can be a problem, policy or law reform based. Non-doctrinal legal research can be qualitative or quantitative. *Op cit* Singhal, A. K., Malik. I.

[115] Blainpain, R. (Ed.) Comparative labour law and industrial relations in industrialized market economies. Xth Edition. Alphen aan den Rijn: Kluwer Law International 2010.

[116] *op cit* McConville, M., Chui, W. H.

[117] Weiss, M. The future of comparative labor law as an academic discipline and as a practical tool. Comparative Labor Law and Policy Journal 2003/25.

[118] Wilson, G. Comparative Legal Scholarchip. In McConville, M., Chui, W. H. (Eds.) Research Methods for Law. UK: Edinburgh University Press 2017.

countries (Estonia, UK, Germany, Finland) to analyse under what conditions employers are allowed to carry out background checks on social media and whether the employer may base their hiring decision on the information found on these public domains. Comparative research has also been used, for example, in publication IV, which studies the guidance issued by data protection authorities and the EDPB. In particular, I have compared and analysed the guidance issued by national data protection authorities in 20 European countries. Also, in all publications as well as in this dissertation, I have used examples from legislation, jurisprudence, guidance and studies around the world (e.g. US, India, Canada) to enrich the discussion.

2. Protection of employee privacy under the ECHR

2.1 The notion of privacy

The right to privacy has been called one of the most open-ended rights, which has not received a comprehensive definition as there are conflicting interpretations of which types of privacy warrant legal recognition and protection.[119] One of the possible definitions of privacy has been provided by Warren and Brandeis, who argued that humans have a natural right to be left alone to determine to what extent their own thoughts and emotions are communicated to others.[120] Privacy has also been described as a freedom from the judgments of others[121] or seen as ensuring a personal zone of non-interference.[122] Our current understanding of informational privacy is based on how an individual relates to and controls access to information about themselves.[123] A specific and relevant notion of privacy has been given by Poullet, who said the right to privacy is associated with 'discretion, anonymity and solitude' or 'escape and withdrawal' that are necessary for an individual to think about or to question their life and to develop their personality and relationships with others.[124] Poullet's interpretation of privacy is also relied upon in the present dissertation when discussing the employee's right to privacy protection.

Standards in relation to the protection of privacy, including in employment relationship, have been established by the international human rights framework, most notably the ECHR and its case law. Article 8(1) of the ECHR states: 'Everyone has the right to respect for his private and family life, his home and his correspondence'. Researchers argue that term 'private life' in the ECHR is used by European legislature as a synonym of privacy that denotes the right to live one's own life with a minimum of interference.[125] The ECtHR case law has systematically stretched and redefined the notion of privacy and gone far beyond the limits

---

[119] Lasprogata, G., King, N. J., Pillay, S. Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada. – Stanford Technology Law Review 2004/4.; Roagna, I. Protecting the right to respect for private and family life under the European Convention on Human Rights, Council of Europe human rights handbooks. Council of Europe Strasbourg 2012.

[120] Warren, S. D., Brandeis, L. D. The Right to Privacy. – Harvard Law Review 1890/4 (5).

[121] Introna, L. D., Pouloudi, A. Privacy in the information age: Stakeholders, interests and values. – Journal of Business Ethics 1999/22 (1).

[122] *Op cit* De Hert, P., Gutwirth, S.

[123] Robinson, N., Graux, H., Botterman, M., Valer, L. Review of the European Data Protection Directive, Santa Monica, Calif.: RAND Corporation 2009.

[124] *op cit* Poullet, Y.

[125] Fabbrini, F. The European Multilevel System for the Protection of Fundamental Rights: A 'Neo-Federalists' Perspective. Jean Monnet Working Paper 2010/15 – https://jeanmonnetprogram.org (31.07.2021).

of traditional wording of the Convention. According to the case law, the ECHR is a 'living instrument' that must be construed 'in the light of present day conditions',[126] which means that ECtHR interprets the right to privacy in the context of changing social, economic and technological developments.[127]

Although Article 8 of the ECHR does not refer to work or workplace in its wording, the ECtHR has, over the course of time, introduced the concept of privacy in the context of work under the scope of this provision and in voluminous case law, the court has analysed whether the actions by the employer may be considered an unjustified interference in the employee's private life.[128] This has led the researchers in Eurofound to argue that the ECHR has so far proven to be flexible enough to address some of the issues arising from technological developments at work.[129] However, Otto criticizes the 'open-texture' of Article 8 and points out that the article is not sufficiently clear and coherent in the context of employment relations, leading to inconsistencies in case law and broad discretion of employers.[130] She emphasizes that digital monitoring technologies have changed the character and reach of the traditional instruments of employer supervision and considerably challenged assumptions concerning the employee's expectations of privacy, noting that enclosing privacy in employment context is a particularly difficult task.[131] The present dissertation contributes to the discussion by analysing, in the following sections, how the ECHR protects employees if digital monitoring technologies are used by the employer in the digital workplace.

2.2 An employee's reasonable expectation of privacy

To better understand the notion of privacy in an employment relationship, it is important to analyse different cases of the ECtHR. In the case of Niemietz vs Germany, the court argues that the professional activities should fall within the range of Article 8 as 'respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings' and explains that 'it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world.'[132] Later cases have confirmed that right to privacy according to the ECtHR in the employment context relies on 'the right to establish and to develop relationships with other human beings, especially in the emotional

[126] ECtHR 5856/72, Tyres v. The United Kingdom.

[127] *Ibidem.*

[128] ECtHR 13710/88, Niemietz v. Germany; ECtHR 27798/95, Amann v Switzerland.

[129] *op cit* Eurofound. Employee monitoring and surveillance.

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

[131] *Ibidem.*

[132] ECtHR 13710/88, Niemietz v. Germany.

field for the development and fulfilment of one's own personality'.[133] Since Niemietz vs Germany, the ECtHR has expanded the scope of Article 8 of the ECHR in employment matters, however, the question how to determine whether the monitoring was excessive and in contradiction with employee's privacy is still under construction in case law.

The ECtHR case law dealing with employee privacy has relied on the 'reasonable expectation of privacy test'.[134] The notion of reasonable expectation of privacy is not new and has been shaped in US jurisprudence for years.[135] Today, this notion is the fulcrum on which employee monitoring cases in US turn and, therefore, a further explanation concerning US practice is discussed below.

US case law confirms that a reasonable expectation of privacy is an objective entitlement founded on broadly based and widely accepted community norms.[136] When considering invasion of privacy claims, courts generally weigh the employee's expectation of privacy against the employer's asserted business purposes for monitoring its employees.[137] When it comes to privacy expectations for employees, many courts have found that employees do not have a reasonable expectation of privacy when employer-owned equipment or technology is involved, the employer has a legitimate business interest, and the intrusion occurs during normal work hours.[138] Courts have recognized that lack of notice and consent typically support employees' invasion of privacy claims.[139] Therefore, in the US, the case law often concentrates on information distribution. For example, in United States vs Simons, the court held that employees do not have a reasonable expectation of privacy regarding their use of the internet when the employer has policies in place that allow to 'audit, inspect, and/or monitor' employees' internet use.[140] However, scholars in the US are not ready to accept this approach as final. According to experts, future research agenda needs to further define 'a reasonable

---

[133] ECtHR 6959/75, Bruggemann and Scheuten v. Federal Republic of Germany.

[134] ECtHR 20605/92, Halford vs The United Kingdom; See also Bygrave, L. A. Data Protection Pursuant to the Right to Privacy in Human Rights Treaties. – International Journal of Law and Information Technology 1998/6 (12).

[135] Katz v. United States, 389 U.S. 347 (1967). The Court's test to determine whether a defendant had a 'reasonable expectation of privacy' in a given area involves a two-step inquiry: (1) whether the individual 'exhibited an actual (subjective) expectation of privacy'; and (2) whether that expectation is 'one that society is prepared to recognize as reasonable.'

[136] Gonzales v. Uber Techs., Inc., 305 F. Supp. 3d 1078 (N.D. Cal. 2018).

[137] Swaya M. E., Eisenstein, S. R. Emerging Technology in the Workplace. – The Labor Lawyer 2005/21 (1).

[138] *op cit* Ajunwa, I., Crawford, K., Schultz, J.; Tsao, C. L., Haskins, K. J., Hall, B. D. The Rise of Wearable and Smart Technology in the Workplace, ABA National Symposium on Technology in Labor and Employment Law 2017.

[139] *op cit* Swaya M. E., Eisenstein, S. R.

[140] U.S. v Simons, 206 F.3d 392 (4th Cir. 2000).

expectation of privacy' for employees.[141] According to Ajunwa, as employees are obliged to interact with emerging technologies in the workplace, the question of what constitutes or should constitute a reasonable expectation of privacy for employees remains an important one for legal scholars in the US.[142] Also, the US Supreme Court has emphasized that modern communications technology and its role in a society is still evolving. In City of Ontario vs Quon, the court stated that it is difficult for them to predict how employees' privacy expectations will be shaped by technological changes or the degree to which society will be prepared to recognize those expectations as reasonable.[143] As the court explained, the more pervasive and essential or necessary digital monitoring technology becomes for an individual's self-expression or identification, the stronger is the case for an expectation of privacy.[144]

Similarly to the US case law, the main criteria established by the ECtHR to assess if an employee has a reasonable expectation to privacy under Article 8 of the ECHR is knowing whether the employer had warned the employee in advance about the existence of the monitoring measures.[145] This means that the employee's reasonable expectation of privacy may be limited by a notification, privacy policy or implied conditions of an employment contract. This leads to the conclusion that if employee is aware of monitoring activities, it is not reasonable for them to expect that their activities will be private. From the perspective of the employer, a notification, policy or a contract may be used to set clear boundaries for the employees. However, as noted by Abril et al., employers should be particularly careful in that written policies must be carried out, enforced consistently and incorporated into the organization's culture to form the rational foundation of employees' privacy expectations.[146] Otherwise, as argued by Broughton et al., the mere existence of a policy may not be sufficient, as policies can be too broad, ambiguous or unwise[147] and it is not self-evident that employees find the time to examine them.[148] According to Otto, reliance on prior notice shows the weakness of the ECtHR case law, as the existence of a policy or a notice should not cancel employees' right to privacy.[149] Similarly, as explained by Ford, the approach taken

---

[141] *op cit* Ajunwa, I., Crawford, K., Schultz, J.; Anderson, A., Private Government: How employers rule our lives (and why we don't talk about it). Princeton University Press 2017.

[142] *op cit* Ajunwa, I., Crawford, K., Schultz, J.

[143] City of Ontario, California *et al*. vs Quon *et al*., 560 U.S. 746 (2010).

[144] Ibidem.

[145] ECtHR 62617/00, Copland v. the United Kingdom; ECtHR 420/07, Köpke v Germany; ECtHR 61496/08 Bărbulescu v Romania.

[146] *Op cit* Abril, P. S., Levin, A., Del Riego, A.

[147] Broughton, A., Higgins, T., Hicks, B., Cox, A. Workplaces and social networking – The implications for employment relations. Brighton: Institute for Employment Studies, 2009.

[148] Lamoureux, S. Implementing the General Data Protection Regulation. The experiences of three Finnish organizations. Master's thesis in Governance of Digitalization. Åbo Akademi 2020.

[149] *Op cit* Otto, M.

by the court enables privacy to be set aside by management decisions, considering that an employer who informs employees that they are monitored removes any expectation employees had of privacy.[150] In publication II, interviews with the employees revealed that although there were social media guidelines and policies in some of the interviewees' organizations, not a single interviewee was actually well informed about the content of these documents. In a majority of cases, interviewed employees had simply forgotten the content of these documents, but there were also some who said they had never even read the guidelines. To conclude, it would appear unjust to leave employees without privacy protection solely over the fact that a notice, policy or a contract clause warned them of possible invasive monitoring activities. Mere notification would probably not justify invasions into employee's privacy using technologies that enable covert and continuous monitoring at work.

2.3 Balance of interests

Recent case law has taken a step back from the reasonable expectation of privacy test by classifying it as 'a significant though not necessarily conclusive factor' to decide on the existence of an interference with private life.[151] In a 'a landmark privacy ruling'[152] Bărbulescu vs Romania, the court reduces the ambiguity surrounding the legality of employee monitoring and emphasizes that the employee should also be allowed a certain degree of personal life at work as the employer's instructions cannot reduce private social life in the workplace to zero.[153] In this case, the ECtHR carries out a proportionality test by balancing the interests at stake, and in doing so provides instructions on the factors that need to be considered when balancing the interests of employers and employees. More specifically, in Bărbulescu vs Romania, the ECtHR gives a number of relevant criteria for domestic courts to assess when dealing with monitoring cases, which can be summarized as follows: (i) the existence of prior notification on the possibility that the employer might take measures to monitor the employee, and of the implementation of such measures; (ii) the extent of the monitoring by the employer and the degree of intrusion into the employee's privacy; (iii) legitimate aim pursued by the employer that could justify the monitoring; (iv) if it would have been possible for the employer to establish a monitoring system based on less intrusive

[150] Ford, M. Article 8 and the Right to Privacy at the Workplace. In Ewing K. D. (ed) Human Rights at work. Institute of Employment Rights 2000.

[151] ECtHR 420/07, Köpke v Germany; ECtHR 61496/08 Bărbulescu v Romania.; ECtHR 70838/13, Antović and Mirković v Montenegro.

[152] European court sides with worker in landmark privacy ruling. Deutsche Welle 2017. – http://www.dw.com; Wilhelm, E. O. Bărbulescu ruling: Workplace privacy is alive and kicking, IAPP Privacy Tracker 2017. – https://iapp.org.

[153] ECtHR 61496/08 Bărbulescu v Romania.

methods; (v) the consequences of the monitoring for the employee subjected to it and (vi) if adequate safeguards had been provided to the employee.

Clearly, the balancing of the interests gives a better chance for employees to protect their privacy as it gives more protection besides the preliminary formality of a prior notice. However, the test given in Bărbulescu vs Romania is not without its faults when considering the digital monitoring technologies used at work. One fault is because it once again emphasizes prior notice as one of the first and main criteria when considering whether monitoring is privacy invasive or not. That makes the role of the privacy notice in future cases unclear – will it be only one element discussed in the case or will it still have significant impact on the court's decision? Secondly, the ECtHR also takes into consideration the intrusiveness of the monitoring measure and whether there are other equally effective ways for the employer to monitor employees. In the context of digital monitoring technologies, this seems to be a crucial factor when deciding if the practice is privacy invasive or not. However, the notion of intrusiveness can also be criticized as being too vague in the context of digital monitoring technologies. For example, should social media monitoring be compared to more traditional methods of hiring (such as an interview) or would it matter that the search was carried out in, for example, social media accounts meant for professional activities (such as LinkedIn)? As another example, it is unclear how an employer should ascertain the intrusiveness of microchips, which are used to enter the premises in lieu of keys, access cards or other similar devices. Due to these questions, it is not clear how the ECtHR would classify digital monitoring technologies such as social media monitoring and monitoring microchipped employees in terms of their intrusiveness compared to other methods of monitoring. With foresight, the Court has concluded that 'the competing interests concerned might well be given a different weight in the future, having regard to the extent to which intrusions into private life were made possible by new, more sophisticated technologies'.[154] The court makes it evident that the more pervasive and insidious the monitoring deployed, the stronger the legitimate aim pursued has to be. Although court practice is forward-looking, ultimately the digital monitoring technologies do not comfortably fit in with the criteria introduced by the court. Therefore, legislators, judges, employers, and employees are left without a clear direction how to regulate, judge, and manage possibly invasive monitoring activities.

2.4 Elements of the balancing test

In this section, analysis of other significant ECtHR cases concerning employee monitoring is carried out, a hypothetical case in the context of digital monitoring technologies is compiled and components of the balancing test are more closely discussed to better understand the protection offered by the ECHR.

[154] ECtHR 420/07, Köpke v Germany.

Indeed, the court has showed in numerous cases[155] what an employer should do when carrying out monitoring measures on employees; however, these solutions may not be suitable in the case of digital monitoring technologies. In Köpke,[156] for example, the court noted that monitoring struck a fair balance between the different interests at stake as the covert video surveillance was targeted to specific employees, limited in time, processed by a limited number of people, and only used for specific purposes. Although reasonable in the case of video surveillance, the judgement shows its constraints when considered in another context, such as microchips. For instance, it would be impossible to limit the use of microchips only for a specific period of time, as employees cannot easily remove or switch off the chips. In these cases, the court should probably analyse what information is gathered with the help of the microchip (e.g. access times, movements, health data from the chip) and rely mostly on the legitimate aim and necessity of processing that would justify an intrusion.

In another case, López Ribalda and Others vs Spain[157], the ECtHR decided that Article 8 of the ECHR had been violated as employees were not informed about the covert video surveillance, the surveillance was not directed towards specific individuals (surveillance affected all the employees) and was relentless, having lasted for a disproportionate period of time (covered all working hours). However, the court also stressed that the intrusion on employees' private life could have been mitigated if, for instance, the employer had informed employees about the existence of the monitoring. More specifically, the court pointed out that the provision of information to the individual being monitored and its extent constitute one of the criteria to be taken into account in order to assess the proportionality of a monitoring measure. However, the court also stated that if such information is lacking, the safeguards deriving from the other criteria will be all the more important. With this statement, the court highlighted the essentiality of information when assessing the legality of employer's actions. The reasoning in this case is questionable in the context of employee monitoring as the court once again focuses on the formality of prior notification. Fortunately, the court further stressed that the monitoring of employees can be justified when there is a reasonable suspicion of serious misconduct. This reasoning of the court makes it possible to argue that possibly in future cases where the employee is suspected of minor wrongdoing, the court will find covert monitoring privacy invasive (even if there is a prior notice).

Let us now analyse a hypothetical case concerning social media monitoring to better understand the possible shortcomings of the circumstantial and broad case law of the ECtHR. In this hypothetical case, an employer has used social media monitoring for selecting job applicants, limited its activities to a specific period, targeted specific applicants and used monitoring only for hiring purposes. At first

---

155 ECtHR 420/07, Köpke v Germany; ECtHR 70838/13, Antović and Mirković v Montenegro.

156 ECtHR 420/07, Köpke v Germany.

157 ECtHR 1874/13 López Ribalda and Others v Spain.

glance this practice seems to be in conformity with the ECtHR case law as the monitoring may not seem particularly intrusive and the employer has a legitimate aim. As discussed in my publication I, even if the information that an individual places on social networking site is personal or protected, many are convinced that a person waives an expectation of privacy to that information when they post it on a social networking site.[158] According to Warren and Brandeis, the right to privacy ceases upon the publication of the facts by the individual.[159] US courts have also expressed a disinclination to find rights to privacy in online information and according to some US scholars, internet postings are not considered private since they are available to the general public.[160] Similar ideas are also predominant among employers, as discussed in my publications I and II. Empirical studies carried out in Estonia reveal that employers believed information on social networking site is publicly available and may hence be browsed by them without any restrictions.[161] On the other hand, I argue in my publication I that compromising applicants' privacy on social networking site may result in various types of harm and might, therefore, intrude into employee's privacy as discussed below.

Therefore, to understand the invasion into employee's privacy in this hypothetical case of social media monitoring, it is also important to discuss the harm that this type of monitoring may cause. According to Van der Hoeven and Weckert, harm that may arise as a result of the compromise of privacy protections is information injustice – i.e. information presented in one context is used in another.[162] Therefore, negative information conveyed through the applicant's personal profile may not be considered in the proper context, and could result in a hasty rejection decision.[163] Furthermore, social networking sites represent an extensive source of information that may be able to reveal untapped job-relevant (and job-irrelevant) applicant characteristics. For example, an internet search might reveal job-irrelevant information about the applicant's political activities, national origin, sexual preferences and other information that might not arise during a traditional background check. The use of internet screening for selection may therefore lead employers to use the available information on public profiles to discriminate against applicants on the basis of protected class information (e.g. religion, race, sexuality etc.)[164], but also due to applicants' lifestyle and

---

158 *op cit* Introna, L. D., Pouloudi, A.

159 *op cit* Warren, S. D., Brandeis, L. D.

160 Sprague, R. Invasion of the Social Networks: Blurring the Line between Personal Life and the Employment Relationship. – University of Louisville Law Review 2011/50.

161 Publikatsioon II; *op cit* Ivask, E.-L.

162 Hoven, J.vd., Weckert, J. (Eds) Information Technology and Moral Philosophy. New York: Cambridge University Press 2008.

163 o*p cit* Brown, V. R., Vaughn, E. D.

164 Davison, H. K., Maraist, C.C., Hamilton, R. H., Bing, M.N. To Screen or Not to Screen? Using the Internet for Selection Decisions. – Employee Responsibilities and Rights Journal 2012/24 (1); Valentino-DeVries, J. Bosses May Use Social Media to Discriminate Against Job Seekers. – The Wall Street Journal 20.11.2013.

behaviour (e.g. personal relationships, political activities, daily habits, etc.) – when lifestyles clash with employers' interests, 'lifestyle discrimination' can result.[165] Also as discussed in publication I, information on social networking sites may vary considerably, which makes comparison between applicants unreliable. Shared information on social networking sites might be distorted by social desirability or high levels of self-monitoring and social networking sites may contain inaccurate information. Despite these different harms that might occur, the interviews with Estonian employers indicated that they rarely saw any ethical dilemmas when conducting such checks and information found from social networking sites truly affected the applicant's ability to be hired (see publication II).

Finally, let us draw conclusions from this discussion. The harm that may arise through social media monitoring or other digital monitoring technologies when privacy protection is compromised is alarming. Due to the available information, employers are often able to investigate and monitor various pieces of data that are out of context, inaccurate, irrelevant, and unreliable. Furthermore, the issue is substantial as employers rely on AI tools to extract and sort the information. For these reasons, the ECtHR should take into consideration possible harms of digital monitoring technology when assessing if a monitoring activity infringes on an employee's privacy. Possible harms that should be considered include information injustice, digital monitoring technologies are an extensive source of information and may possibly reveal job-irrelevant information, data obtained by digital monitoring technologies may vary considerably and be inaccurate. Also, the question of necessity – whether the information available from digital monitoring technology is even relevant to the job performance or not – should have more weight when discussing these technologies. This question can be looked at the light of judgement Pay vs UK, where the court noted that the mere fact that the monitoring activities did not take place in an entirely private forum could not be sufficient to constitute a waiver of the employee's Article 8 rights.[166] Potentially, this judgement – which endorses the employee's right to privacy outside work and working time – may help in the future cases that concern employer monitoring activities that reveal off-duty behaviour of employees (such as monitoring employee's social media accounts). However, it is mere conjecture for now how cases related to social media monitoring will be ruled on in the future.

To conclude, although the ECtHR sets the direction for the future assessments of the legality of employee monitoring, it also poses unanswered questions concerning digital monitoring technologies. As discussed in this dissertation, ECtHR case law regarding monitoring of employees is extensive and trend-setting. However, the judgements are still limited in scope and based on specific monitoring situations. Today, the ECtHR has expanded the reach of private life

[165] Sugarman, S. D. Lifestyle Discrimination in Employment. – Berkeley Journal of Employment and Labor Law 2003/24 (2).

[166] ECtHR 32792/05, Pay v UK.

to telephone conversations,[167] video surveillance[168] and internet messaging applications.[169] So far, the court has yet to analyse other forms of monitoring. As the ECtHR gives assessment on a case by case basis, researchers argue that the case law has led to establishing subjective expectations of privacy in specific circumstances.[170] As described by Otto, the protection afforded by the ECtHR is highly circumstantial and largely dependent upon the employer's policies and practices.[171]

Due to extensive remote work during the COVID-19 pandemic, employers' interest in using various digital monitoring applications grew considerably, making these issues related to employees' privacy more pressing than ever. As digital monitoring technologies give employers the ability to gather various data concerning employees on a large scale, their use could probably have a chilling effect on privacy. Although the test in Bărbulescu vs Romania is a step in the right direction, it remains to be seen what components in that test will be used in future cases. Reliance on prior notice should lose its importance and intrusiveness of monitoring show the need to regulate employee monitoring practices in a more precise and comprehensive way. Also, other factors should be added in the balancing test so that it is better suited for digital monitoring technologies (such as possible harms of digital monitoring technology and necessity of monitoring). Pending further cases, digital monitoring technologies will rapidly grow and become more efficient in workplaces and the jurisprudence will lag behind. Today's broad ECtHR case law is unlikely to be enough to effectively protect employees from privacy intrusions from digital monitoring technology.

[167] ECtHR 20605/92, Halford vs The United Kingdom.

[168] ECtHR 420/07, Köpke v Germany.; ECtHR 70838/13, Antović and Mirković v Montenegro.

[169] ECtHR 61496/08 Bărbulescu v Romania.

[170] Oliver, H. E-mail and Internet Monitoring in the Workplace: Information Privacy and Contracting-Out. –Industrial Law Journal 2002/31.

[171] *op cit* Otto, M.

3. Protection of employee's privacy under the GDPR

3.1 Significance of the GDPR

If an employer processes EU employee personal data obtained via digital monitoring technology, compliance with the GDPR's data protection rules will need to be considered. Researchers have argued that the GDPR coupled with ECtHR judgement in Bărbulescu vs Romania amounts to a coherent framework ensuring workplace privacy.[172] However, as the ECHR and its case law gives guidance but does not really address the digital monitoring technologies used in workplaces, it is even more important to look at more specific data protection rules as part of privacy enacted in the GDPR. The next subchapters are therefore dedicated to discussing the applicability of the GDPR and allowing a better understanding of employees' rights to data protection if an employer uses digital monitoring technologies. More specifically, in the next sections I discuss under which conditions the GDPR applies if an employer uses digital monitoring technologies. I also question which monitoring practices used by employers in the digital workplace under the GDPR could potentially invade privacy and data protection rights of employees and ask which monitoring practices used by employers in the digital workplace do not fall under the scope of the GDPR but should nevertheless be regulated to protect employees' privacy.

3.2 Processing employee data

As the GDPR applies to processing of personal data, its scope is dependent on two notions – 'processing' and 'personal data'. Hence, for the GDPR to be applicable, the employer's monitoring activities have to amount to the processing of employee personal data. Pursuant to Article 4(2), the definition of 'processing' is broad, enabling the GDPR to regulate an indefinite number of activities performed on personal data to fall under its scope, such as collection, recording, organization, structuring, storage, use, disclosure, dissemination, erasure and so on. In fact, it is difficult to think of anything an employer might do with employees' data that would not be considered as processing. The 'processing requirement' is therefore readily ascertained in all monitoring activities as the notion encompasses every kind of operation possible on personal data. In the context of digital monitoring technologies, it is important to note, that the term 'processing' covers various operations on data regardless of the technical means used.[173] The GDPR also specifies that it 'applies to the processing of personal data wholly or partly by automated means' and, therefore excludes from its scope of application processing operations performed without automated means.

---

[172] *op cit* Esfola, J. P. M.

[173] CJEU C-101/01, Bodil Lindquist

The main discussion and concern here is related to the availability of increasingly powerful tools that enable processing and analysis of information concerning individuals (also referred as 'people analytics'). The rise of AI in general, and machine learning in particular, enables probabilistic analyses of large datasets, relying on sophisticated statistical modelling to spot patterns or correlations in the data.[174] In addition to the sheer quantity of information that can be captured and enables algorithmic management of employees, the traditional boundary between the workplace and individuals' private lives is also rapidly breaking down. New sources of information can reveal patterns far beyond traditional employer concerns. Information about an employee's weekend activities harvested from a social media profile can be combined with data from a wearable technology that measures Monday morning productivity. The increasing trend of self-monitoring with the use of fitness trackers or health-apps on smart phones, has created possibilities to combine the result of self-monitoring with data gathered in the workplace.[175] As argued by Mascheroni and Siibak, the users of health apps often 'simply cannot imagine that their mundane everyday practices and the data these evoke could be of any use to anyone'.[176] Mascheroni and Siibak emphasize that it is crucial to acknowledge that the practice of self-monitoring reproductive health tracking apps invite, cannot be separated from the discussions about the capitalist data relations and the considerable risk to privacy they pose. According to an article published in *The Washington Post*, for example, popular menstrual cycle tracking apps (e.g. Ovia) have been found sharing user data (e.g. current trimester; the average time it took employees to get pregnant; the percentage who had high-risk pregnancies etc) with employers, indicating that the data traces collected through these apps can be used for making various assumptions and conclusions in the employment context.[177] Taken the above practices into consideration, it is important to note that the GDPR does not distinguish processing activities where data collection is limited from other activities were increasingly powerful tools can process and analyse information concerning employees and spot patterns or correlations in their data. These data practices significantly influence employment relationships and communication between employer and employee, therefore making it important to consider whether specific EU legislation is needed to protect employees from unnecessary and excessive monitoring. For example, all the data processing activities often associated with digital monitoring technologies, such as collecting the location data of employees, looking for patterns in work settings, gathering information concerning employee's

[174] Polson, N., Scott, J. AIQ: How Artificial Intelligence Works and How We Can Harness its Power for a Better World. – Bantam Press 2018.

[175] *op cit* Prassl, J; Neff, G., Nafus, D. Self-Tracking. MIT Press Essential Knowledge series, 2016.

[176] Mascheroni, G., Siibak, A. Datafied childhoods: data practices and imaginaries in children's lives. New York: Peter Lang 2021.

[177] Harwell, D. Tracking your pregnancy on an app may be more public than you think. – The Washington Post 10.04.2019.

private life (e.g. health information from a contact tracing app) and using AI generated datasets and algorithmic management fall under the scope of the GDPR and, therefore in principle, are allowed if the employer has legitimate grounds for processing (see also subchapter 3.2). Hence, it can be argued that the GDPR allows for monitoring practices that are in accordance with the GDPR but still could potentially invade privacy and data protection rights of employees.

It is questionable whether all these processing activities and data received as a product of such monitoring should be allowed in the context of employment. The breadth of the GDPR may also be considered its weakness when analysing employee monitoring. For example, in Finland employers can process only personal data that are directly necessary for the employment relationship, thus limiting the scope of monitoring activities.[178] Some countries have prohibited the use of more intrusive digital monitoring technologies or allowed their use to a certain extent and others have made covert monitoring unlawful.[179] Similarly, European Parliament should clarify the scope of employee data processing and employee monitoring. For example, EU legislation should clearly indicate that if not necessary, employers should refrain from the use of digital monitoring technology for the purpose of monitoring particular employees in the workplace. Using digital monitoring technologies might be allowed only in case of criminal activities or serious wrongdoing or other just causes such as prevention of accidents at work.

3.3 Identifiable data

The other criterion established in Article 4(1) that triggers the applicability of the GDPR is 'personal data', defined as 'any information relating to an identified or identifiable natural person'. The concept of personal data is broad and comprises all kinds of information, regardless of their objectiveness or format. Therefore, personal data covers a wide range of information and also accommodates data relating to 'working relations or the economic or social behaviour of the individual'.[180] With the increasing use of digital monitoring technologies, employers have readily available different sources of data and are able to collect new types of data. Today, data can be collected at a greater level of granularity and scale than ever before.[181] However, as discussed by Kitchin, the collection, processing and use of personal data is ethically, politically, socially and legally complex and

[178] Act on the Protection of Privacy in Working Life (759/2004). – http://ilo.org/dyn/natlex (18.08.2021).

[179] *op cit* Eurofound. Employee monitoring and surveillance.

[180] Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. 2007 01248/07/EN WP 136.

[181] *op cit* Eurofound. Employee monitoring and surveillance.

it is difficult to draw a clear line between 'good' and 'bad' personal data,[182] which leaves employers the possibility to process all kinds of data obtained via digital monitoring technologies.

According to Prassl, there are three broad sources of data in the modern workplace: digital information, sensors, and the growing trend of employee self-tracking.[183] For example, personal data can be verified or come from an opinion or assessment[184] expressed in a social media profile or become available with the increasing use of devices endowed with sensors/readers (such as microchips) that capture every piece of information available about the surrounding work environment. Today a wide range of 'embodied computing devices' – technologies that exist in topographical (on the body), visceral (in the body), and ambient (around the body) relationships with the body – are available and enable to assist the individual in collecting, managing, and preserving various kinds of personal information.[185] Also, with the help of large number of providers employers are able to capture employees' digital activities, from keystroke logs to screenshots taken at regular intervals.[186] However not all data captured with these digital monitoring technologies falls under the scope of the GDPR.

It is important to note that the GDPR is applicable if the individual is directly or indirectly identifiable. According to Pangrazio & Selwyn, personal data is referred to as any 'personally identifiable information'.[187] Westerlund defines personal data in the light of the GDPR, stating that '[p]ersonal data is characterized as only such data that can be linked to a natural person.'[188] Hence, personal data is information that is linked to a living individual and can, on its own or combined with other information, lead to the identification of that individual. Therefore, in order for the GDPR to be applicable, digital monitoring technologies (such as contact tracing apps, wearables, or microchips) have to give out information that is linked to an employee and can, on its own or combined with other information, lead to the identification of that employee. However, regardless of the existence of a legal definition, identifying which information constitutes personal data or even understanding when employers receive personal data in the context of digital monitoring technologies is not a clear-cut exercise. As discussed in publication III, in the case of microchips, the question of personal identifiable data can be a crucial one, as due to different types of technology, the

---

[182] Kitchin, R. The data revolution: Big data, open data, data infrastructures & their consequences. London 2014.

[183] *op cit* Prassl; *op cit* Neff, G., Nafus, D.

[184] Article 29 Data Protection Working Party. Opinion 4/2007.

[185] Pedersen, I., Iliadis, A. (Eds.) Embodied computing. Wearables, implantables, embeddables, ingestibles. The MIT Press 2020.

[186] *op cit* Prassl.

[187] Pangrazio, L., Selwyn, N. 'Personal data literacies': A critical literacies approach to enhancing understandings of personal digital data. – New Media & Society 2019/21 (2).

[188] Westerlund, M. A Study of EU Data Protection Regulation and Appropriate Security for Digital Services and Platforms. Åbo: Åbo Akademi University Press 2018.

employer may or may not have access to personal data. Hence, the applicability of the GDPR depends on what data is accessible from the digital monitoring technology to the employer and what form the data is collected and stored in.

According to Poullet, data obtained by digital monitoring technologies can be divided between primary and secondary digital identifiers.[189] She argues that due to technological developments, employers are today not only able to receive primary identifiers directly connected to the person (e.g. name, address, mobile phone number, password), but also often get access to secondary identifiers that are indirect but based on known information concerning the individual as 'cookies', IP addresses or RFID tag numbers, while not necessarily known to the employee, can be associated with an employee or a site or object with which the employee is connected.[190] Similarly, as I also argued in publications III and V, digital monitoring technologies (such as microchips and contact tracing technologies) can collect personally identifiable information that is available to the employer (specifically if the app/wearable/microchip has been developed in collaboration with an employer or sourced specifically for contact tracing in a workplace) and trigger the applicability of GDPR. The applicability of the GDPR in respect to digital monitoring technologies is illustrated below by two examples – using microchips and contact tracing to monitor employees.

Microchips may be possible sources of employee's personal data. As discussed in publication III, RFID systems may be structured so that the employer does not retrieve any personal information about the employee. However, there are several ways that the data contained on a chip may become personal data. This possibility is also suggested in recital 30 of the GDPR, which does not mention microchips, but clearly states that natural persons may be associated with online identifiers provided by their devices, applications, tools, and protocols, such as RFID tags. As analysed in publication III, microchipping enables the processing of employees' personal data in two ways. Firstly, the chip itself may contain information about the employee. In other words, the chip can function as an information carrier, storing data such as the person's name and address, age or medical condition.[191] Furthermore, a photograph, a fingerprint or a retinal scan may also be included, which would enable facial or biometric identification.[192] When information about an employee is stored on the chip, it is beyond doubt that this information qualifies as personal data. Secondly, and more commonly, the chip only contains a unique number.[193] This unique number is useless as a piece of data in isolation. However, the Court of Justice of the European Union

---

189 *op cit* Poullet, Y.

190 *Ibidem.*

191 Halperin, D., Heydt-Benjamin, T. S., Fu, K., Kohno, T., Maisel W. H. Security and privacy for implantable medical devices. – IEEE Pervasive Computing 2008/7 (1).

192 *op cit.* Graveling, R., Winski, T., Dixon, K.

193 Fischer-Hübner, S., Hedbom, H. (Eds.) FIDIS Deliverable D12.3*:* A Holistic Privacy Framework for RFID Applications 2008.

has ruled that a dynamic IP address can be personal data.[194] So the question arises whether a unique chip identifier can be regarded in a similar manner. In the case of microchipping, the backend system typically incorporates a database allowing the matching of the data on the chip to other stored information or storing of the data itself.[195] The unique number becomes relevant if it can be linked to an employee and the employee is eventually identifiable with the help of data stored in a database.[196] In such a case, the information would be considered personal data and the GDPR would apply. Therefore, either personal data are directly stored on the chip or can be indirectly linked to an employee by combining the chip's unique number with data stored in a backend system. If data from microchips is linked to an employee who is identified or identifiable (today or in the future), it will become personal data and the processing of their data will fall in the scope of the GDPR. However, it is questionable whether this information received from the microchip should be used to monitor employees without a serious cause as the microchip may enable the gathering of various amounts of detailed data concerning the employee. As privacy is the right to anonymity and solitude and the possibility to withdraw from others (see subchapter 2.1), this form of digital monitoring can be considered too privacy invasive.

Contact tracing technologies may also be possible sources of employee's personal data. As discussed in publications IV and V, contact tracing apps and other technologies that were introduced to mitigate the spread of COVID-19 gather lots of different data. More conventional personal data that might be involved includes identity data such as the user's name, address, gender, contact details. Contact tracing apps and other technological solutions may also process data such as health data (whether the user has tested positive to the virus or not) and location data or social/proximity graphs that give indication of the interactions between users and the people they came into close contact with.[197] However, depending on the user of the contact tracing app, type of the technology, e.g. the architecture and salient features of the app[198], employers may or may not receive personal data of employees. The choice is often left to employers, who may choose what data to collect. For example, Onspota developed the Shield For Business app, which enables organizations to define what employee data is collected for the purpose of identifying that employee. Some companies ask that employees be identified by name and phone while other companies want their employees identified by a number.[199] Other Bluetooth contact tracing apps broadcast anonymous 'chirps' or 'keys' from the phone. These keys change frequently,

---

[194] CJEU C-582/14, Patrick Breyer v Bundesrepublik Deutschland.

[195] *op cit.* Gille, D., Wohlgemuth, S., Strüker, J.

[196] *op cit.* Roosendaal A. P. C., Kosta, E.

[197] Nadeem, A. *et al*. A Survey of COVID-19 Contact Tracing Apps. – IEEE Access 2020/8.

[198] Ajmal, A. M. *et al.* A First Look at Privacy Analysis of COVID-19 Contact Tracing Mobile Applications. – *IEEE Internet of Things Journal* 2020, arXiv:2006.13354 [cs.CR].

[199] Shemer, S. Could A New Israeli App Help Tackle COVID-19 Tracing In the Workplace? – NoCamels 24.01.2021.

possibly every few minutes. If two phones running an app come in close enough contact for a long enough period of time, then the two phones exchange keys.[200] Scholars have said that these unique identifiers, although encrypted, could also be linked to the natural person and most likely meet the GDPR definition of personal data.[201] However, if the employer does not receive these unique identifiers or users are assigned a randomly generated identifier that does not reveal any personal information about them,[202] the applicability of the GDPR is not triggered. This is also the most privacy friendly solution. Again, in the case of this digital monitoring technology, employers should only receive employee's personal data in cases where it is necessary (e.g. to mitigate the spread of deadly disease in the middle of a pandemic).

In addition, as information is increasingly organized in machine-readable formats, researchers note that information that may be collected and stored in anonym zed form can easily be combined from different sources of data to build large employee databases, and in principle identify employees.[203] In these cases, where the analysis of the movement patterns reveals the employee's identity (e.g. implanted employee is demanded to perform tasks in a specific location in the workplace), the GDPR should apply even if the employer uses anonymization techniques. For example, as discussed in publications III and V, contact tracing and RFID enabled systems (such as microchips) may also record the instances when a person is present in a specific room every day and from there on it can readily be assumed who the person is. Thus, when technologies are used for their ability to monitor location and if the traced employee is performing their tasks in a specific workplace, it is also possible that, through the analysis of employee's movements, their identity would become known.

To conclude, the GDPR with its broad wording is applicable to digital monitoring technologies if they encompass personal data and the employee is identifiable, which is often the case. However, identifying which information constitutes personal data or even understanding when employers receive personal data in the context of digital monitoring technologies is a complicated exercise. Today it is possible to distinguish between primary and secondary digital identifiers, where the first is relatively easy to understand as it is directly connected to the person (e.g. name, address, mobile phone number), but the latter identifiers are much more hidden as they are indirect (e.g. 'cookies', IP addresses, RFID tag numbers). Digital identifiers are not necessarily known to the employee; however, they can be associated with an employee or a site or object with which the employee is connected. Contact tracing apps, microchips and other technological solutions that use these secondary identifiers may also process various amounts of other

---

[200] Brown, S. R., Linden, M. F., Sullivan, E. J., Torres. J. J. May an Employer Require Its Employees to Use a Contact Tracing App? Jenner&Bloc 24.04.2020. – https://jenner.com (31.07.2021).

[201] *op cit* Bradford, L., Aboy, M., Liddell, K.

[202] *op cit* Watkins, K.

[203] *op cit* Prassl.

data (e.g. health data, location data, behavioural data, social/proximity graphs, interactions between users and the people they came into close contact with) and do so covertly. These different identifiers make opaque monitoring an even greater possibility in the work environment than ever before and therefore EU legislation should be considered that enables employees to ascertain when and how monitoring is taking place. The monitoring activity should bring forth stricter obligations to employers (e.g. employer's obligation to give more detailed instructions to employees; special signs in a workplace to indicate were monitoring is taking place) or prohibition on using certain monitoring methods (e.g. prohibition of covert monitoring or the inability to gather movement data inside the workplace). Employees should also have a possibility to choose between 'new' and more 'traditional' monitoring methods (e.g. instead of apps that gather location data, employees may be identified by scanning a card at the entrance and exit). Also, employers should not be allowed to combine different sources of data obtained via digital monitoring technologies to build large employee databases that might reveal the employee's identity even if anonym zed.

3.4 Non identifiable data

In this subchapter, I discuss the possibility that the collection of data from unidentified individuals may also violate the employee's privacy. The GDPR is not applicable if the employer receives generalized unidentified information about employees. For instance, with the help of data from contact tracing apps, employers may get access to analysis of a specific room or workplace (e.g. location of users who tested positive for COVID-19 test that show high-level hotspots for COVID-19 infections) and overall health status of the workforce (e.g. which departments are experiencing COVID-19 symptoms). Although these methods of monitoring can be considered justifiable for the purposes of mitigating the spread of COVID-19, it is doubtful whether an employer should have the option of using similar monitoring methods in ordinary work conditions. Regardless of the fact that employees are not identified and the GDPR is not applicable, this practice can potentially invade the employee's privacy.

Technology enables detailed monitoring of an employee's life and behavioural patterns as increasingly sophisticated sensors allow the capture of physical and other information. For instance, Uber pioneered the use of its drivers' iPhones to measure how quickly individuals accelerate and/or break, thus capturing smooth and abrupt driving patterns.[204] Also, microchips, contact tracing apps or wearable devices that allow monitoring the location of employees, their movements, the duration of meetings and the level of interaction with colleagues may enable employers to uncover patterns on how teams work. Hence, these data collection practices can reveal vast amounts of information even if data is anonym zed and can be highly invasive as they are aimed at detecting personal elements. Further-

[204] *op cit* Prassl.

more, using anonym zed information, an employer may initiate activities and guidelines targeted at employees without necessarily knowing their identity. For instance, employer may use implanted employees' location data to release instruction campaigns based on the attendance of workplace cafeteria or rest areas, without associating the chip's behaviours with a specific employee but a group of employees. As discussed in publication V, similar techniques were also used during the COVID-19 pandemic to apply social distancing measures in the workplace. Also, in case of different tools and wearables that incorporate microphones and voice-pitches analysis, the mood of employees can be apprehended without actually recording the content of their conversations.[205] Unfortunately, these practices leave employees without the protection of the GDPR as anonym zed data does not fall into its scope of application (GDPR recital 26).

To conclude, the employee is left without protection concerning their data and privacy if the employer uses the data provided by digital monitoring technologies not to identify the employee concerned but simply to profile a computer, tool, room, or microchip owner in order to decide on certain actions in regard to the employee, such as control and guidance. Due to their possibly invasive nature, EU legislation should regulate the employer's monitoring activities that are aimed at profiling employees without identifying them. Employers should generally be prohibited from carrying out monitoring of an employee's life and behavioural patterns without a specific purpose (such as health and safety) that should be clearly stated in EU legislation.

3.5 Controller of data

An issue that comes up in connection with digital monitoring technologies is the status of the employer. In the context of the GDPR, the concepts of controller, joint controller and processor play a crucial role since they determine who is responsible for compliance with different data protection rules, and how data subjects can exercise their rights in practice.[206] Pursuant to Article 4(7) of the GDPR, data controller means the natural or legal person, which, alone or jointly with others, determines the purposes and means of the processing of personal data. In the case of joint controllership, two or more entities determine the purposes and means of a processing operation. An important criterion is that the processing would not be possible without both parties' participation in the sense that the processing by each party is inseparable, i.e. inextricably linked.[207] 'Data processor' means a natural or legal person which processes personal data on behalf of the controller (GDPR Article 4(8)). The differentiation is important as it is the

[205] Fischbach, K. *et al.* Analyzing the Flow of Knowledge with Sociometric Badges – Procedia – Social and Behavioral Sciences 2010/2 (4).

[206] *op cit* Bradford, L., Aboy, M., Liddell, K.

[207] EDPB. Guidelines 07/2020 on the concepts of controller and processor in the GDPR. 02.09.2020.

controller who bears responsibility for meeting the data protection obligations and may be held liable for data protection violations. Therefore, to ensure accountability, the identity of the controller of any monitoring technology should be clearly understood.

As key factors that can be emphasized in an employment relationship are control of the employer and subordination of employees[208], the controller of employees' data should by default be the employer. However, operations with personal data may not be dictated by the employer but instead dealt with by a third party. In fact, often the employer only partially or not at all controls the data and employees' data is handled by an employing enterprise, designers, or providers of a software product. As the required 'control' in the GDPR stems from 'factual influence', which requires assessing factual conditions of the case – e.g. why is processing taking place, who initiated the processing, who decides the means and extent of processing,[209] – even if personal data is handled by a third party on behalf of the employer, the employer should still be considered the controller of data. For example, as discussed in publication V, if the employer opted to use organization based technology as opposed to government-sponsored contact tracing apps to monitor employees and combat COVID-19 in the workplace, the employer is most likely the controller of the app and has greater data protection responsibilities in respect to any data generated by the app. This can be illustrated by the statement from a spokesperson for a contact tracing app maker, BrightHR: although the app collects data, that data 'belongs to the customer organization' – meaning, the company using the app – and therefore is subject to the company's own policies.[210] As a controller, the employer has to follow the rules of the GDPR (e.g. they must have legal justifications for data collection and follow the principles of data processing). This also means that if the employer outsources monitoring technologies, they need to choose processors (e.g. app developers) who can demonstrate compliance with the GDPR's data protection rules. For example, if an employer uses an external processor, it should be the employer's responsibility to verify that the processor handles the personal data as predefined through the purposes and means of processing.[211]

However, in practice, digital monitoring technologies and possibilities for algorithmic management diffuse responsibility[212] and it may be difficult to establish who determines the purposes and means of the processing of personal data. Furthermore, employees' self-tracking tools generate more confusion if they are used in workplaces due to the encouragement of the employer or on the

---

[208] Waas, B., van Voss, G. H. (Eds), Restatement of Labour Law in Europe: Volume I . Oxford: Hart Publishing 2017.

[209] Article 29 Data Protection Working Party. Opinion 1/2010 on the concept of 'controller' and 'processor'. 2010 00264/10/ WP 169.

[210] Johnson, E. School custodian refuses to download phone app that monitors location, says it got her fired. – CBC News 12.04.2021.

[211] *op cit* Westerlund.

[212] *op cit* Prassl.

employer's orders. As discussed in my publication V, the roles of controller and joint controller are not always clear-cut if an employer uses contact tracing technologies that are developed by government or large corporations for wider use. For example, during the spread of COVID-19, the national health authorities should be the controllers of personal data in the case of government-launched contact tracing apps, as they determine the purposes and means of data processing. However, employers may also wish to make use of government-launched contact tracing apps to assure the health and safety of their employees and clients. One way of doing this would be to ask employees whether they have the app installed on their smartphones and if so, what their status is (i.e. if they have received an infection alert). As discussed in publication V, the extent of an employer's responsibility for privacy in relation to such apps will depend on the role the employer takes. If the employer is relying on its employees to voluntarily pass on relevant information generated from contact tracing government-launched contact tracing apps, they are probably not controllers of data for the purposes of the GDPR as they do not determine the purposes and means of the processing. However, the role of employers inevitably becomes more complicated if they insist that employees download and use government apps as a workplace safety measure. In this instance, employers have a more active role; however, it is questionable whether they define the purpose and means of the processing and become controllers of the data for the purposes of the GDPR. Also, the employer might not receive any data from the technology (e.g. employer only monitors the existence of an app in employee's or company's phone) or might not process data with automated means and therefore the applicability of the GDPR is not triggered.

The monitoring activity discussed above – i.e., which is not in the scope of the GDPR – should be regulated to protect employee privacy rights. The requirement to monitor one's own health, working speed and time using wearables or apps seriously invades employee privacy as it interferes with the employee's right to withdraw on their own terms. Therefore, the employer should not have the right to require employees to use digital monitoring technologies such as apps, wearables or microchips to carry out self-controls without a serious cause (e.g. to prevent accidents in dangerous work environments or mitigate the spread of a contagious disease). I suggest that EU legislation should specify in which situations and under what conditions employers may require employees to use digital monitoring technologies such as apps or wearables (e.g. smart watches). To avoid ambiguities, EU legislation should clearly state that data collection from employee-owned sources (e.g. self-tracking app) is prohibited.

Another factor that complicates the issue of control is the widespread use of different forms of work and the greater numbers of 'atypical' or 'non-standard' employees.[213] The issue is not discussed further in this dissertation but deserves

[213] A vast literature on 'atypical work' has explored the problematic implications of this approach in work arrangements which deviate from the received paradigm of stable, open-ended employment for a single employer. See for example 1) International Labour Organisation, Non-Standard Employment around the World: Understanding Challenges, Shaping

special mention under the topic of data controllers as it may generate even more confusion as these different forms become more normalized. Examples include the 'fissuring workplace',[214] where employer control is exercised by multiple parties through outsourcing agreements, the use of temporary agency work, or complex corporate groups and false self-employment, where employer control is contractually denied through a fictitious independent contractor status.[215] Once the reality of control is thus camouflaged, employees may no longer enjoy access to data-protective norms.[216] These topics are not regulated in the GDPR, but should be also discussed and clarified in the case of employee monitoring.

Prospect. Geneva: International Labour Office 2016. 2) For an overview, see Albin, E., Prassl, J. Fragmenting Work, Fragmented Regulation: The Contract of Employment as a Driver of Social Exclusion. In Freedland, M *et al.* (Eds) The Contract of Employment. OUP 2016.

[214] Weil, D. The Fissured Workplace: Why Work Became so Bad for so Many and What Can Be Done to Improve it. Harvard University Press 2014.

[215] Bogg, A. Sham self-employment in the Supreme Court. – Industrial Law Journal 2012/41.

[216] *op cit* International Labour Organisation, Non-Standard Employment around the World.

4. Legal basis for data processing

4.1 Lawfulness of processing

The legal bases in Articles 6 to 10 of the GDPR[217] are a precondition for the processing of employees' personal data. Regardless of the monitoring technologies used, employers must first establish a legal basis for lawful processing of employees' data.

Opinions concerning these legal bases differ. From an employer's perspective, BusinessEurope has welcomed the variety of solutions and noted that the 'application of all legal data processing possibilities should be permitted instead of forcing one method'.[218] Hence, employers seem to prefer a broad approach where different legal bases can be used to collect data concerning employees. Still, notwithstanding the importance of legality of processing, some researchers have been critical of the generalized nature of these legal basis. For example, Otto has specifically drawn attention to certain ambiguity concerning the actual scope of rather broadly termed legitimacy premises.[219] Indeed, the principle of lawfulness offers a first set of protection to the employee if workplace monitoring is used, and the employer has several possible legal justifications to process employees' personal data (also health data) obtained via digital monitoring technologies used at workplaces. However, as argued in publications IV and V, the myriad of possibilities also causes confusion and finding a legal basis to lawfully monitor employees can be challenging. For example, as discussed in publication IV, during the spread of COVID-19, the EDBP and national data protection authorities referred in their guidance to almost all legal bases enacted in the GDPR as relevant, gave sometimes contradictory explanations and left it up to employers to choose the legal basis suitable or convenient for them. Furthermore, as brought out in publication II, majority of the interviewed employers stated that the use of digital monitoring technology (in that case social media monitoring for pre-employment screening) had become such a routine practice that most of them never considered the need for any legitimate grounds for data processing. These practices and concerns highlighted above bring forward the need for a closer analysis of legal bases enacted in the GDPR. The next subchapters therefore concentrate on legal bases to better understand how they are used by employers in digital workplace. More specifically, the discussion focuses on the question of which legal bases used by employers in the digital workplace to monitor employees under the GDPR could potentially invade the privacy and data protection rights

[217] The list of legal bases in the GDPR is exhaustive – when none of them applies, the collecting and processing of personal data is not allowed. See also Article 29 Data Protection Working Party. Opinion 8/2001 on the processing of personal data in the employment context. 2001 5062/01/EN/Final WP 48.

[218] BusinessEurope. The GDPR in review: A good start but improvement necessary. Press release 24.06.2020. – https://www.businesseurope.eu (18.08.2021).

[219] *op cit* Otto, M.

of employees. The four main legal bases discussed in the next subchapters that may justify employee monitoring are data processing under employment contract (Article 6(1)(b) GDPR), under legal obligation (Article 6(1)(c)), by employee's consent (Article 6(1)(a) GDPR) and in accordance with legitimate interests pursued by the employer (Article 6(1)(f) GDPR).

4.2 Processing of personal data based on employment contract

Under the employment contract, the employee enters an environment where the employer has a strong interest in operating a business efficiently, protecting property and mitigating risk. As indicated by researchers[220] and stated by the Article 29 Working Party[221], a certain amount of loss of privacy is an inevitable and accepted part of employment relationship, since the sharing of personal information is an integral part of this relationship. However, the employment contract can only work as a legal basis for the processing of data if this processing is necessary for the performance of the contract. For example, the processing of an employee's contacts and bank accounts allows the employer to comply with their obligations under employment contract such as paying the salary. These particular data processing operations fall under Article 6 (1) (b) of the GDPR and hence can deemed lawful.

Researchers have seen the possibility of using the employment contract to justify digital monitoring in some situations. For example, Esfola has argued that an employment agreement could implicitly justify positioning of microchipped employees, when they pass by readers that receive information from these chips.[222] Similarly, Mangan has stated that in the scenario where an employer wants to monitor employee's social media activity, the employer may argue that it must be able to determine whether or not the employee is adhering to contractual obligations and that this is an aspect of the performance of the employment contract.[223] However, Mangan also notes that an employee may claim that observing social media activity is not germane to the performance of contractual obligations.[224] Overall, it seems that researchers are hesitant to suggest that the use of employment contract as a legal basis can be made a general rule, especially in the case of more intrusive forms of surveillance, and this is because the activity would not be genuinely necessary for the performance of the contract. It is doubtful whether the employment agreement as a legal basis for data processing

---

[220] Fragale, R., Jeffery, M. Information Technology and Workers' Privacy: Notice and Consent. – Comparative Labour Law & Policy Journal 2005/23.

[221] Article 29 Data Protection Working Party. Working document on the surveillance of electronic communications in the workplace. 2002 5401/01/EN WP 55.

[222] *op cit* Esfola, J. P. M.

[223] Mangan, D. Online Speech and the Workplace: Public Right, Private Regulation. – Comparative Labour Law & Policy 2018/39.

[224] *Ibidem.*

gives the employer certain prerogatives concerning monitoring of its employees using digital technologies. Surveillance activities are not indispensable for performing an employment contract and therefore it is reasonable to conclude that obligations arising from the contract cannot justify data collection using digital monitoring technologies. This argument was also corroborated by the ECtHR in Bărbulescu v Romania[225], indicating that the legitimate reasons to justify monitoring employee's electronic communications must be weightier than simply stating that the employer has the right and the duty to ensure the smooth running of the company and the right to supervise its employees performing their professional tasks.

On the other hand, employers have invoked obligations arising from employment contracts to dismiss employees after monitoring activities revealed inappropriate behaviour. For example, social media activity considered inappropriate has led to numerous labour dispute cases in the EU and US. In a case in Italy, a prison guard was fired because he 'liked' a comment on a social network about an inmate's suicide in the prison where he was staffed. The prison's governing body was informed about the conversation and took disciplinary action against the employee on the grounds that the guard's opinion painted a negative picture of the penitentiary administration in the public eye. The administrative tribunal sided with the employer and ruled against the employee based on the reasoning that the opinion embedded in the 'like' could damage the reputation of the prison's governing body.[226] On the basis of the principle of freedom of expression, employees are free to express their ideas about the situation at work unless their statements exceed boundaries imposed by national laws and courts. According to Topo and Razzolini, labour dispute institutions in Italy have to take into consideration the accuracy of facts, the offensiveness of expressions, whether the expression violates the duty not to disclose information on the work organization, and how swiftly the employee removed his comment from the web or whether the comment reached a wide pool of recipients.[227] In conclusion, obligations arising from an employment contract should not justify the monitoring of employees social media accounts; however, offensive comments or 'liking' an inappropriate content may still lead to a disciplinary action or dismissal posed by the employer.

To conclude, although an employment contract is a valid basis under the GDPR for processing employee data, it should not be applied in the case of workplace monitoring. The mere fact that an employment contract is concluded should not justify any type of monitoring of employees, and especially not digital monitoring technology. Monitoring activities are not indispensable for performing an employment contract and therefore obligations arising from the contract cannot justify data collection during monitoring activities. This should be the case even

---

[225] ECtHR 61496/08, Bărbulescu v Romania.

[226] Topo, A., Razzolini, O. The Boundaries of the Employer's Power to Control Employees in the ICTs Age. – 39 Comparative labour Law & Policy, 2018/39.

[227] *Ibidem.*

if data processing is taking place during trivial operations such as starting up computers and entering facilities. Therefore, any kind of monitoring via apps, wearables, microchips or using employees' phones or computers should not be based on the sole existence of a contractual obligation. Hence, contract clauses or policies at work should not entitle employers to carry out monitoring activities and should not justify employment decisions based on such monitoring (e.g. disciplinary actions against employees). Therefore, EU legislation should remove the employment contract as a possible legal basis for employee monitoring.

4.3 Processing of personal data based on legal obligations

Researchers have argued that it is not always clear as to whether an employer's activities concerning data processing received from digital monitoring technologies are mere contractual obligations, as discussed in the previous subchapter, or should be restricted to legal obligations imposed by law.[228] The employer is often required by law to provide personal data related to those under their direction and supervision (e.g. disclosure of employee data to tax authorities). For this, the legal ground enshrined in Article 6(1)(c) of the GDPR, 'for compliance with legal obligation to which the controller is subject' is appropriate. However, processing of personal data in the course of monitoring activities is allowed only whenever processing is necessary and inevitable for fulfilling legal obligations. For example, as illustrated in publication IV, during the spread of COVID-19 most data protection authorities in EU member states suggested that employers use this ground as a relevant means of gathering personal data of employees so that health and safety rules can be applied in the work environment. Unfortunately, there is still some confusion how the obligations need to be enacted to allow data processing. For example, whether a general obligation of health and safety justifies monitoring and data gathering or more specific rules need to be put in place for specific data collection.

Therefore, laws may encourage or even require workplace monitoring, which places greater pressure on employers to monitor employees and guides them to use readily available and often affordable technology. For example, health and safety obligations may justify the use of digital monitoring technology. As noted by Sprague, in the US, hostile work environment jurisprudence is one area in which law may compel surveillance.[229] Hence, different digital monitoring technologies are developed and used in workplaces to help to reduce risks at work. Various devices (such as wearables and microchips) may be used to augment human capabilities, overcome physical limitations and increase safety, especially

[228] Kuner, C. European Data Protection Law: Corporate Compliance and Regulation. Oxford University Press 2007.

[229] *op cit,* Sprague (2018).

in hazardous or emergency situations.[230] The technology may guide employees in performing their tasks more effectively and provide them with useful information about their work environment. As an example, wearable technology may detect and correct poor posture, prevent falls and monitor deviations from a prescribed path.[231] Technologically enhanced caps can detect the wearer's brain activity and fatigue levels by reading their brain waves, sensors can measure and record information about the wearer's surroundings and wristbands may alert employees when they are entering a hazardous zone.[232] These devices may present visual overlays of information (e.g. instructions or warnings) or activate audio and visual alarms (e.g. when the user's fatigue level drops or device is removed).[233] Furthermore, it is probable that employers and employees will start to use information received from digital monitoring technologies in workplace injury cases.[234] For example, better safety and employee performance may lead to reduction of damages or compensation schemes in case of work accidents as employers are able to get access to real-time reporting of an employee's location, immediate reporting of an employee in distress and measuring of the force of impact for diagnosis and treatment of workplace injury.[235] In one of the first cases of such data being used in a legal proceeding, a Canadian law firm used evidence collected by a wearable device (activity data from a Fitbit) in a personal injury case to show the effects of an accident.[236] Hence, laws that regulate working conditions, such as workplace health and safety, compensation of occupational accidents and working time, may lead employers to use obligations enacted in the legislation as a justification for employee monitoring. However, the necessary cause may often be determined with a digital monitoring technology that might be overly intrusive and employers may base their monitoring actions on

---

[230] *op cit,* Eurofound. Employee monitoring and surveillance.; Mathiason *et al*. The Transformation of the Workplace Through Robotics, Artificial Intelligence, and Automation. Littler reports January 2016. – https://www.littler.com (19.08.2021).

[231] Sf. Stack, M. B. Wearable Technology in Workers' Compensation. AMAXX 27.07.2017. – https://blog.reduceyourworkerscomp.com (02.08.2021).;
Robitzski, D. How A.I. Exoskeletons Could Make People Super-Human. INVERSE 22.06.2017. – https://www. inverse.com (19.08.2021).

[232] Coxworth, B. SmartCap Monitors Workers' Fatigue Levels by Reading Their Brain Waves. New Atlas 31.01.2012. – https://newatlas.com (19.08.2021); Holmes, N. Wearable Technology within the Workplace. CONVENE. – https://convene.com (19.08.2021).

[233] *op cit* Coxworth, B.

[234] Vogeler, W. Technology Is Quickly Reshaping Workers' Compensation Claims, FindLaw 24.02.2017. – https://blogs.findlaw.com (19.08.2021).

[235] *op cit* Stack, M. B..; *op cit* Mathiason *et al.*

[236] Peyton, A. The Connected State of Things: A Lawyer's Survival Guide in an Internet of Things World. – Catholic University Journal of Law and technology 2016/24; Crawford, K. When Fitbit Is the Expert Witness. The Atlantic 19.11.2014. – https://www.theatlantic.com (24.08.2021); Olson, P. Fitbit Data Now Being Used in the Courtroom. Forbes 16.11.2014 – https://www.forbes.com (24.08.2021).

obligations that are very generic (e.g. need to check working time; guarantee employee's safety).

Furthermore, laws, collective agreements and court practices can prohibit or allow new types of privacy invasive practices used by employers. As an example, in the US, employer demands for access to job applicants' or employees' social media accounts has resulted in the enactment of prohibitory laws in several states.[237] At the same time, the EU relies on the guidance given by the Article 29 Working Party, which suggests that there is no legal ground for an employer to require potential employees to 'friend' the potential employer, or in other ways provide access to the contents of their social media profiles.[238] Another example of regulating possibly invasive monitoring practices can be drawn from the field of biometric monitoring. Like the biometric laws in the US (in particular in Illinois)[239], the topic of biometric monitoring has come under scrutiny in several EU member states, such as France, Portugal and Cyprus, which have prohibited or regulated specific types of monitoring.[240] For example, in Cyprus the use of biometrics for monitoring purposes is forbidden.[241] Similarly, in Portugal specific legal provisions apply in the scope of employment relationships, notably in relation to processing of biometric data and stipulate that the processing of employees' biometric data is permitted only for the purpose of monitoring attendance and controlling access to the employer's premises.[242] In France, employers must ask for permission from the French Data Protection Authority before processing biometric data and data protection impact assessment must be done and submitted to the authority.[243] Employers using biometric access controls have to justify their choice of a biometric device and explain why the use of other measures (e.g. badges) is not sufficient given the level of security required.[244] In addition to biometric monitoring, other types of monitoring methods have been addressed in EU member states' legislation, such as video surveillance. In

---

[237] *op cit,* Topo, A., Razzolini, O.; Finkin, M. W. Privacy: Its Constitution and Vicissitude – A Half-Century On. – Canadian Labour & Employment Law Journal 2015/18.

[238] *op cit,* Article 29 Data Protection Working Party. Opinion 2/2017.

[239] Sf. Tagvoryan, A., Iley, B. T., Oberly, D. J. Learn the Rules on Employers' Use of Biometric Data. SHRM 01.04.2019. – https://www.shrm.org (25.08.2021).

[240] Sf. Thomas, L. France Continues to Focus on Use of Biometrics. SheppardMullin 02.04.2019. – https://www.eyeonprivacy.com (25.08.2021); Sahinyilmaz, T. Worldwide: Biometric Authentication In The Workplace In Terms Of Employee Privacy. Mondaq 16.03.2021. – https://www.mondaq.com (25.08.2021); Williams, A., Georgopoulou, S. France: CNIL standard on processing personal data for the purpose of human Resources. DataGuidance June 2020. – https://www.dataguidance.com (25.08.2021).

[241] *op cit* Eurofound. Employee monitoring and surveillance.

[242] Data Protection Act law no 58/2019 of 8 August. Diário da República n.º 151/2019, Série I de 2019-08-08. See also Data Protection Laws of the World. Portugal. DLA Piper 2021. – www.dlapiper.com (24.08.2021).

[243] *op cit* Thomas, L.; *op cit* Williams, A., Georgopoulou, S.

[244] Data Protection Act, Law 2018–493 of 20 June 2018.

Portugal, recorded images and other personal data recorded through video systems or other technological means of remote surveillance may only be used in criminal proceedings.[245] In Belgium, monitoring of electronic communications or camera surveillance is permitted only for the objectives stipulated in a collective agreement.[246] A new approach has been enacted in Spain, where the concept of 'digital rights' sets limits on the use of digitally enabled monitoring.[247] The law recognizes the right of employees to privacy in regard to the use of digital devices provided by their employer and stipulates that employers must establish criteria for the use of digital devices for employee monitoring. In this sense, the employer must implement a policy for the use of digital devices subject to the minimum privacy standards, where employees' representatives must be involved in the drafting.[248] Also, several member states have included the 'right to disconnect' into their legislation.[249] In addition, many countries promote bargaining and consultation on employee monitoring, giving employee representatives or work councils powers in this area. For example, involvement or even consent of employee representative, work council or a trade union is often mandatory when implementing measures related to employee monitoring.[250]As seen above, several member states have found that more versatile and specific rules are needed to regulate new digital monitoring methods.

To conclude, t is currently not sufficiently clear when employers may rely on legal obligations to justify data collection during monitoring under the GDPR. Employers may use this legal basis under the GDPR only whenever processing is necessary and inevitable for fulfilling legal obligations. Unfortunately, there is confusion how the obligations need to be enacted to allow data processing in the case of employee monitoring. For example, it is unclear whether a general health and safety obligation justifies monitoring and data gathering or more specific rules need to be put in place for specific data collection, as several member states have done. Necessity and irreplaceability of using digital monitoring technologies is often difficult to argue under general legal obligations (such as verifying

---

[245] Labour Code 7/2009. Diário da República n.º 30/2009, Série I de 2009-02-12.

[246] European and Middle East Guide to Monitoring of Employees in the Workplace. Meritas 2018. – www.meritas.org (29.08.2021).

[247] Organic Law 3/2018 of December 5, on Data Protection and Guarantee of Digital Rights.

[248] Organic Law 3/2018, of December 5, Protection of Personal Data and Guarantee of Digital Rights. ECIJA 11.12.2018. – https://ecija.com (25.08.2021).

[249] For example, Spain, Belgium, France and Italy. Other countries are planning or discussing possible regulation in this topic (e.g. the Netherlands). Sf Henshall, A. Governments have long been trying to enact laws to give workers the right to log off BBC 21.05.2021. – https://www. bbc.com (25.08.2021); Govaert, M. van Beers, A., Daniels, C. The Right To Disconnect. Global Workplace Insider 25.03.2021. – www.globalworkplaceinsider.com (25.08.2021); *op cit* Eurofound. Employee monitoring and surveillance; *op cit* Organic Law 3/2018, of December 5, Protection of Personal Data and Guarantee of Digital Rights. ECIJA.

[250] Sf *op cit* Eurofound. Employee monitoring and surveillance; *op cit* Organic Law 3/2018, of December 5, Protection of Personal Data and Guarantee of Digital Rights. ECIJA.

applicant qualifications and values, or investigating workplace discrimination claims in social media, not to mention monitoring measures such as micro-chipping or contact tracing). Therefore, although legal obligations justify the processing of employee data under the GDPR, this legal basis should only be applied if national law is specific and clearly regulates employee monitoring using digital monitoring technologies. The mere fact that employers are required by law to carry out numerous obligations does not justify the use of digital monitoring technologies.

4.4 Processing of personal data based on employee consent

The possibility to control personal information is a cornerstone of informational privacy and data protection.[251] Researchers have described privacy as individuals' right to determine for themselves when, how, and to what extent information about them is communicated to others.[252] However, as discussed by Otto, granting greater freedom to individuals to structure their privacy in employment has brought us to situation wherein the threat of intrusion into employees' private lives is potentially greater and less controllable'.[253] In the GDPR, the control of information is manifested in Article 4(11) of the GDPR that provides consent as a legal basis allowing the processing of personal data if the data subject has indicated ones wishes – either by a statement or a clear affirmative action. Hence, if employees agree to the use of their personal data, all discussions about the lawfulness of data processing are more or less obsolete. Still, if consent is used as a legal basis for workplace monitoring, it should be restricted to situations where the employee is genuinely able to exercise free choice without any negative consequences[254]. Thus, in accordance with the GDPR consent should not be regarded as freely given if the data subject is unable to refuse or withdraw consent without detriment (GDPR recital 42). More specifically, in order for consent to be valid, it has to be freely given, specific, informed and unambiguous. If any of these requirements as present in Article 4(11) of the GDPR prove to be impossible or difficult to demonstrate, employer should rely on other grounds for data processing. Unfortunately, in an employment relationship these basic prerequisites (e.g. freely given, informed) may be difficult to prove conclusively.

According to recital 43 of the GDPR, consent 'should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller'. For example, in order for the employee's consent to be effective, it should be given in the context where the employee has the possibility to negotiate regarding a possibly privacy invasive

---

[251] *op cit* Otto, M.

[252] Westin, A. F. Privacy and Freedom. – Washington and Lee Law Review 1968/25 (1).

[253] *op cit* Otto, M.

[254] *op cit* Article 29 Data Protection Working Party. Opinion 2/2017.

digital monitoring technology. Researchers, however, are reluctant to recognize consent as a fair ground for data processing in employment.[255] Scholars have argued that consent is powerless in circumstances where a data subject requires a certain good[256] and due to the imbalance of power that exists in the employment relationship, consent is likely to turn into an empty ritual[257]. As noted by Bygrave and DW, consent is problematic when it comes to ensuring strong data protection, mainly because information asymmetry between the data controller and the data subject, and inability of the data subject to fully evaluate the substance and consequences of what he is consenting to.[258] Moore calls this 'thin consent' because an employee must agree to surveillance.[259] The requirement of the consent to be freely given with no imbalance in the relationship between controller and individual is also one of the manifestations of the principle of fair processing of personal data.[260] This has led researchers to argue that if employee monitoring is based on consent, it will not only be unlawful but also unfair as the employer should not be given the opportunity to use its disciplinary powers to persuade employees into agreeing to be subject to monitoring.[261]

The challenges of using consent in an employment relationship have also been raised multiple times by the Article 29 Working Party and later EDBP and according to their guidance, in most types of workplace processing activities, the legal basis cannot and should not be the employees' consent due to the nature of the employment relationship.[262] Similarly, some national data protection authorities[263] and the European Union Agency for Fundamental Rights, the European Data

---

[255] Sf Custers, B., Ursic, H. Worker Privacy in a Digitalized World under European Law. – Comparative Labour Law and policy 2018/39; Moore, A. D. Employee Monitoring and Computer Technology: Evaluative Surveillance v. Privacy. – *Business Ethics Quarterly* 2000/10 (3); Ajunwa, I. Workplace Wellness Programs Could be Putting Your Health Data at Risk. Harvard Business Review 19.01.2017. – https://hbsp.harvard.edu (25.08.2021); *op cit* Peyton, A.

[256] Luca, B., Schwartz, M., Louzada, L. Selling Your Soul While Negotiating The Conditions: From Notice And Consent To Data Control By Design. – Health and Technology 2017/7 (4).

[257] Padi, J. Big data analytics, consent and the European Union (EU) General Data Protection Regulation 2016 (GDPR) – The fallacy of consent and control. Dissertation, Keele University 2018; *op cit* Otto, M.; *op cit* Custers, B., Ursic, H.

[258] Bygrave, L. A., Schartum, D. W. Consent, Proportionality and Collective Power. In Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., Nouwt, S. Reinventing Data Protection? Springer 2009.

[259] *op cit* Moore, A. D.

[260] Bygrave, L. A. Data Privacy Law: An International Perspective. Oxford: Oxford University Press 2014.

[261] *op cit* Esfola, J. P. M; *op cit* Otto, M.; *op cit* Custers, B., Ursic, H; *op cit* Moore, A. D.; *op cit* Ajunwa, I. Workplace Wellness Programs Could be Putting Your Health Data at Risk; *op cit* Peyton, A.

[262] *op cit* Article 29 Data Protection Working Party. Opinion 2/2017; European Data Protection Board. Guidelines 05/2020 on consent under Regulation 2016/679. 04.05.2020.

[263] Sf Information Commissioner's Office (UK). Consent. – https://ico.org.uk/ (25.08.2021).

Protection Supervisor and the Council of Europe[264] have questioned the validity of consent as a legal basis for processing data about employees and indicated that employers should avoid over-reliance on consent. As a result, consent given in circumstances where 'there is risk of deception, intimidation, coercion or significant negative consequences if data subject does not consent', should be qualified as invalid.[265] Nevertheless, reliance on consent as a legal basis to process employees' data is allowed under the GDPR and therefore often suggested by data protection experts[266] and national data protection authorities[267] as a suitable legal basis for data processing where digital monitoring technologies are used at work. This has led employers to also use consent as a legal basis that justifies employee monitoring.

Thus, if the employer wants to use consent as a legal justification for surveillance, the exact circumstances of the case should be taken into account and it should be up to the employer to surpass the burden of proof and demonstrate that data processing was consented freely. Although consent can be linked to privacy as a means for individuals to achieve particular ends according to their will,[268] in the case of digital monitoring technology, it may be hard or even impossible to distinguish freely given and not freely given consent. This can be complicated because not every employee is in a situation of clear imbalance of powers (e.g. managers, specialists with certain qualifications and employees in small enterprises might have more room for negotiation) and it is possible that some employees are willing to accept a lower degree of privacy in order to enjoy the benefits brought by new technologies. For example, as discussed in publication III, employees may desire microchip implants to be early adopters of new technology and appreciate the conveniences of the microchips (e.g. microchips granting access to workplace, releases the employee of the burden of having to carry and not forget or lose their access card used for same reasons).

However, as discussed above, employees may feel that their refusal not to adopt microchip implants or to disclose data from social media can result in a career limiting move (e.g. not getting hired for a job). In these situations: how-

---

[264] European Union Agency for Fundamental Rights, European Data Protection Supervisor, the Council of Europe. Handbook on European data protection law. 2018 edition. Luxembourg: Publications Office of the European Union 2018.

[265] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent. 2011 01197/11/EN WP187.

[266] Sf. Lukka, N., Strickland, D. How to Monitor Employees While Respecting Data Privacy. CPO Magazine 05.06.2020. – https://www.cpomagazine.com (25.08.2021); Workplace Monitoring: What Are Your Employees' Rights? GDPRinformer 20.09.2017. – https://gdprinformer.com (25.08.2021); Suemo. J. 12 most asked questions on EU employee monitoring laws. Worktime 13.10.2020. – https://www.worktime.com (25.08.2021).

[267] Sf. Andmekaitse Inspektsioon. Töötajate isikuandmete töötlemisest koroonaviiruse kontekstis [Data Protection Inspectorate. Processing of personal data of employees in the context of the coronavirus.] 20.03.2020. – https://www.aki.ee (25.08.2021).

[268] Bruyer, R. Privacy: A Review and Critique of the Literature. – Alberta Law Review 2006/ 43 (3).

ever, according to article 7(4) of the GDPR, their consent should be invalid. This article states that when assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia,* the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. As analysed by Mangan, this provision appears to contemplate an employment situation in which a job offer is made by way of a standard form contract on a 'take it or leave it' basis.[269] Therefore, employment should never be made contingent on a willingness to download a contact tracing app or implant a microchip. If the employee refuses, dismissal upon these grounds could be judged unlawful. Unfortunately, it is hard to prove that the loss of a job opportunity resulted from refusing or withdrawing consent.

As argued in publication III, the technology may also limit the employee's options to choose from, disallowing or making it difficult to withdraw the consent or refuse to give consent. For example, in case of microchips implanted under the employee's skin, withdrawing consent is truly possible only if the employer covers the cost of the surgery to remove the microchip. Moreover, in case of social media monitoring, the withdrawal of consent has no considerable effect. As discussed by Solove, information once known by others, cannot be eradicated from their minds.[270] Other factors also influence the quality of the consent given by employees, for example, the existence of facilitating conditions. If the work-places decided to support only one form of technology (e.g. employers using services that cater only to microchip implants), the infrastructure would lead the individual to support the perceived usefulness of the technology and, as a result, consent to the technology. For instance, refusing a microchip that is used for monitoring can be difficult if the same chip also gives access to work premises. In these situations, the possibility to refuse or withdraw consent in a microchip authentication enabled workplace seems difficult to achieve without exiting or limiting the microchip-enabled service provided by the microchips in the work-place. Therefore, for employees to truly have a choice, companies should provide infrastructure supporting the use of different technologies. For instance, Onspota's team, the developers of the Shield For Business app that helps employers to track possible COVID-19 exposures in work premises by collecting data on a employees' location, movements and proximity to others, also offers non-consenting employees, an alternative solution: scanning various QR codes all across the factory floor instead.[271] Hence, employers should ensure that the removal of microchips or other digital monitoring technologies does not lead to a decrease in the level of service offered, avoiding digital discrimination among their employees.

---

269 *op cit* Mangan, D.

270 Solove, D. J. Conceptualizing Privacy. – California Law Review 2002/90 (4).

271 *op cit* Shemer, S.

Sometimes, it is also difficult for the employee to refuse consent, i.e. refusing becomes somehow 'abnormal'[272] as the wider use of technology in workplace may influence the employee's decision making. As discussed by Gauttier, colleagues who have implanted microchips can set the trend for others, thus decreasing scepticism towards the technology,[273] and therefore generating a culture where employees are expected to endorse this technological solution. According to Gauttier, employees may feel that technology allows them to use services conveniently, enables them to explore the potential of the technology and be part of the future that is promoted by the company.[274] As discussed in publication III, these triggers of digital monitoring technologies, e.g. the spread of individual cases, peer pressure, different affordances provided by the chip and the infrastructure in a workplace, have an impact on the quality of the consent given by the employee and may reduce employees' organizing and negotiating powers. As a consequence, employees may often be conditioned when giving consent to make a calculated and rational decision about digital monitoring technologies.

Furthermore, as Ajunwa, Crawford and Ford argue, employers may present digital technology as a benefit to employees.[275] Employees are encouraged and often rewarded for providing their information. For instance, about 90% of companies in the US offer wellness programs, some of which encourage employees to use Fitbit and other devices that measure the quantity and intensity of their workouts and to employ simple visual and motivational tools to track their progress and help sustain their engagement.[276] For example, a major corporation in the US, Target, is using activity and sleep-tracking devices to promote health habits for employees.[277] Digital monitoring technologies may also contribute to the gamification of work, making employees feel that they are constantly in competition with one another.[278] These practices discussed above may also lead to implications for consent quality and reduce employees' organizing and negotiating power.

In addition, the world of work has been profoundly affected by the COVID-19 pandemic during which digital contact tracing and other digital monitoring

---

[272] *op cit* Poullet, Y.; *op cit* Raskar, R. *et al*.

[273] *Op cit* Gauttier, S.

[274] *Ibid*; see also Custers, B., van der Hof, S., Schermer, B., Appleby-Arnold, S., Brockdorff, N. – SCRIPTed 2013/10 (4).

[275] Ajunwa, I, Crawford, K., Ford, J. Health and Big Data: An Ethical Framework for Health Information Collection by Corporate Wellness Programs. – The Journal of Law Medicine & Ethics 2016/44 (3).

[276] Wilson, H. J. Wearables in the Workplace. Harvard Business Review September 2013. – https://hbr.org (25.08.2021). See also Troiano, A. Wearables and Personal Health Data: Putting a Premium on Your Privacy. – Brooklyn Law Review 2017/82; Fitbit. Help employees build healthy habits across key areas of their health and wellbeing. – https://www.fitbit.com (25.08.2021).

[277] *op cit* Vogeler, W.

[278] *op cit* Eurofound. Employee monitoring and surveillance.

technologies have been increasingly put into use in the hopes of slowing the spread of the virus[279] and for enabling employees to return to work safely. For example, various smartphone contact tracing apps enable real-time tracing of a massive number of potentially infected individuals.[280] However, one concern is that contact tracing apps, although explicitly voluntary in many countries[281], might become mandatory in workplaces.[282] As discussed in publication V, given that it is unlikely that the app will be adopted so extensively in a given workplace if it is merely voluntary, many employers may want to encourage its use among employees to make it effective. It is likely that many businesses will promote the relevant app as part of the organization's health and safety strategy and highlight the benefits of everyone using it. Although this measure may be justified during a health and safety crisis, it also raises new concerns as the practice may lead to overall acceptance of different intrusive digital monitoring technologies after the pandemic ends and therefore reduce the employee's consenting power considerably. In fact, not all countries are willing to leave the decision-making in the hands of the employers, which is the case under the GDPR. For example, Australia passed legislation that prevents private sector actors from requiring use of the contact tracing app.[283] The situation is the opposite in the US, where employers would be permitted to require employees to use a contact tracing app as a condition of employment.[284] In India, a national contact tracing app has been made mandatory for government and private sector employees, some of whom need to download the app in order to access their workplaces or get paid.[285]

In addition to the criteria that consent must be freely given, specific and unambiguous, it also has to be informed. The informed consent requirement brings a certain degree of transparency: consent should be based on comprehensive notification and be explicit (e.g. given in writing).[286] Thus, as argued by Mitrou,

---

[279] Oswald, M., Grace, J. The COVID-19 Contact Tracing App in England and 'Experimental Proportionality'. – *Public Law 2021*; Watts, D. COVIDSafe, Australia's Digital Contact Tracing App: The Legal Issues. – SSRN 2020.

[280] Kretzschmar, M. E. *et al*. Impact of Delays on Effectiveness of Contact Tracing Strategies for COVID-19: A Modelling Study. – The Lancet Public Health 2020/5 (8); Yasaka, T. M., Lehrich, B. M., Sahyouni, R. Peer-to-peer contact tracing: Development of a privacy-preserving smartphone app. – JMIR Mhealth Uhealth 2020.

[281] *op cit* European Commission. Mobile applications to support contact tracing …

[282] *op cit* Scassa, 2021.

[283] Privacy Amendment (Public Health Contact Information) Act 2020, No. 44, 2020.

[284] *op cit* Brown, S. R., Linden, M. F., Sullivan, E. J., Torres. J. J.; *op cit* Bodie, M. T., McMahon, M.; Ropes&Grey. Going Back to Work: Employer Use of 'Apps' on Employee PDAs/Smart Phones for COVID-19 Contact Tracing". Ropes&Grey 01.05.2020. – https://www.ropesgray.com (25.08.2021).

[285] Ghoshal, S. Open book? In India, where people are forced to download a tracking app to get paid, journalists are worried about it also being used to access their contacts. – Index on Censorship 2020/49 (2).

[286] Article 29 Data Protection Working Party. Opinion 15/2011.

consent needs a clearly defined scope of action, i.e. the consenting employee needs to have the relevant information so that they would know what they are consenting to.[287] However, in the case of digital monitoring technologies, an informed decision is hard to make as employees may be unable to understand the consequences of consent. As noted by Moreham, in practice it is difficult or even impossible to have absolute control over information, especially in the contemporary, digital, networked world.[288] The extent of data collected about employees, especially in the context of digital monitoring technologies and greater connectivity, enhances data processing capabilities, which make the issue of informed consent even more challenging. According to the European Fundamental Rights Agency, individuals often lack a clear understanding of the extent of the data collected, of the technical functioning of the processing and therefore of what they are consenting to.[289] As discussed in publication V, informed consent should include proper knowledge about the use of the data from the technology. For example, in case of microchip implants, the employee should be informed about the placement of possible readers that trace employees' movements and whether the data from the chip is combined with other data. Employees should also know that the design of the technology does not allow the chips to be turned off and it is impossible to shield one's personal data on the devices from being read.

Furthermore, attempts to meaningfully inform employees may also be inadequate. Research suggests that highly technical, long, and complex privacy notices, policies or contract clauses often fail to inform data subjects about the true nature of data processing practices.[290] Research shows that even if a company has guidelines and policies in place, employees are not properly informed about the content of these documents (see also publication II). In addition, employers often rely upon the employment contract for consent to a range of matters. For example, as discussed by Mangan, speech may be curbed remarkably through the expansive wording of employment contract clauses that confer unilateral authority on employers to determine 'offending' speech[291] (e.g. in social media). According to Solove, an employer's notices or policies often fail to make it clear to employees what data is collected and for what purposes, how the data is analysed, and which decisions result from the analyses.[292] Also, as discussed by Padi, in a bid to avoid liability and take account of future data uses, it is foreseeable that

---

[287] Mitrou, L. Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'? – SSRN 2018.

[288] Moreham, N. A. Privacy in the Common Law: A Doctrinal and Theoretical Analysis. Law Quarterly Review 2005/121.

[289] *op cit* European Union Agency for Fundamental Rights *et al*.

[290] Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union. TNS Opinion & Social 2011.

[291] *op cit* Mangan, D.

[292] Solove, D. J. Privacy Self-Management and the Consent Dilemma. – Harvard law Review 2013/126.

employers may draft vague privacy policies to cover any unforeseen eventuality of processing.[293] Therefore, I believe that consent gathered by such contract clauses, privacy notices or policies is meaningless as broad and permissive information fails to genuinely inform the employee about all aspects and consequences of digital monitoring technology. Furthermore, as the employers do not usually develop technologies (e.g. apps, wearables, microchips) themselves, they often do not know enough about how data will be collected, stored, shared or used[294] and therefore are not able to communicate this information to their employees.

Concerns around the legal feasibility of consent have led researchers to argue that consent cannot automatically validate the employers' privacy invasive practices and considered necessary to move from the legal basis of consent to the legal basis of legitimate interest that fits best to the new technologically-driven workplace.[295] Also, the Article 29 Working Party has recognized the specific features of the employment relationship, and concluded that, bar exceptional situations, employers will have to rely on a legal ground other than consent – such as the necessity to process the data in their legitimate interest.[296]

To conclude, consent as a legal basis may be used by employers to justify employee monitoring under the GDPR; however, this legal basis may also potentially invade privacy and data protection rights of employees. Due to GDPR's complex and vague rules related to consent, digital monitoring technologies are likely to expand without clear direction in workplaces, which may cause further deterioration in employee privacy protections. Employees and employers would benefit from a clear and stable approach concerning these technologies. Thus, due to the imbalance of power between employers and employees and the features of digital monitoring technologies, I argue that it would be necessary for EU legislation to strengthen employees' ability to reject digital monitoring technologies and stipulate specific rules for these technologies. EU legislation should prohibit the use of consent as a sole legal basis for employee monitoring (e.g. consent could be used together with another legal basis such as legitimate interests). However, as agreement and relevant information remains the mechanism through which employees can exercise control over their personal data, the legal basis for processing should be accompanied by the obligation to carry out information and consultation among employees and seek their approval of these technologies (e.g. by way of negotiations with work councils or other employee representatives). Also, legislation should always require companies to provide the infrastructure supporting the use of different technologies and employers should not rely on one specific digital monitoring technology (such as microchip implants) exclusively.

---

[293] *op cit* Padi, J.

[294] *op cit* Johnson, E.

[295] *op cit* Custers, B., Ursic, H; *op cit* Esfola, J. P. M.

[296] *op cit* Article 29 Data Protection Working Party. Opinion 2/2017.

4.5 Processing of personal data based on the legitimate interests of the employer

4.5.1 Legitimate interests as a balance of different elements

On the grounds of legitimate interests, employers can process their employees' data when their commercial interests are so strong that they prevail over employees' rights such as privacy, data protection, etc. The application of this lawful ground therefore calls for balancing the interest of the employer with interests and fundamental rights of employee, similarly to the exercise carried out by the ECtHR (e.g. in Bărbulescu v Romania) referred in subchapter 2.3 of this dissertation. Although possibly a good alternative in employment relationship for other legal grounds discussed above, this basis is also not without its faults. Researchers have indicated that legitimate interest as a legal basis is formulated broadly and therefore is too ambiguous.[297] For example, Otto has argued that neither the GDPR nor the CJEU provides clear guidance concerning the types of interests that may legitimize the free processing of personal information, the conditions of under which such interest may be considered to override data subjects' rights, or who should be entitled to make such a decision.[298]

It is important to note that reliance upon Article 6(1)(f) of the GDPR does not automatically validate any kind of processing implemented by the employer. As mentioned, processing under this legal basis is possible if it is necessary for the purposes of the legitimate interests pursued by the employer, except where such interests are overridden by the interests or fundamental rights and freedoms of the employee which require protection of personal data. The notion of the interest in Article 6(1)(f) of the GDPR relates to benefits the employer derives from the processing. An interest should be considered legitimate as long as it is in accordance with the law in its broadest sense, specific enough and represents an actual interest.[299] Under the GDPR, all sorts of possible interests seem to be covered.[300] In its Opinion, the Article 29 Working Party lists prevention of fraud, employee monitoring for safety or management purposes and physical security or IT and network security as examples of situations that may amount to legitimate interests of the employer.[301] As discussed in publications IV and V, collection of employee data during the outbreak of COVID-19 for health and safety purposes (e.g. using contact tracing apps or other similar technologies), appear to be aligned with the employees' individual interests in their well-being, so it is

---

297 *op cit* Otto, M.; *op cit* Esfola, J. P. M.

298 *op cit* Otto, M.

299 Article 29 Data Protection Working Party. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. 2014 844/14/EN WP 217.

300 Sf Voigt, P., Bussche, A. The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer International Publishing 2017. The GDPR in recitals 47–49 also provides some examples of processing that might amount as necessary for a controller's legitimate interests.

301 *op cit* Article 29 Data Protection Working Party. Opinion 06/2014.

unlikely that there would be overriding compelling individual rights that would invalidate the processing. Other possible situations in which legitimate interest could be used are extremely broad, such as positioning employees using microchip implants in sectors where a constant knowledge of their whereabouts is needed (e.g. ambulance teams).

Under Article 6(1)(f) of the GDPR, the employer also has to evaluate the impact of the monitoring activities on the employee. The objective of this 'balancing test' is to ensure that the degree of intrusion on the employee's privacy is proportionate to the goals pursued by the employer. The purpose of this assessment under Article 6(1)(f) of the GDPR is not to erase any possibility of negative consequences for the employee but to ensure that the impact is proportionate.[302] As stated by the Article 29 Data Protection Working Party, the employer has to establish interests that provide justification for employee surveillance, but also take into account that its actions 'cannot unjustifiably prejudice the rights and freedoms of the data subjects'.[303] Otto has criticized this concept by saying that 'from the employer's perspective, establishing the required nexus between the privacy invasive measure/policy and the relevant interest represents in practice pure formality.'[304] She emphasizes that 'in order to protect the employees' privacy from pervasive and endless interference' based on apparently legitimate interests, the concepts 'individualization' and 'relevance' should be incorporated into the assessment of the legitimacy of a privacy-invasive measure.[305]

During the balancing test under Article 6(1)(f) of the GDPR, the employer needs to establish the potential consequences for the employee by identifying the possible privacy risks of monitoring, and their likelihood of materialising and severity.[306] Possible privacy related risks can be found in recital 75 of the GDPR. In accordance with the recital, evaluation of personal aspects may be damaging (the recital refers to physical, material or non-material damage) as it leads to 'analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles'. The Article 29 Working Party goes even further, stating that 'broader emotional impacts'[307] on the employee must also be duly considered, as well as the employee's reasonable expectation of privacy. Unfortunately, it is unclear whether the reasonable expectations of the employees should be considered as established by the ECtHR or as

---

302 *op cit* Article 29 Data Protection Working Party. Opinion 06/2014.

303 Article 29 Data Protection Working Party. Opinion 8/2001.

304 *op cit* Otto, M.

305 *Ibidem.*

306 *op cit* Article 29 Data Protection Working Party. Opinion 06/2014.

307 *Ibidem.*

rooted in the US case law.[308] It therefore remains to be seen how the potential consequences for the employee and their reasonable expectations should be evaluated during a balancing exercise in the context of digital monitoring technologies under the GDPR. To complicate the matter, this legal basis also requires a necessity test,[309] which means that the employer needs to show that the use of digital monitoring technology is necessary and that there are no other means of monitoring less intrusive to the employee.

To summarize, the balancing exercise under Article 6(1)(f) of the GDPR has been criticized due to its broadness and lack of understanding as the test leaves much room for interpretation.[310] As seen above, the balancing test consists of several components and considerations, such as the employer's interests, potential consequences for the employee, possible privacy risks and their likelihood of materialising, reasonable expectation of privacy and intensity of monitoring. Unfortunately, these components and considerations have not been indicated in the GDPR but have been generally explained in the Article 29 Working Party's guidance[311]. Therefore, it is unclear if the mentioned list is exhaustive or open, and how these elements should be interpreted in the context of digital monitoring technologies. The difficulty with the balancing test is that a balancing of rights is never clear-cut and depends on the specifics of the case. As the balancing test is carried out by the employer, it is questionable if the test strikes a fair balance between the parties of the employment relationship and is not biased. The balancing test also needs a strict and substantive analysis that may be complicated for employers to carry out. To better illustrate the difficulties that accompany balancing of interests and necessity test, the next subchapter looks at some examples of national jurisprudence concerning digital monitoring technologies.

4.5.2. Possibly intrusive monitoring under the legitimate interests

Examples of balancing employer's and employee's interests can be found in the case law of the ECtHR and national courts. Helpful guidance in this matter comes from Bărbulescu v Romania[312], where the court conducted a proportionality analysis and shed light on a number of relevant criteria for domestic courts to assess when dealing with employee privacy (see subchapter 2.3). Most importantly, the ECtHR requires an examination of 'the extent of the monitoring by the employer and the degree of intrusion into the employee's privacy' as well as an

---

[308] On the protection of employees' privacy in the United States see, Katz v. United States, 389 U.S. 347 (1967); Finkin, M. Privacy in Employment Law (4th ed. 2013). On the application of the 'reasonable expectation of privacy' in the EU jurisprudence, see Hendrickx, F., Van Bever, A. Article 8 ECHR: Judicial Patterns of Employment Privacy Protection, Oxford: Hart Publishing 2013.

[309] *op cit* Article 29 Data Protection Working Party. Opinion 06/2014.

[310] *op cit* Esfola, J. P. M.

[311] *op cit* Article 29 Data Protection Working Party. Opinion 06/2014.

[312] ECtHR 61496/08 Bărbulescu v Romania.

assessment of the possibility for the implementation of less invasive monitoring techniques.[313] Furthermore, examples of this balancing test can also be found from other parts of the world. The Federal Court in Australia, for example, gave a four-part test that can also be used to assess the appropriateness of using digital monitoring technologies at work. The test asks the following questions: if the measure is demonstrably necessary for meeting a specific need; is it likely to be effective in meeting that need; is the loss of privacy proportional to the benefit gained, and is there a less privacy-invasive way of achieving the same end?[314]

National jurisprudence shows that there are situations in which intrusive monitoring may be justified and legitimate. For example, in one peculiar case in Italy, an employer persuades a human resources manager to create a fake Facebook account to chat with the employee during his working time, in order to collect the evidence that the employee frequently leaves his workstation unattended to chat on Facebook, thereby leaving a dangerous machine uncontrolled. As the employee, indeed, started the conversation on Facebook, the employer dismisses him on serious breach of contract. In this case, the judge said the interference with the employee's private sphere was not a violation of the right to privacy because of the purposes of the employer's interference: defending the employer from the employee's wrongdoing.[315] Concerning this case, researchers Topo and Razzolini refer to an Italian regulation that allows interference with the employee's privacy only when strictly necessary[316] and say that these concealed 'defensive controls' should be justifiable only if there is no other possibility to detect the employee's misdeeds. They explain that defensive controls are considered to be lawful only to the extent that there is a legitimate aim and the means used to achieve this aim are proportionate and necessary.[317] Furthermore, the limits of defensive controls in Italy also lie with the general employer's duty of good faith and with the duty to respect, as far as possible, the employee's dignity and privacy in accordance with data protection principles.[318] This judgement clearly shows that even very intrusive monitoring methods, such as faking a Facebook account to communicate with the employee under a false name, may be considered acceptable if an employer is able to show that the interests of the company prevail over the interests of the employee. Unfortunately, these and similar cases also leave ample room for interpretation and lack clarity for future decisions.

Also, as discussed in publication III, in a hypothetical case concerning microchips, the employer may have the right to monitor employees. For example, a

---

313 ECtHR 61496/08 Bărbulescu v Romania.

314 Eastmond v. Canadian Pacific Railway (11.06.2004). The Judgement of the Federal Court of Australia. No FC852.

315 The Cassazione 10955/2015. – www.iusexplorer.it.

316 *op cit,* Topo, A., Razzolini, O.

317 Ibidem.

318 Ibidem.

company may implant microchips into employees to provide them with access to rooms and lockers containing hazardous chemicals. The purpose of the chip is to block unauthorized access to chemicals and monitor their use by the worker to guarantee employee safety and preclude the misuse (e.g. theft, misplacement) of chemical substances. In this case, if microchipping employees has substantial safety benefits, the use of microchips might be considered lawful under the GDPR, especially for possibly preventing an accident and loss of lives. Here, the impossibility to be able to detach the microchip from the body can be a positive aspect as it prevents employees from taking off the chip and causing dangerous situations. I believe that in case of microchipping, the specific nature of the sector and the job position will play an important role in determining whether the rights of employment parties are balanced, and the level of intrusiveness is reasonable. As the employer's responsibility is to ensure the safety and health of professionals and clients, microchipping might be more easily accommodated for certain occupations, e.g. locating police officers, soldiers or firefighters who need to be rescued in an emergency, providing secure restricted access to vaults containing highly sensitive data or preventing accidents in laboratories or mining sites, or in settings such as psychiatric clinics. In these cases, employer may argue that implanting microchips in an employee's hand is necessary and the least intrusive means for employee monitoring, and that alternative solutions are not that effective. Unfortunately, it will remain for future case law to determine, whether this practice is in accordance with the GDPR. Despite the guidance given by the Article 29 Working Party and ECtHR, there is still no readily available annotated guide to assist employers who plan to use digital monitoring technologies. I argue that such explanations are needed as addressing these issues allows employers to determine whether it is appropriate to use digital monitoring technologies (such as microchip implants) in the workplace and fosters the development of good practices before privacy-invasive ones become entrenched.

Therefore, the question arises: what monitoring may be considered too intrusive and out of balance under a 'balancing test'. To answer this question, it would be useful to analyse another case concerning a different digital monitoring technology. For example, the Federal Labour Court of Germany concluded that installing keystroke-tracking software on the company's devices to record every keystroke and regularly take screenshots was an unlawful way to monitor employees, as it violates employees' right to informational self-determination and is too intrusive on the employee's right to privacy.[319] Although the case was based on Section 32(1) of the BDSG, which allows an employer to process employee data for the purposes of the employment relationship if this is necessary for its establishment, implementation or termination, the discussion also focused on the balancing of interests, therefore serving as a relevant example in the context of Article 6(1)(f) of the GDPR. In its ruling, the court stated that the fact that the employee admitted to using the company computer for private purposes during

[319] Bundesarbeitsgericht [The German Federal Labor Court] 27.07.2017, case no. 2 AZR 681/16.

working hours did not justify the circumstances of the dismissal. This was not changed by the fact that the employee was aware that the company computer systems would be logged and that company also had a policy that forbade private use of computers. Therefore, the court determined that because the evidence used to dismiss the employee had been obtained illicitly, the termination of employment contract was void. The measures initiated by the employer were therefore disproportionate. The judges added that using such software could be legitimate if there was a pre-existing concrete suspicion of a criminal offence or serious dereliction of work duties. In this case, the use of digital monitoring technology and the continuity of employer's activities rightly tilted the decision of the court in favour of the employee. In another dispute in Ireland, the balance was swung in the favour of the employer. In this case the employer had installed a camera on the truck of a driver working for him. The video recorded only the fuel usage and showed the driver had been siphoning fuel for private use and as a result, he was dismissed. The Commissioner ruled that the dismissal in this case was lawful, stating that covert surveillance – as in this case – may be justified when there is a concrete suspicion of fraud or serious dereliction of duty.[320] As these decisions illustrate, the balance of interests often relies on the details and facts of the case.

The opinion of the Article 29 Working Party also explores a number of possible monitoring scenarios and their lawfulness. For example, in screening candidates' social media profiles during the recruitment process, the collection of data must only take place to the extent 'necessary and relevant to the performance of the job'.[321] Keystroke logging and screen capture technology, particularly when deployed in order to monitor home or remote working, on the other hand, is unlikely to be permissible under the GDPR. As the Working Party concludes, 'the processing involved in such technologies are disproportionate and the employer is very unlikely to have a legal ground under legitimate interest'.[322] As discussed in publication III, monitoring microchipped employees may also lead to very serious consequences for the employee. For example, this could be the case if an employer starts to gather real-time data from chips and capture exit and entry sequences, location, speed and movement of the employee. This kind of systematic reading of a chip can expose the habits of employees and thus possibly establish a profile for them. Continuous monitoring of employees constitutes serious interference with their right of privacy and as a consequence, employee monitoring should be prohibited.

Regardless of the Article 29 Working Party guidance, there are still several shortcomings in the context of reconciliation the competing interests. For example, the Working Party's recommendations also exhort employers to ensure that in order to prevent monitoring of private information, appropriate measures must be

---

[320] Peninsula team. Can you spy on employees? Peninsula 23.08.2018. – https://www.peninsulagrouplimited.com (25.08.2021).

[321] *op cit* Article 29 Data Protection Working Party. Opinion 2/2017.

[322] *Ibidem.*

in place to distinguish between private and business use of the device.[323] Given the increasingly fluid boundaries between work and the private sphere, however, it is not immediately clear how such lines might be drawn. In addition, critics of the concept of legitimate interests have said that '[p]privacy will not be weighed appropriately when balanced against employers' interests unless the socio-economic counterparts of civil and political rights of employees are recognized.'[324] Therefore, indicating that 'social rights (such as the right to dignity at work, just conditions of work, health and safety) should be used to determine the scope of coverage of employees' privacy rights and to delineate the scope of permissible infringements on employee privacy.'[325] Furthermore, the role of the principle of fairness is debatable if legitimate interest is used as a legal basis for processing employee data harvested from monitoring activities. Unfortunately, it is unclear under what circumstances monitoring of employee's personal data can be considered fair. In addition, researchers have expressed their doubts concerning this legal basis as it rules out control of the data by the subject and puts employees in a situation of having to trust employers to take care of their rights and to conduct the balancing test in a way that strikes a fair balance.[326]

To conclude, it is advisable to rely on legitimate interests as a legal basis for monitoring employees. However, this legal ground is not without its faults. Similarly to ECtHR case law, the employer is required by the GDPR to carry out a balancing exercise which takes into consideration different elements. However, these elements are not clearly regulated in the legislation but rather given in a guidance of the Article 29 Working Party and derive from national jurisprudence. For better understanding, these elements should clearly be defined in a legal instrument. In the case of digital monitoring technologies, the employer should take into consideration the necessity of monitoring, the means of monitoring (whether an access card or implanted microchip), specific characteristics of the technology and the harm which the monitoring may cause to employees' privacy. In addition, it should be further discussed how the role of fairness, social rights at work, good faith, right to health and safety (e.g. right to working environment that is suitable for employee's mental health), freedom of speech (e.g. right to express opinions on the internet and social media) and the need to respect employee's dignity also influence the balancing test. Furthermore, the specific nature of the sector and the job performed should play a large role in determining the level of intrusiveness allowed for monitoring systems. It also seems that digital monitoring technologies (such as microchip implants) will find greater legitimation in more dangerous and adverse working sites prone to accidents. As it is left for the employer to decide which interest may be considered as overriding employee's rights and therefore sufficient justification for data processing, EU

---

323 *op cit* Article 29 Data Protection Working Party. Opinion 2/2017.

324 *op cit* Otto, M.

325 *Ibidem.*

326 *op cit* Custers, B., Ursic, H.

legislation should clarify which overriding compelling individual rights would invalidate the processing or as a second possibility, legislation should regulate what interests or purposes justify monitoring of employees. EU legislation should also specify what other factors or steps need to be considered before monitoring is lawful. Perhaps an employer might be required to inform employees about digital monitoring methods and be obliged to hear their views in this matter. Employee's representatives could also be involved in an implementation and use of a privacy invasive monitoring technology in the workplace.

5. Protection through principles of data processing

5.1 Significance of principles of data processing

In the next subchapters, I focus on principles of data processing (Article 5) as they form the backbone of the GDPR and help to interpret the other data protection provisions. In conjunction with the ECtHR's case law on employee monitoring, these principles serve to shape and safeguard workplace privacy. As principles must be respected by 'all processing of personal data'[327], they give guidance to employers who process data related to employees. The GDPR strengthened and detailed the principles[328] and today, as argued by researchers, these privacy principles should apply to all types of use of personal data in a modem workplace.[329] Nevertheless, substantial doubts have been expressed as to whether the attempt to enforce the data protection principles through legislation has actually protected privacy.[330] Scholars have identified issues that should be resolved in order to accommodate privacy principles in different environments[331] and they argue that these principles have increasingly been reduced to narrow, legalistic principles that place the burden of protection on the individual rather than on society and its institutions.[332] In addition, extensive use of digital monitoring technologies and the spread of COVID-19 have sparked a discussion on this matter and raised the need to revisit these principles. According to Newlands et al., principles of data protection are key to the successful deployment and adoption of digital monitoring technologies during the spread of COVID-19.[333] Similarly, as discussed in publications IV and V, most EU data protection agencies[334] have underlined the importance of general principles of data

---

[327] CJEU C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.

[328] While the principles under the GDPR are similar to those found in the Data Protection Directive, certain concepts are more fully developed, for example the explicit reference and clarification of the transparency and minimisation principle and the establishment of a new principle called 'integrity and confidentiality'.

[329] *op cit* Custers, B., Ursic, H.

[330] Bonner, W., Chiasson, M. If fair information principles are the answer, what was the question? An actor-network theory investigation of the modern constitution of privacy. – Information and Organization 2005/15 (4); Tene, O. Privacy: The New Generations. – International Data Privacy Law 2011/1 (1).

[331] Karyda, M., Gritzalis, S., Park, J. H., Kokolakis, S. Privacy and fair information practices in ubiquitous environments: Research challenges and future directions. – Internet Research 2009/19 (2).

[332] Cate, F. H. The Failure of Fair Information Practice Principles. In Winn, J. K (Ed.) Consumer Protection in the Age of the 'Information Economy'. Routledge 2006.

[333] *op cit* Newlands, G. *et al*.

[334] Sf Hungarian National Authority for Data Protection and Freedom of Information. Information on processing data related to the coronavirus epidemic. 2020. – https://www.naih.hu (25.08.2021).

processing in cases where an employer monitors employees to limit the spread of COVID-19. However, scholars have also raised concerns. For example, Custers and Ursic argue that adapting digital monitoring technologies to the sometimes rigid rules of data protection law is not always easy.[335] In the same manner, scholars from the US have also stated that digital technology may pose challenges to traditional privacy principles.[336] Due to the importance of data protection principles and possible concerns related to technological advances, in the next subchapters, I focus on these principles and ask what protection they offer if an employer monitors employees in a digital workplace. I have not analysed all principles enacted in the GDPR but concentrated on principles of purpose limitation, fairness and transparency that are vital for the implementation of digital monitoring technologies and at the same time raise concerns in the context of these technologies.

5.2 The principle of purpose limitation

As many authors have observed, privacy is not only an absence of information, but about ensuring that personal information is used for the purposes one desires (decisional privacy).[337] Thus, it is understandable why purpose limitation is one of the core principles of data protection.[338] It requires personal data to be 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes'.[339] Furthermore, designating a purpose to the monitoring is vital for defining lawful basis under the GDPR and for achieving compliance with the other data protection principles.[340] One important reason behind the purpose of data processing is that any use of data should remain within a data subject's reasonable expectations and be in compliance with the principle of transparency as the employees need to be provided with precise information about the purposes of the monitoring in clear and concise form to avoid any ambiguity.[341] Unfortunately, the principle of purpose limitation is often disregarded or sometimes even in contradiction with digital monitoring technologies, as discussed below.

One problem with purpose limitation is that both employees and employers may get used to digital monitoring technologies and view their use as a common practice that needs no purpose. As discussed in publication II, the use of digital

---

335 *op cit* Custers, B., Ursic, H.

336 *op cit* Ajunwa, I., Crawford, K., Schultz, J.

337 Inness, J. C. Privacy, Intimacy, and Isolation. Oxford University Press 1992.

338 Article 29 Data Protection Working Party. Opinion 03/2013 on purpose limitation. 2013 00569/13/EN WP 203.

339 GDPR Article 5 (1)(b)

340 Article 29 Data Protection Working Party. Opinion 03/2013.

341 *Ibidem.*

monitoring technology may become such a routine task that monitoring is carried out without having a clear aim in mind. For example, employers often carry out social media monitoring with the hope of finding some new information about the applicant. Interviewed employers justified their practice by emphasising that the applicant needed to 'fit in' with the rest of the staff. This practice is inconsistent with the GDPR; however it is a good example of digital monitoring technology becoming normalized as a tool for human resource management.

Additional problems with the principle of purpose limitation are caused by the potentially wide range of purposes legitimizing the collection and processing of data in the employment context. For example, contact tracing apps were used during the spread of COVID-19 to ensure a safe work environment and prevent the virus from spreading. One of the functions of the purpose limitation principle is to limit the further data processing in a manner incompatible with the initial purpose. However, the precise purpose(s) often depend on the functionalities of these technologies. As discussed in my publication V, data processing during COVID-19 must be specific enough to exclude further processing for purposes unrelated to the management of the COVID-19 health crisis (e.g. for monitoring the behaviour and performance of employees). Examples of illegitimate further processing include using wearables or apps to prevent the spread of COVID-19 in the workplace, only to repurpose them afterwards to monitor how employees are performing, how much time they spend at their workstations or which colleagues are holding a meeting, etc. The concern is that contact tracing apps will increase the amount of data generated in the workplace environment and that existing technologies will covertly be used to monitor employees, although initially intended for different purposes. For example, some employers are integrating AI software into existing security cameras to make it possible to count individuals in a room and track employee compliance with social distancing and mask-wearing regulations and send alerts when employees are not practicing social distancing.[342] In these cases employers need a suitable legal basis to process employees' data (see chapter 4). Employers may also combine different technologies used in a workplace to combine multiple data sources and gain comprehensive insight across an entire company and to reduce virus transmission in the workplace. Considering the fact that contact tracing is easier to justify in a workplace, the power imbalance in an employment relationship makes it easier for the employers to mandate employees to use apps or other technologies for health and safety purposes. Hence, on the one hand, the use of different technical solutions may help employers to create effective contact tracing programs, and to reinforce social distancing practices as part of a digitized working environment. On the other hand, however, this brings forth the inevitable rise of surveillance in a workplace. It is important to note that as these technologies can be endorsed during a time of crisis, they can be problematic in a post-pandemic work environment.

[342] *op cit* As employees return to the office, banks explore surveillance tech.; Paresh, D. Companies bet on AI cameras to track social distancing, limit liability. – Reuters 27.04.2020.

The above practices may lead employers to use technologies for the purposes other than originally planned and bring with illegitimate further processing of employee data, generate the risk of 'function creep' and use of data purposes unintended by the employee. As a result, if the consequences of monitoring are not reasonably expected by the employees, they would most likely be in breach of the principle of purpose limitation. For example, data used for contact tracing is later used to control employees' attendance and observance of working and rest time.[343] Because of these concerns, both EU data protection agencies[344] and researchers[345] have emphasized that digital infectious disease surveillance and related measures need to be ceased at the end of the pandemic. Therefore, any personal data collected to combat COVID-19 pandemic must be deleted once it no longer serves the purpose for which it was collected – i.e., when the pandemic has ended or is sufficiently contained. For example, this means that a contact tracing app should be discontinued once the pandemic has ended, and residual personal data stored should be destroyed permanently. Also, some of the authorities managing contact tracing apps have indicated that the app data collected would be removed once the system gets de-activated at the end of the pandemic[346]. However, the 'end of the pandemic' is a vague term and researchers have already before the spread of COVID-19 expressed their doubts that employers may hide secondary purposes in long, legalistic texts of privacy policies that no one reads.[347] Also, there is no specific knowledge what will happen to technologies used in a workplace after the virus has receded as the principle of purpose limitation is in conflict with the very idea of the data economy, which is to reuse data. Due to new monitoring methods and the widespread use of different technologies at work to mitigate the spread of COVID-19, there is inherent pressure for more efficient use of data that often comes at the expense of employees' privacy.[348] When the real need for the technology to keep employees safe has receded, it is important that regulations and guidance prevent future harms and ill-use by employers, such as function creep if these digital monitoring technologies are used. Similar examples of possible threats to employees' privacy and data protection rights can be constructed with other digital monitoring technologies. For example, via the use of digital technology in wellness programs, employers may wish to use, for other purposes, data originally collected under the guise of helping employees achieve their personal health goals. Research in

---

343 *op cit* Johnson, E.

344 Sf German Data Protection Supervisory Authorities joint information paper on data protection and the Coronavirus pandemic. Datenschutzrechtliche Informationen zur Verarbeitung von personenbezogenen Daten durch Arbeitgeber und Dienstherren im Zusammenhang mit der Corona-Pandemie. – https://www.bfdi.bund.de (25.08.2021).

345 Urs, G., Ienca, M., Scheibner, J., Sleigh, J., Vayena, E. Digital tools against COVID-19: Framing the ethical challenges and how to address them. 2020. arXiv:2004.10236.

346 *op cit* Ahmed, Nadeem *et al*. 2020.

347 *op cit* Custers, B., Ursic, H.

348 *Ibidem.*

the US has revealed that employee data collected as part of workplace wellness programs are frequently sold to third parties without the employee's knowledge or consent.[349]

Therefore, as there is a high risk of further use of data in case of digital monitoring technologies, it can be argued that the principle of purpose limitation is broadly worded and allows for monitoring practices that are in line with the GDPR but still invade data protection rights and privacy of employees. Due to the imbalance of power in an employment relationship, legislation is needed to strengthen employees' ability to reject digital monitoring technologies and the purposes that allow for employee monitoring should be more specifically regulated. For example, some member states have allowed specific digital monitoring technologies only if their use is permitted for the purposes enacted in legislation or collective agreements. For example, monitoring of electronic communications or camera surveillance is permitted in Belgium only for the objectives stipulated in a collective agreement.[350] A similar approach should be used in EU legislation.

5.3 Principle of fairness

The provision in Article 5(1)a) of the GDPR sets out that personal data shall be 'processed lawfully, fairly and in a transparent manner in relation to the data subject', thus intertwining the principle of fairness with other principles such as lawfulness and transparency of processing and overall compliance of the norms enacted in the GDPR.[351] The principle of fairness is therefore linked with numerous procedural safeguards that should, as a whole, result in fair processing of data. For example, in accordance with the GDPR, in order to be fair, the processing should be transparent. As argued by Koops, only after employees are provided with information concerning data processing will they be able to question the dataveillance practices of their employers[352] and properly exercise the prerogatives granted to them by the GDPR. However, according to Custers and Ursic, this approach focuses on procedural fairness rather than substantive fairness. They contend that even if companies are compliant with EU data protection law, people may still perceive interference with their privacy.[353] Similarly, other researchers argue that legal basis and transparency should not be the only notions that determine whether the activities are considered privacy-invasive and therefore unfair. For example, Otto states that a 'fairness requirement, by its very nature, includes a more sensitive value judgment, namely on pertaining to

---

[349] *op cit* Ajunwa, I, Crawford, K., Ford, J.

[350] *op cit* Eurofound. Employee monitoring and surveillance.

[351] *op cit* European Union Agency for Fundamental Rights *et al*.

[352] Koops, B.-J. On decision transparency, or how to enhance data protection after the computational turn. In Hildebrandt, M., de Vries K (Eds.) Privacy, Due Process and the Computational Turn. Abingdon Routledge 2013.

[353] *op cit* Custers, B., Ursic, H.

perceived equity in the given practice'.[354] Furthermore, in her opinion, the court should intervene in a situation where an employer's exercise of power forces employees to trade away more of their rights to privacy than would normally be acceptable in the given employment context.[355] As also discussed in publications I and II, the importance of context when assessing if the processing is fair is crucial.

Therefore, adhering to the principles and other provisions of the GDPR does not necessarily mean that processing should be considered fair. Fairness should be examined in a more substantive way taking into account the theory of 'contextual integrity' introduced by Nissenbaum, who argued that privacy norms in semi-public spheres (such as employment relationship) must respect contextual norms.[356] Nissenbaum gives relevant parameters, such as the nature of information in question, its appropriateness to the context, and the general contextual norms of flow/distribution.[357] In publication II, I refer to interviews with Estonian employers, which indicate that employers' actions often breach contextual integrity and result in unjustifiable negative consequences for employees. For instance, some of the interviewed employers who had had previous negative experiences with employees' alcoholism took special notice during social media background checks of various party photos and photos in which alcohol was displayed. This may lead employers to judge employees or applicants unfairly. Therefore, although not required by the GDPR, employers should refrain from monitoring employees' social media activity at all or if they do so (e.g. use LinkedIn for its intended professional purposes) consider the role of context and abstain from any unjust activities (e.g. eliminating an applicant from the list of candidates).

Also, features of digital monitoring technologies highlight that the context of data processing should be taken into consideration when assessing whether employer's surveillance practices can be considered fair. A good example here again is social media monitoring. Conversations taking place on social media are usually meant for a group of friends or acquaintances as social media can be a place to share opinions. However, messages, texts, videos and pictures visible on a social media profile may impact an employment relationship in many ways. For example, different services are offered to employers that allow to analyse the content and information posted on the site by applicants or employees. This enables employers to evaluate a candidate for a particular job or assess employee's behaviour or commitment to work. As argued by Poullet, the data from social networking sites enables employers to potentially profile the employee and take advantage of the knowledge thus acquired, including use of the knowledge

---

354 *op cit* Otto, M.

355 *Ibidem.*

356 Nissenbaum, H. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press 2009.

357 *Ibidem.*

outside of its original context. She further states that, 'it is troubling to see how 'private' and 'public' spheres are intermingled on these sites'.[358] Indeed, social networks make it easy to communicate so that a flow of information invades everyday life. As has been pointed out the overflowing of information has cancelled the 'right to ignore'.[359] Situations that would be insignificant outside social networking community are amplified, because they are available to a wide audience and with this comes the increase of responsibility of the employees who post online. As explained by Mangan, courts in UK also do not do much to draw a line between on- and off-duty conduct as it remains advisable for employers to discipline (even terminate) for social media usage. According to Mangan, the 'benchmark for harm (anything that could reflect poorly on the employer) remains robust'.[360] In this regard, Topo and Razzolini state that it is important to leave room for an employee's right to express opinions on social media whenever the behaviour does not seriously offend decency and the dignity of others and does not disclose business information.[361]

Another example of using technology out of context may be seen in the case of monitoring employees with microchip implants. As microchip readers can be placed anywhere and log everything employees do in their daily lives, their movements, their working time and use of office supplies or even what employees purchase at the work cafeteria. These pieces of information separately are not that revealing but can be combined to form a bigger portrait of the employee. In his works, Solove highlights the potential of this kind of practice to cause harm to dignity as it upsets one's expectations. In his view, people do not expect that small bits of information may reveal much.[362] Furthermore, as argued by Hildebrandt, concerns around 'ubiquitous' technology can be aggravated when the knowledge derived from the profiling activity does not aim to 'single out' an employee from all others, but rather identify them as a member of a certain group of employees with whom they shares a set of correlated attributes, a process commonly referred as 'group profiling'.[363] In those cases, a properties of the group may be imposed as traits to all individual employees which may lead to the creation of 'false positives' or 'false negatives' and illegitimately exclude those employees for a promotion, for instance.[364]

In the light of the above, it can be argued that the principle of fairness is broadly worded, therefore allowing for monitoring practices that are in line with the GDPR but could still potentially invade data protection rights and privacy of the

---

[358] *op cit* Poullet, Y.

[359] *op cit,* Topo, A., Razzolini, O.

[360] *op cit* Mangan, D.

[361] *op cit,* Topo, A., Razzolini, O.

[362] Solove, D. J. A Taxonomy of Privacy. – University of Pennsylvania Law Review 2006/154.

[363] Hildebrandt, M., Backhouse, J. (Eds.), D7.2: Descriptive analysis and inventory of profiling practices. FIDIS 2005.

[364] *Ibidem.*

employee. Fairness should be examined in a more substantive way and the processing to be fair, needs to be evaluated within the given context. This means that employers may monitor employees only in ways the employees would reasonably expect and not use the data in a manner that unjustifiably has a negative effect on employees. For example, employers should consider the context when assessing social media profiles or collecting data from microchip implants. Also, profiling groups of employees to combine a bigger portrait of the workforce might lead to out-of-context conclusions and attribute to a single employee with characteristics not related to them. The actions mentioned above should be considered unfair. The ambiguity and narrow scope of fairness principle show the weakness of EU legislation in the context of employee monitoring and reveal the need for more specific rules for monitoring at work.

5.4 Principle of transparency

The principle of transparency is central to ensuring privacy and adequate data protection. As discussed in subchapter 2.2, according to the ECtHR, the employee must be notified in advance of the existence of the monitoring measures and their nature and extent.[365] Providing information about the data processing activities has also an important role in the GDPR as it gives the employee the opportunity to act upon the received knowledge, including the possibility to exercise the rights provided by the GDPR such as the right to request access to all of the information gathered through the monitoring practices, the right to erasure of personal data and the right to object to being the subject of monitoring.[366] The principle of transparency is specified through the requirement to provide required information under Articles 13 and 14 of the GDPR. To meet the transparency requirement of the GDPR, employees should be informed of some key aspects of data processing (e.g., the purposes for which personal data are to be processed).[367] Together with transparency employers also need to keep the focus on data minimization[368] to foster employees' control of their personal data. Hence, there must be no secret and covert processing of personal data and such processing should not have unforeseen negative effects. However, in the case of digital monitoring technologies, this aim is often difficult to achieve, as explained below.

Although inconsistent with the GDPR, many employees experience secret and excessive data processing due to digital monitoring technologies as discussed in publication II. Transparency is also endangered by the features of these technologies and the use of AI. Researchers argue that digital monitoring technologies

[365] ECtHR 61496/08, Bărbulescu v Romania.

[366] GDPR Articles 15, 17 and 21.

[367] GDPR Articles 13–14.

[368] GDPR 5(1)c.

lack transparency and are difficult to challenge.[369] For example, an employer might have invited people for interviews after their CVs and social media information were ranked by algorithms. Those that did not succeed may never find out what factors the algorithm took into account when making the decision and how their applications were assessed. Or in another case, employers may encourage employees to use wearables or microchip implants to monitor attendance in the workplace, offering discounts to those who meet certain goals. As argued by Custers and Ursic, the use of a multi-factor, multilevel analysis of employee data makes it hard to determine precisely what kind of performance leads to results (e.g. bonuses, getting hired).[370] Therefore, where digital monitoring technologies are concerned, it is important to remember Koops's advice that quality of information that must be provided to data subjects is more important than the quantity.[371]

The transparency requirement should act as a deterrent on employers seeking to implement overly intrusive monitoring activities. If they know that employees must be notified in detail of the existence of monitoring activities, employers will be more reluctant to introduce highly intrusive measures.[372] However, as explained by Poullet, 'the new monitoring technology is largely invisible in two ways; it operates in a largely hidden way (we do not know what information is collected, when or for whom), but also, as a natural extension of an activity or movement (a door opens and the computer comes on) assisting us in our choice of activities'.[373] The same problem can be noted by the Article 29 Working Party. According to their guidelines, owing to the capabilities of such technologies, employees may not be aware of what personal data are being processed and for which purposes, while it is also possible that they are not even aware of the existence of the monitoring technology itself.[374] Possible examples can be drawn from social media monitoring and using microchips to monitor employees as these technologies also enable the employer to covertly observe employees. As discussed in my publication III, microchips enable covert monitoring thanks to the electromagnetic waves' ability to travel easily and silently through almost every kind of material, without implanted employees being aware of the monitoring taking place. Employees may therefore suffer from the inability to be aware of the surveillance taking place and eventual profiling that might occur through the aggregation of the different data from chip readers present in the workplace. For this reason, the Article 29 Working Party highlights the idea that

---

369 *op cit* Custers, B., Ursic, H.

370 *Ibidem.*

371 Koops, B.-J. The trouble with European data protection law. – International Data Privacy Law 2014/4 (4).

372 *op cit* Otto, M.

372 *op cit* Esfola, J. P. M.

373 *op cit* Poullet, Y.

374 *op cit* Article 29 Data Protection Working Party. Opinion 2/2017.

being informed of the geographical or digital vicinity of sensors/readers, when the collection of data refers to them or their environment, represents a crucial expectation of those users.[375] However, these details of monitoring are not regulated in the GDPR. Although the list of information that has to be given to the data subject is long in the GDPR, additional information, falling outside the scope of the Regulation, should be given to employees when workplace monitoring is conducted using digital technologies. For example, in case of some digital monitoring technologies (e.g. RFID enabled microchips, AI enabled workplaces) it is important to understand the specific times, actions and methods performed to process data obtained by monitoring activities. The additional information that should be explained to the employees therefore includes information on what digital monitoring technologies are used, their specific features and details of monitoring, such as what times and where specifically monitoring is taking place, what security safeguards have been put in place and what will be the consequences of the monitoring activities (might monitoring lead to disciplinary decisions or dismissal of the employee).

According to the GDPR, the employee should be notified 'at the time the personal data are obtained', meaning no later than the beginning of monitoring activities. This means, for example, that if the social media activities or employees' movements are subject to monitoring, the employer should notify its employees, without undue delay, during their very first day of employment. Researchers have been critical of this solution, stating that notification obligation is required at a time where it is not yet clear for the employee how they will be affected by the monitoring.[376] According to Esfola, if the burden of providing information is imposed only at the beginning of the processing operation, real-time transparency is arguably inexistent.[377] Therefore, employees might not be told about monitoring until judicial proceedings against them. In this regard, Esfola argues that while the GDPR provides 'more' information to the employees, it seems to have missed an opportunity to provide them with 'better' information. He claims that the possibility to give information at the beginning of the processing activity allows a certain degree of 'function creep', enabling use of the data beyond the initially collected purpose for which it was intended in the first place, with very little accountability.[378] As argued by Solove, it is not clear what the notified employee can, in reality, do with the knowledge that monitoring is taking place, besides see their privacy disappear. According to Solove, if individuals are aware that monitoring might take place, the feelings of anxiety and discomfort become more prominent, which may ultimately result in self-censorship, impairing employees'

[375] Article 29 Data Protection Working Party. Opinion 8/2014 On the On Recent Developments On The Internet Of Things. 2014 14/EN WP223.

[376] *op cit* Esfola, J. P. M.

[377] *Ibidem.*

[378] *op cit* Esfola, J. P. M.

self-determination.[379] Therefore, it can be argued that the employer's obligation to inform employees under the GDPR, although extensive, occurs at a moment when monitoring activities have no effect on the employee and therefore lose their relevance and timeliness. If the deployment of a digital monitoring measure renders it difficult for one to assess its impact in the workplace, more transparency is necessary to hold employers accountable.

Additionally, the need to give employees information concerning monitoring has been stressed in the ECtHR judgement in Barbulescu v. Romania.[380] In his partly dissenting opinion, Judge De Albuquerque holds that a comprehensive policy in the workplace must be put in place, including specific rules on the use of email, instant messaging, social networks, blogging and web surfing.[381] Similarly, it is a standard practice for the information required by the GDPR to be delivered in the form of a privacy policy. To be compliant with the GDPR, the privacy policy needs to be in a 'concise, transparent, intelligible and easily accessible form, using clear and plain language'.[382] Still, this approach in the GDPR has been characterized by researchers as procedural and formalistic.[383] Researchers argue that the current way these obligations are established in the GDPR seem to enable employers to conduct 'box-ticking' exercises, providing a false sense of security to the employees[384] and leading to 'transparency illusion'.[385] However, transparency should be more than ticking a box and checking if every aspect has been included on the list in an employer's privacy policy. According to Koops, for transparency to be relevant, a shift is necessary from (i) process to event transparency, (ii) retrospective to real-time transparency and (iii) nominal to effective transparency. He explains that procedural components of transparency should be replaced by some measurements like inputs, outputs and outcomes, organizations should be subject to periodical scrutiny and effective measures should be applied to increase transparency.[386] Therefore, clear and comprehensive policies can be helpful for employees to understand and exercise their rights. However, unambiguous, complicated and lengthy privacy policies may also not offer sufficient protection. It is also unreasonable to describe details of specific monitoring activities in a general policy, mainly because different aspects of monitoring (such as the placement of sensors) might be too specific to add into a document that usually focuses on general rules. Furthermore, activities, times and

---

379 *op cit* Solove, D. J. (2006).

380 ECtHR 61496/08, Bărbulescu v Romania.

381 *Ibidem.*

382 GDPR Article 12(1), recital 60.

383 *op cit* Custers, B., Ursic, H., *op cit* Otto, M.

384 *op cit* Koops, B.-J. (2014).

385 Heald, D. Varieties of Transparency. In Hood, C., Heald, D. (Eds.) Transparency: The Key to Better Governance? British Academy 2006.

386 *op cit* Koops, B.-J. (2014).

subjects connected to monitoring might change over time, which makes the policy rapidly obsolete.

Furthermore, employers often use these privacy policies or contract clauses to legitimize disciplinary action if monitoring reveals traits and behaviours of employees. For example, there is a permissive attitude toward employers disciplining employees for remarks on social media. Cases where employees are fired due to social media posts often focus around trust; suggesting that if the employer contends it has lost trust in the employee, dismissal will be found to be justified.[387] To avoid an excessive response to employees' activities on social media, researchers advise employers to 'put in place transparent and appropriate procedures ensuring arrangements for the proportionate and independent investigation of facts reported.'[388] Other scholars argue that by accepting contractual clauses, employees are understood to have consented to the broad constraint placed on their social media activity.[389] As explained by Mangan, the possibility of losing a job may be one of the most potent of the chilling effects in these cases and may give employers the role 'as gatekeepers of online speech'.[390] He further explains that the acceptability of an employer's response in case of dismissal is challenged on the basis that speech stands out as an important element of democracy and should not be casually set aside based upon a contract clause or a policy. The above shows the weakness of privacy policies or contract clauses in regulating aspects of employee monitoring. Therefore, it has to be agreed that a contract clause or notification in the privacy policy cannot legitimize any privacy-intrusive monitoring measure and employers should refrain from surveilling the social media activities of their employees without a just cause (such as doubts about possible fraudulent or criminal behaviour).

To avoid possible infringements on employee privacy and data protection rights through monitoring, several member states have enacted legislation that mandates the employer to consult or ask prior consent of the employee's representatives, trade unions or work councils if the employer intends to adopt new employee monitoring practices in the workplace.[391] In Austria, Finland, Germany, the Netherlands and Sweden, employees and employers are required to reach agreement on the monitoring rules.[392] Information and consultation is required in other countries such as Belgium, France and Romania.[393]Consultations and negotiations can be helpful to mitigate the risks of monitoring. However, lack of cooperation between employer and employees may hinder the employee's rights. Unfortunately, the practice of involving employee representatives is not enshrined

---

387 *op cit* Mangan, D.

388 *op cit,* Topo, A., Razzolini, O.

389 *op cit* Mangan, D.

390 *Ibidem.*

391 *op cit* Eurofound. Employee monitoring and surveillance.

392 *Ibidem.*

393 *Ibidem.*

in the GDPR and today must be agreed in each member state. This hinders the protection of employees in countries where collective bargaining and employee representation is not prevalent (such as eastern EU member states).

To conclude, it can be argued that the principle of transparency is broadly worded, therefore allowing for monitoring practices that are in line with the GDPR but still invade data protection rights and privacy of employees. In light of the above analysis, it is evident that under the GDPR, employees do not receive adequate information at the right time concerning digital monitoring technologies and therefore are not able to understand how monitoring is carried out. Due to the possibility of hidden monitoring, legislation in the EU should be enacted to oblige employers to periodically inform and communicate monitoring activities to employees. Furthermore, it should be mandatory for employers to consult employee representatives if they plan to implement digital monitoring technologies. If the monitoring is continuous, employers should require the consent of employee representatives before implementing such a measure and carry out regular consultations on the issue. In addition, information concerning employees' data and monitoring should not only be added to privacy policies, but the employer should be obliged to carry out training courses and visualize monitoring activities (such as signs at a workplace that indicate places were monitoring is taking place). Also, additional information should be given to employees such as specific details of monitoring, information on whether the private use of the company's technology is allowed and to what extent (such as internet use), what technological safeguards have been put in place and what will be the consequences of the monitoring activities. Employees should also be aware of the specific times, actions and methods performed to process data. Therefore, employees should be informed when and how they are being monitored and, for example, know the location of sensors and readers and their monitoring radius. If employer is basing its decisions on monitoring results, employees should have detailed knowledge what effect the monitoring has on decision making and what data is being observed to reach a decision.

6. Conclusions

6.1 Extending the protection of privacy

Digital technologies used at work will lead to new legal controversies in the field of privacy and data protection. As shown by the analysis in the present dissertation, although the ECHR and its case law is extensive and deals with employee's privacy protection, its scope and content are limited. The ECtHR's judgements do not cover digital monitoring technologies and are largely dependent upon sometimes formalistic criteria. For that reason, the broad case law of the ECtHR is unlikely to be enough to effectively protect employees from privacy intrusions in the context of digital monitoring technologies. The argumentation and findings of this dissertation show that due to digital monitoring technologies, imbalance of power in an employment relationship, ambiguities and lack of specificity concerning employee monitoring in the ECHR and the GDPR, EU legislation is needed to strengthen employees' ability to reject privacy-invasive monitoring technologies and give employers clarity under what conditions employee monitoring is allowed.

Although the ECtHR has expanded the scope of Article 8 of the ECHR in employment matters, the question how to determine whether the monitoring was excessive and in contradiction with employees' privacy is still unsettled in case law. In Bărbulescu vs Romania, the ECtHR reduces the ambiguity surrounding the legality of employee monitoring and carries out a proportionality test by balancing the interests at stake, and in doing so provides instructions on the factors that need to be considered when balancing the interests of employers and employees. However, the test given in Bărbulescu is not the solution for extensive monitoring practices taking place at work.

Similar to previous cases, the court in Bărbulescu emphasizes prior notice as one of the first and main criteria when considering whether monitoring is privacy-invasive or not. Therefore, the role of the privacy notice in future cases is unclear – will it be only one element discussed in the case or will it still have a significant impact on the court's decision. As discussed in the present dissertation, although clear policies and instructions are necessary for monitoring, it is unjust to strip employees of privacy protection merely on the basis of a notice given by employer. An existence of a policy cannot justify invasive technologies that enable covert and continuous monitoring (e.g. such as microchip implants, wearables, contact tracing apps). For these reasons, reliance on prior notice should lose its importance in future cases.

The ECtHR also takes into consideration the intrusiveness of the monitoring measure and whether there are other equally effective ways for the employer to monitor employees. In the context of digital monitoring technologies, this seems to be a crucial factor. However, the notion of intrusiveness can be criticized as being too vague in the context of digital monitoring technologies. It is unclear how an employer should ascertain the intrusiveness of digital monitoring technologies (such as microchips), which are used to enter the premises in lieu of keys,

access cards or other similar devices. The broadness of the concepts, such as intrusiveness of monitoring, point to a need to regulate employee monitoring practices in a more precise and comprehensive way.

Furthermore, the harm that may be caused by digital monitoring technologies when privacy protection is compromised is alarming. The issue is even more relevant as employers rely on AI tools to extract and sort the information. For these reasons I suggest that the ECtHR should take into consideration possible harms of digital monitoring technology when assessing whether a monitoring activity intrudes on an employee's privacy. Possible harms that should be considered include information injustice – i.e. information presented in one context is used in another – digital monitoring technologies are an extensive source of information that may possibly reveal job-irrelevant information, data obtained by digital monitoring technologies may vary considerably and be inaccurate. Also, the question of necessity – whether the information available from digital monitoring technology is even relevant to the work performance – should have greater weight when discussing these technologies.

6.2 Specifications for the processing of employee data

As discussed in the present dissertation, the GDPR is broadly worded, therefore allowing monitoring practices in the digital workplace that are in line with the GDPR but still could potentially invade privacy and data protection rights of employees. Also, there are monitoring practices used by employers in the digital workplace that do not fall under the scope of the GDPR but should be regulated to protect employee privacy rights. These findings indicate the need for EU legislation that regulates monitoring in the digital workplace.

The GDPR does not distinguish processing activities where data collection is limited from other activities where increasingly powerful tools enable processing and analysis of information concerning employees and spotting patterns or correlations in their data. As the rise of AI enables algorithmic management of employees, the traditional boundary between the workplace and individuals' private lives is also rapidly breaking down and new sources of information can reveal patterns far beyond traditional monitoring methods. In addition, the increasing trend of self-monitoring with the use of fitness trackers or health apps on telephones has created possibilities to combine the result of self-monitoring with data gathered in the digital workplace. This trend significantly influences employment relationships and communication between employer and employee, therefore making it important to consider possible new rules in EU that protect employees from unnecessary and excessive monitoring activities. For example, all the data processing activities often associated with digital monitoring technologies, such as collecting location data of employees, compiling patterns in work settings, gathering information concerning employee's private life (e.g. health information from a contact tracing app) and using AI-generated datasets and

algorithmic management, fall under the scope of the GDPR and therefore in principle are allowed if employer has a legitimate grounds for processing.

It is questionable whether all these processing activities and data received as a product of such monitoring should be allowed in the context of employment. EU legislators should clarify the scope of employee data processing and employee monitoring. For example, EU legislation should clearly indicate that if not necessary, employers should refrain from the use of digital monitoring technology. The exception to this rule might be allowed only in case of criminal activities or serious malpractice or other just causes such as prevention of accidents at work. One possibility is to distinguish different monitoring activities from least invasive to most invasive and set clear and more stringent rules to monitoring measures that strongly interfere with employees' rights.

In addition, identifying which information constitutes personal data or even understanding when employers obtain personal data in the context of digital monitoring technologies is a complicated exercise. Today it is possible to distinguish between primary and secondary digital identifiers, where the first is relatively easy to identify as it is directly connected to the person (e.g. name, address, mobile phone number, password), but the latter identifiers are much more hidden as they are indirect (e.g. 'cookies', IP addresses, RFID tag numbers). Digital identifiers are not necessarily known to the employee; however, they can be associated with an employee or a site or object with which the employee is connected. Contact tracing apps, microchips and other technological solutions that use these secondary identifiers may also process various amounts of other data (e.g. health data, location data, social/proximity graphs, interactions between users and the people they came into close contact with) and do so covertly. These different identifiers make opaque monitoring a possibility in the work environment and therefore new EU legislation should be considered that enable employees to ascertain when and how monitoring is taking place. The monitoring activity should entail stricter obligations for employers (e.g. the employer's obligation to give more detailed instructions to employees; special signs in a workplace to indicate where monitoring is taking place) or prohibition on using some monitoring (e.g. prohibition of covert monitoring or the inability to gather movement data inside the workplace). Employees should also have a possibility to choose between the 'new' and more 'traditional' monitoring methods (e.g. instead of apps that gather location data, employees may be identified by scanning a card at the entrance and exit). Also, employers should not be allowed to combine different sources of data obtained by way of digital monitoring technologies to build large employee databases that might reveal the employee's identity even if anonym zed.

There are also monitoring activities that do not fall under the scope of the GDPR but should be regulated to protect employee's privacy rights. Employees are deprived of clear protection concerning their data or privacy if their employer uses the data from cookies or RFID tags without seeking to identify the employee concerned but simply to profile a computer, tool, room or chip owner so as to decide on certain actions in the employee's regard. As employees are left without protection, EU legislation should regulate monitoring activities where the

employer profiles employees without using their personal data. For instance, employers should generally be prohibited to carry out monitoring of an employee's life and behavioural patterns without a specific purpose (such as health and safety) that is clearly stated in legislation.

In the case of digital monitoring technology, personal data collection may not be dictated by the employer but dealt with by a third party. In fact, often the employer only partially or not at all controls the data and employees' data is handled by an employing enterprise or software developers or service providers. Furthermore, the role of controller is not always clear-cut if an employer uses employees' self-tracking tools or third-party-owned technologies (e.g. contact tracing apps developed by governments or large corporations for wider use during COVID-19) at workplaces to encourage or compel employees to use this technology. The extent of an employer's responsibility for privacy in relation to such apps will depend on the role the employer takes. If the employer is relying on its employees to voluntarily pass on relevant information generated from contact tracing government-launched contact tracing apps, they are probably not controllers of data as defined by the GDPR as they do not determine the purposes and means of the processing. However, the role of employers inevitably becomes more complicated if they insist that employees download and use government apps as a workplace safety measure. In the latter case, employers have a more active role; however, it is questionable whether they define the purpose and means of the processing. In these cases, the employer might not obtain any data from the technology (e.g. employer only monitors the existence of an app on the employee's or company's phone) and therefore is not considered to be the controller of data under the GDPR. Such monitoring activity, even if it does not fall under the scope of the GDPR, should be regulated to protect employee's privacy rights. The requirement to monitor one's health, working speed and time using wearables or apps seriously invades the employee's privacy as it interferes with the employee's right to escape and withdraw as she desires. Therefore, the employer should not have the right to require employees to use digital monitoring technologies such as apps, wearables or microchips to carry out self-monitoring without a serious reason (e.g. to prevent accidents in dangerous work environments or mitigate the spread of a contagious disease). I suggest that EU legislation should specify in which situations and under what conditions employers may require employees to use digital monitoring technologies such as apps or wearables (e.g. smart watches). To avoid ambiguities, EU legislation should clearly state that data collection from employee-owned sources (e.g. self-tracking app) is prohibited.

6.3 Appropriate legal bases for employee monitoring

Although in principle, employers may use several of the legal bases enacted in the GDPR such as employment contract, legal obligations, consent and legitimate interests, these grounds could potentially invade privacy and data protection rights of employees and do not offer adequate protection to employees or clarity to employers on their possible use.

Under the GDPR, an employment contract is a valid ground to use for processing an employee's data, however, it should not be applied in the case of workplace monitoring. The mere fact that an employment contract is concluded should not justify any type of monitoring of employees, especially when making use of digital monitoring technology. Monitoring activities are not indispensable for performing an employment contract and therefore obligations arising from the employment contract cannot justify data collection during monitoring activities. This should be the case even if data processing is taking place during trivial operations such as turning on/logging in to computers and entering facilities. Therefore, any kind of monitoring via apps, wearables, microchips or using employees' phones or computers should not be based on the sole existence of a contractual obligation. Hence, contract clauses or policies at work should not entitle employers to carry out monitoring activities and should not justify employment decisions based on such monitoring (e.g. disciplinary actions against employees). For these reasons, EU legislation should remove contractual obligations as a possible legal basis for employee monitoring.

In addition, it is currently not sufficiently clear when employers may rely on legal obligations to justify data collection during monitoring in digital workplace. Employers may use this legal basis only whenever processing is necessary and inevitable for fulfilling legal obligations. Unfortunately, there is confusion around how the obligations need to be enacted to allow data processing in case of employee monitoring – for example, whether a general obligation of health and safety justifies monitoring and data gathering or more specific rules need to be put in place for specific data collection. The necessity and irreplaceability of using digital monitoring technologies is often difficult to justify under general legal obligations (such as verifying applicant qualifications and values or investigating workplace discrimination claims on social media, not to mention monitoring measures such as microchipping or contact tracing). Therefore, although legal obligations justify the processing of employee data under the GDPR, this legal basis should only be applied in case national law is specific and clearly regulates employee monitoring. The mere fact that under legal acts, employers need to carry out numerous obligations does not justify the use of digital monitoring technologies.

Consent as a legal basis is allowed under the GDPR but might still invade data protection rights of employees, and for these reasons should not be used in the case of workplace monitoring. The main reason this legal basis fails to offer strong data protection is information asymmetry between the employer and the employee and the inability of the employee to fully evaluate the substance and consequences of what they are consenting to. This imbalance in the employment relationship changes consent into an empty process as employees' possibilities to negotiate are limited. Also, it is hard to distinguish when data processing was done because of the employer's wishes and when the processing was voluntarily accepted by the employee. The technology may also limit the employee's options to choose whether to accept or decline, disallowing or making it difficult to withdraw the consent or refuse consent. Other factors also influence the quality of the consent given by employees, for example, the spread of individual cases in

a workplace and accompanying social pressure to accept the technology. Furthermore, attempts to meaningfully inform employees may also be inadequate as highly technical, lengthy and complex privacy notices, policies or contractual clauses fail to inform employees about the true nature of data processing practices in a digital workplace. Due to the complex and vague rules related to consent in the GDPR, digital monitoring technologies (such as microchips implants) are likely to expand without clear direction in workplaces, which may cause employee privacy protections to deteriorate further. I believe that employees and employers would benefit from a clear and stable approach concerning these technologies. Thus, due to the imbalance of power between employers and employees and the features of digital monitoring technologies, I argue that EU legislation should strengthen employees' ability to reject digital monitoring technologies and give specific rules for use of these technologies. EU legislation should prohibit the use of consent as a sole legal basis for employee monitoring (e.g. consent could be used together with another legal basis such as legitimate interests). However, as agreement and relevant information remains the mechanism through which employees can exercise control over their personal data, legal basis of the processing should be accompanied by the obligation to carry out information and consultation among employees and seek their approval of these technologies (e.g. by way of negotiations with work councils or other employee representatives). Also, legislation should always require companies to provide the infrastructure supporting the use of different technologies and employers should not rely on one specific digital monitoring technology (such as microchip implants) exclusively.

It is advisable to rely on legitimate interests as a legal basis to monitor employees. However, this legal basis is not without its faults. Legitimate interest as a legal basis is formulated broadly and is too ambiguous. The balancing exercise under Article 6(1)(f) of the GDPR lacks clarity, leaving much room for interpretation. The balancing test consists of several components and considerations, such as potential consequences for the employee, possible privacy risks and their likelihood to materialize, severity of monitoring and reasonable expectation of privacy. Unfortunately, these components and considerations have not been specified in the GDPR but have been generally explained in the Article 29 Working Party's guidance and derive from national jurisprudence. It is unclear whether the mentioned list is exhaustive or open and how these elements should be interpreted in the context of digital monitoring technologies. The difficulty with the balancing test is that a balancing of rights is never clear-cut and depends on specifics of the case. As the balancing test is carried out by the employer, it is questionable whether the test strikes a fair balance between the parties to the employment relationship and is not biased. The balancing test also needs a strict and substantive analysis that may be complicated for employers to carry out. For better understanding, the elements of a balancing test should clearly be defined in a legal instrument. Also, if digital monitoring technologies are used, the employer should take into consideration the necessity of monitoring, the means of monitoring (whether it is an access card or microchip implanted under one's skin), specific characteristics of the technology and the harm which the monitoring may

cause to employees' privacy. As it is left up to the employer to decide which interest may be considered to override the employee's rights and therefore justify data processing, EU legislation should clarify which overriding compelling individual rights would invalidate the processing or, as a second possibility, legislation could regulate what interests or purposes justify monitoring of employees. In addition, it should be further discussed how the role of fairness, social rights at work, good faith, right to health and safety (e.g. right to working environment that is suitable for employee's mental health), freedom of speech (e.g. right to express opinions on the internet and social media) and the need to respect the employee's dignity also influence the balancing test at hand. Furthermore, the specific nature of the sector and the job performed should play a large role to determine the level of intrusiveness allowed for monitoring schemes. It also seems that digital monitoring technologies (such as microchip implants) will find greater legitimation in more dangerous and adverse working sites prone to accidents. EU legislation should also specify what factors or steps need to be considered before monitoring is lawful. For example, the employer might be obliged to inform employees about digital monitoring methods and hear employees' views in this matter. Employees' representatives should also be involved in implementation and use of a privacy-invasive monitoring technology in workplace.

6.4 Special regulation on data processing principles

As discussed in my dissertation, the principles of data processing, specifically purpose limitation, fairness and transparency are broadly worded. This allows for monitoring practices in a digital workplace that are in line with the GDPR but still invade employee data protection rights and privacy.

Technological enhancements together with the spread of COVID-19 have contributed to an increase of monitoring in digital workplaces and volume of data generated in the work environment, which may lead employers to use technologies for purposes other than the ones originally planned and result in illegitimate further processing of employee data, generating the risk of 'function creep' and use of data purposes unintended by the employee. As a result, if the consequences of the monitoring are not reasonably expected by the employees, they would most likely be in breach of the principle of purpose limitation. This means that any monitoring activities and personal data collection that has been used to combat the COVID-19 pandemic must be ceased once it no longer serves the purpose of protecting employees' health. However, as discussed in the present dissertation, the end of the pandemic is a vague term and in addition, employers may hide secondary purposes in long, legalistic privacy policy fine print that is not unambiguous. Also, there is no specific knowledge what will happen to technologies used in a workplace after the virus has receded as the principle of purpose limitation conflicts the very idea of the data economy, which is to reuse data. Therefore, as there is a high risk of further use of data collected through digital

monitoring technologies, it can be argued that the principle of purpose limitation is too broadly worded and allows for monitoring practices that are in line with the GDPR but still invade data protection rights and privacy of employees. Due to the imbalance of power in an employment relationship, legislation is needed to strengthen employees' ability to reject digital monitoring technologies and the purposes that allow for employee monitoring should be more specifically regulated. For example, some member states allow specific digital monitoring technologies only if their use is permitted for the purposes enacted in legislation or collective agreements. A similar approach should be used in legislation at the EU level.

The principle of fairness is linked with numerous procedural safeguards that should support fair processing of data, however, the principle focuses on procedural fairness rather than substantive fairness. In order for the processing to be fair, it should be transparent and have a legal basis. However, these should not be the only criteria that determine whether the activities are considered fair. As argued in the present dissertation, the importance of contexts is crucial when it comes to assessing whether processing is fair. Mere adherence to the principles and other provisions of the GDPR does not necessarily mean that processing is fair. Digital monitoring technologies highlight that fairness should be examined in a more substantive way and for processing to be fair, fairness needs to be evaluated within the specific digital monitoring context, meaning that employers may monitor employees only in ways the employees would reasonably expect and not use the data in a manner that unjustifiably has a negative effect on employees. Also, employers should leave room for the employee's right to express opinions on these profiles whenever the behaviour does not seriously violate standards of decency and dignity of others and does not disclose business information. In addition, profiling groups of employees to assemble a larger portrait of the workforce might lead to out-of-context conclusions and attribute to a single employee characteristics not related to that individual and should therefore be considered unfair. Overall, it can be argued that the principle of fairness is too broadly worded, allowing for monitoring practices that are in line with the GDPR but still invade data protection rights and privacy of the employee. The ambiguity and narrow scope of the principle of fairness brings out the weakness of EU legislation in the context of employee monitoring and highlights the need for more specific rules for monitoring in the digital workplace.

Similarly, it can be argued that the principle of transparency is broadly worded and allows for invasive monitoring practices. Under the GDPR employees do not get adequate information at the right time concerning digital monitoring technologies as the employer is required to make the notification only a time (beginning of the monitoring) where it is not yet clear for the employees how they will be affected by monitoring. Also, employees are usually not consulted in the context of digital monitoring technologies and therefore are not able to understand how monitoring is carried out. On one hand, digital monitoring technologies enable covert monitoring as they often form the hidden part of a workplace and seamlessly overlap with work or rest time activities (e.g. allowing employees to carry out their work by starting up computers and equipment, reminding employees to

take rest breaks and allowing them to access cafeterias), which means that employees might not be aware of the monitoring or profiling taking place. On the other hand, if employees are aware that monitoring is taking place, they might feel anxiety and discomfort and self-censor their behaviour unnecessarily and unjustly. Due to the possibility of hidden monitoring and discomfort of employees, EU legislation should be enacted that obliges employers to periodically inform and communicate monitoring activities to employees. Furthermore, it should be mandatory for employers to consult employee representatives if they plan to implement digital monitoring technologies. If the monitoring is continuous, employers should require the consent of employee representatives before implementing such a measure and carry out regular consultations on the topic. In addition, information concerning employees' data and monitoring practices should not only be added to privacy policies, but the employer should be obliged to carry out trainings and visualize monitoring activities (such as signs posted at a workplace that indicate places where monitoring is taking place). Likewise, additional information should be given to employees such as specific details of monitoring, information on whether the private use of the company's technology is allowed and to what extent (such as internet use), what technological safeguards have been put in place and what the consequences of monitoring activities will be. In case employer uses digital monitoring technologies (e.g. RFID-enabled microchips, AI enabled workplaces) employees should also be aware of the specific times, actions and methods performed to process data. Therefore, employees should be informed when and how they are being monitored and, for example, know the location of sensors and readers and their monitoring radius. If employer is basing its decisions (e.g. performance bonuses, warning) on monitoring results, employees should have detailed knowledge about the effect the monitoring has on decision making and what data is being observed to reach a decision.

REFERENCES

Publications

Abril, P. S., Levin, A., Del Riego, A. Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee. – American Business Law Journal 2012/49 (1).

Adams, A. Technology and the Labour Market: the Assessment. – Oxford Review of Economic Policy 2018/34 (3).

Ajmal, A. M. *et al.* A First Look at Privacy Analysis of COVID-19 Contact Tracing Mobile Applications. – IEEE Internet of Things Journal 2020, arXiv:2006.13354 [cs.CR].

Ajunwa, I. Algorithms at Work: Productivity Monitoring Applications and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law. – Saint Louis University Law Journal 2018/63 (1).

Ajunwa, I., Crawford, K., Schultz, J. Limitless worker surveillance. – California Law Review 2017/105 (3).

Ajunwa, I. Workplace Wellness Programs Could be Putting Your Health Data at Risk. Harvard Business Review 19.01.2017. – https://hbsp.harvard.edu (25.08.2021).

Ajunwa, I, Crawford, K., Ford, J. Health and Big Data: An Ethical Framework for Health Information Collection by Corporate Wellness Programs. – The Journal of Law Medicine & Ethics 2016/44 (3).

Albin, E., Prassl, J. Fragmenting Work, Fragmented Regulation: The Contract of Employment as a Driver of Social Exclusion. In Freedland, M *et al.* (Eds) The Contract of Employment. OUP 2016.

Algorithmic Management – A Trade Union Guide. UNI Global Union 2020. – https://www.uniglobalunion.org (30.07.2021).

Anderson, A., Private Government: How employers rule our lives (and why we don't talk about it). Princeton University Press 2017.

Andmekaitse Inspektsioon. Töötajate isikuandmete töötlemisest koroonaviiruse kontekstis [Data Protection Inspectorate. Processing of personal data of employees in the context of the coronavirus.] 20.03.2020. – https://www.aki.ee (25.08.2021).

Andrade, N. Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights. In Fischer-Hübner, S., *et al.* (Eds.) Privacy and Identity Management for Life: 6th IFIP WG PrimeLife International Summer School. Springer 2011.

Article 29 Data Protection Working Party. Opinion 2/2017 on data processing at work. 2017 WP 249.

Article 29 Data Protection Working Party. Opinion 8/2014 On the On Recent Developments On The Internet Of Things. 2014 14/EN WP223.

Article 29 Data Protection Working Party. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. 2014 844/14/EN WP 217.

Article 29 Data Protection Working Party. Opinion 03/2013 on purpose limitation. 2013 00569/13/EN WP 203.

Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent. 2011 01197/11/EN WP187.

Article 29 Data Protection Working Party. Opinion 1/2010 on the concept of 'controller' and 'processor'. 2010 00264/10/ WP 169.

Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. 2007 01248/07/EN WP 136.

Article 29 Data Protection Working Party. Working document on the surveillance of electronic communications in the workplace. 2002 5401/01/EN WP 55.
Article 29 Data Protection Working Party. Opinion 8/2001 on the processing of personal data in the employment context. 2001 5062/01/EN/Final WP 48.
As employees return to the office, banks explore surveillance tech. – Reuters 21.05.2021.
Ball, K. Workplace surveillance: An overview. – Labour History 2010/51 (1).
Barzilay, A. R. Data Analytics at Work: A View From Israel on Employee Privacy and Equality in the Age of Data-Driven Employment Management. – Comparative Labor Law & Policy Journal 2019/40.
Berg, J., Furrer, M., Harmon, E., Rani, U., Silberman, M. S. Digital labour platforms and the future of work. International Labour Organization 2018. – www.ilo.org (30.07.2021).
Blainpain, R. (Ed.) Comparative labour law and industrial relations in industrialized market economies. Xth Edition. Alphen aan den Rijn: Kluwer Law International 2010.
Bodie, M. T., Cherry, M. A., McCormic, M. L., Tang, J. The Law and Policy of Big Data and People Analytics, University of Colorado Law Review 2016.
Bodie, M. T., McMahon, M. Employee Testing, Testing, Tracing, and Disclosure as a Response to the Coronavirus Pandemic. – Washington University Journal of Law and Policy 2020/64.
Bogg, A. Sham self-employment in the Supreme Court. – Industrial Law Journal 2012/41.
Bonner, W., Chiasson, M. If fair information principles are the answer, what was the question? An actor-network theory investigation of the modern constitution of privacy. – Information and Organization 2005/15 (4).
Boudreaux, B., DeNardo, M. A., Denton, S. W., Sanchez, R., Feistel, K., Dayalani, H. Data Privacy During Pandemics: A Scorecard Approach for Evaluating the Privacy Implications of COVID-19 Mobile Phone Surveillance Programs. Santa Monica, Calif.: RAND Corporation 2020.
boyd, d.n., Ellison, N. B. Social Network Sites: Definition, History, and Scholarship. – Journal of Computer Mediated Education 2007/13 (1).
Bradford, L., Aboy, M., Liddell, K. COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR and Data Protection Regimes. – Journal of Law and the Biosciences 2020/7 (1).
Broughton, A., Higgins, T., Hicks, B., Cox, A. Workplaces and social networking – The implications for employment relations. Brighton: Institute for Employment Studies, 2009.
Brown, S. R., Linden, M. F., Sullivan, E. J., Torres. J. J. May an Employer Require Its Employees to Use a Contact Tracing App? Jenner&Bloc 24.04.2020. – https://jenner.com (31.07.2021).
Brown, V. R., Vaughn, E. D. The Writing on the (Facebook) Wall: The Use of Social Networking Sites in Hiring Decision. – Journal of Business and Psychology 2011/26 (2).
Bruyer, R. Privacy: A Review and Critique of the Literature. – Alberta Law Review 2006/43 (3).
Brynjolfsson, E., Rock, D., Syverson, C. Artificial intelligence and the modern productivity paradox: A clash of expectations and statistics. Working Paper No. 24001, National Bureau of Economic Research, Cambridge 2017.
BusinessEurope. The GDPR in review: A good start but improvement necessary. Press release 24.06.2020. – https://www.businesseurope.eu (18.08.2021).
Bygrave, L. A. Data Privacy Law: An International Perspective. Oxford: Oxford University Press 2014.

Bygrave, L. A. The Place of Privacy in Data Protection Law. – University of New South Wales Law Journal 2001/24 (1).
Bygrave, L. A. Data Protection Pursuant to the Right to Privacy in Human Rights Treaties. – International Journal of Law and Information Technology 1998/6 (12).
Bygrave, L. A., Schartum, D. W. Consent, Proportionality and Collective Power. In Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., Nouwt, S. Reinventing Data Protection? Springer 2009.
Callewaert, J. Do we still need Article 6(2) TEU? Considerations on the absence of EU accession to the ECHR and its consequences. – Common Market Law Review 2018/55 (6).
Carpenter, D., McLeod, A., Hicks, C., Maasberg, M. Privacy and Biometrics: An Empirical Examination of Employee Concerns. – Information Systems Frontiers 2018/20.
Carr, C. T. An Uncertainty Reduction Approach to Applicant Information-Seeking in Social Media: Effects on Attributions and Hiring. In Landers, R. N., Schmidt, G. B. (Eds.) Social Media in Employee Selection and Recruitment. Theory, Practice, and Current Challenges. Springer International Publishing Switzerland 2016.
Cate, F. H. The Failure of Fair Information Practice Principles. In Winn, J. K (Ed.) Consumer Protection in the Age of the 'Information Economy'. Routledge 2006.
Chesler, C. Coronavirus will turn your office into a surveillance state. – Wired Daily. 04.05.2020.
Clark, L. A., Roberts, S. J. Employer's use of social networking sites: A socially irresponsible practice. – Journal of Business Ethics 2010/95 (4).
COVID-19 and the world of work: Impact and policy responses. International Labour Organization 2020. – https://www.ilo.org/ (31.07.2021).
COVID-19 Resources Library. Global Privacy Assembly. – https://globalprivacyassembly.org (31.07.2021).
Crawford, K. When Fitbit Is the Expert Witness. The Atlantic 19.11.2014. – https://www.theatlantic.com (24.08.2021);
Custers, B., Ursic, H. Worker Privacy in a Digitalized World under European Law. – Comparative Labour Law and policy 2018/39.
Custers, B. Data Dilemmas in the Information Society: Introduction and Overview. In Custers, B., Calders, T., Schermer, B., Zarsky, T. (Eds.) Discrimination and Privacy in the Information Society. Springer International Publishing 2013.
Custers, B., van der Hof, S., Schermer, B., Appleby-Arnold, S., Brockdorff, N. – SCRIPTed 2013/10 (4).
Coxworth, B. SmartCap Monitors Workers' Fatigue Levels by Reading Their Brain Waves. New Atlas 31.01.2012. – https://newatlas.com (19.082021).
Davis, J. Google Sued, Lawsuit Claims COVID-19 Contact Tracing Tool Exposes Data. – Health IT Security 30.04.2021.
Davis, J. PA Health Dept Sued; Investigation Looms, After Contact Tracing Breach. – Health IT Security 10.05.2020.
Davison, H. K., Bing, M. N., Kluemper, D. H., Roth, P. L. Social Media as a Personnel Selection and Hiring Resource: Reservations and Recommendations. In Landers, R. N., Schmidt, G. B. (Eds.) Social Media in Employee Selection and Recruitment. Theory, Practice, and Current Challenges. Springer International Publishing Switzerland 2016.
Davison, H. K., Maraist, C.C., Hamilton, R. H., Bing, M.N. To Screen or Not to Screen? Using the Internet for Selection Decisions. – Employee Responsibilities and Rights Journal 2012/24 (1).

Data Protection Laws of the World. Portugal. DLA Piper 2021. – www.dlapiper.com (24.08.2021).
Digitalization and decent work implications for Pacific Island Countries. International Labour Organization 2019. – https://www.ilo.org (30.07.2021).
van Dijck, J. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. – *Surveillance & Society 2014/12 (2).*
Esfola, J. P. M. Bar Coded at Work. LL.M. Law & Technology. Tilburg Institute of Law, Technology and Society (TILT). – http://arno.uvt.nl/show.cgi?fid=146486 (30.07.2021).
Eurofound. Employee monitoring and surveillance: The challenges of digitalisation. Luxembourg: Publications Office of the European Union 2020.
Eurofound. Game-changing technologies: Transforming production and employment in Europe. Luxembourg: Publications Office of the European Union 2020.
European and Middle East Guide to Monitoring of Employees in the Workplace. Meritas 2018. – www.meritas.org (29.08.2021).
European Commission. Big data. – https://ec.europa.eu/digital-single-market/en/big-data (30.07.2021).
European Commission. Biometrics technologies: A key enabler for future digital services 2018.
European Commission. EU strategic framework on health and safety at work 2021–2027 Occupational safety and health in a changing world of work. – COM(2021) 323 final.
European Commission. Mobile applications to support contact tracing in the EU's fight against COVID-19. 2020 – https://ec.europa.eu (31.07.2021).
European Commission. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts. – COM/2021/206 final.
European Commission. Questions and Answers – Data protection reform. 21.12.2015) – http://europa.eu (31.07.2021).
European court sides with worker in landmark privacy ruling. Deutsche Welle 2017. – http://www.dw.com.
European Data Protection Board. Statement on the processing of personal data in the context of the COVID-19 outbreak. 19.03.2020.
European Data Protection Board. Guidelines 07/2020 on the concepts of controller and processor in the GDPR. 02.09.2020.
European Data Protection Board. Guidelines 05/2020 on consent under Regulation 2016/679. 04.05.2020.
European Data Protection Supervisor. Orientations from the EDPS. Reactions of EU institutions as employers to the COVID-19 crisis. 15.07.2020.
European social partners framework agreement on digitalisation. ETUC, BusinessEurope, CEEP and SMEUnited. Brussels (2020). – https://www.etuc.org (31.07.2021).
European Parliament resolution of 21 January 2021 with recommendations to the Commission on the right to disconnect 2019/2181(INL).
European Trade Union Confederation. ETUC resolution on digitalisation: Towards fair digital work. 2016. – https://www.etuc.org (31.07.2021).
European Trade Union Institute. Labour in the age of AI: Why regulation is needed to protect workers. 2020. – https://www.etui.org (31.07.2021).
European Union Agency for Fundamental Rights, European Data Protection Supervisor, the Council of Europe. Handbook on European data protection law. 2018 edition. Luxembourg: Publications Office of the European Union 2018.

Fabbrini, F. The European Multilevel System for the Protection of Fundamental Rights: A 'Neo-Federalists' Perspective. Jean Monnet Working Paper 2010/15 – https://jeanmonnetprogram.org (31.07.2021).
Finkin, M. W. Privacy: Its Constitution and Vicissitude – A Half-Century On. – Canadian Labour & Employment Law Journal 2015/18.
Fischbach, K. *et al.* Analyzing the Flow of Knowledge with Sociometric Badges – Procedia – Social and Behavioral Sciences 2010/2 (4).
Fitbit. Help employees build healthy habits across key areas of their health and wellbeing. – https://www.fitbit.com (25.08.2021).
Floridi, L. Mind the App – Considerations on the Ethical Risks of COVID-19 Apps. – Philosophy & Technology 2020/33.
Ford, M. Article 8 and the Right to Privacy at the Workplace. In Ewing K. D. (Ed.) Human Rights at work. Institute of Employment Rights 2000.
Fragala, M. S., Goldberg, Z. N., Goldberg, S. E. Return to Work: Managing Employee Population Health During the COVID-19 Pandemic. – Population Health Management 2021/24 (1).
Fragale, R., Jeffery, M. Information Technology and Workers' Privacy: Notice and Consent. – Comparative Labour Law & Policy Journal 2005/23.
French Implementation of the GDPR. Ahmed Baladi, Gibson, Dunna & Chrutcher. Thomson Reuter 2019. – https://www.gibsondunn.com (31.07.2021).
Galloway, K. The COVID cyborg: protecting data status. – Alternative Law Journal 2020/45 (3).
Gauttier, S. I've got you under my skin' – The role of ethical consideration in the (non-) acceptance of insideables in the workplace. – Technology in Society 2019/56.
German Data Protection Supervisory Authorities joint information paper on data protection and the Coronavirus pandemic. Datenschutzrechtliche Informationen zur Verarbeitung von personenbezogenen Daten durch Arbeitgeber und Dienstherren im Zusammenhang mit der Corona-Pandemie. – https://www.bfdi.bund.de (25.08.2021).
Gille, D., Wohlgemuth, S., Strüker, J. RFID in Germany in A Structured Collection on Information and Literature on Technological and Usability Aspects of Radio Frequency Identification. Future of Identity in the Information Society 2007.
Ghoshal, S. Open book? In India, where people are forced to download a tracking app to get paid, journalists are worried about it also being used to access their contacts. – Index on Censorship 2020/49 (2).
Govaert, M. van Beers, A., Daniels, C. The Right To Disconnect. Global Workplace Insider 25.03.2021. – www.globalworkplaceinsider.com (25.08.2021).
Greenbaum, D. Ethical, Legal and Social Concerns Relating to Exoskeletons. – CM SIGCAS Computers and Society 2015/45 (3).
Guilfoyle, S., Bergman, S. M., Hartwell C., Powers, J. Social Media, Big Data, and Employment Decisions: Mo' Data, Mo' Problems? In Landers, R. N., Schmidt, G. B. (Eds.) Social Media in Employee Selection and Recruitment. Theory, Practice, and Current Challenges. Springer International Publishing Switzerland 2016.
Halperin, D., Heydt-Benjamin, T. S., Fu, K., Kohno, T., Maisel W. H. Security and privacy for implantable medical devices. – IEEE Pervasive Computing 2008/7 (1).
Harwell, D. Tracking your pregnancy on an app may be more public than you think. – The Washington Post 10.04.2019.
Heald, D. Varieties of Transparency. In Hood, C., Heald, D. (Eds.) Transparency: The Key to Better Governance? British Academy 2006.

Hendrickx, F., Taes, S., Wouters, M. Covid-19 and labour law in Belgium. – European Labour Law Journal 2020/11 (3).
Henshall, A. Governments have long been trying to enact laws to give workers the right to log off BBC 21.05.2021.– https://www.bbc.com (25.08.2021).
De Hert, P., Gutwirth, S. Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. In Claes, E., Duff A., Gutwirth, S. (Eds.) Privacy and the criminal law. Antwerp/Oxford: Intersentia, 2006.
Hildebrandt, M., Backhouse, J. (Eds.), D7.2: Descriptive analysis and inventory of profiling practices. FIDIS 2005.
Hodder, A. New Technology, Work and Employment in the era of COVID-19: reflecting on legacies of research. – New Technology, Work and Employment 2020/35 (3).
van Hoecke, M. Legal doctrine: which method(s) for what kind of discipline? In van Hoecke M. (Ed.) Methodologies of legal research: what kind of method for what kind of discipline? Oxford: Hart Publications 2011.
Holmes, N. Wearable Technology within the Workplace. CONVENE. – https://convene.com (19.08.2021).
Hoven, J.vd., Weckert, J. (Eds) Information Technology and Moral Philosophy. New York: Cambridge University Press 2008.
Hungarian National Authority for Data Protection and Freedom of Information. Information on processing data related to the coronavirus epidemic. 2020. – https://www.naih.hu (25.08.2021).
Hutchinson, T., Duncan, N. Defining and describing what we do: doctrinal legal research. – Deakin Law Review 2012/17 (1)).
ILO Monitor: COVID-19 and the world of work. Sixth edition. International Labour Organization 2020. – https://www.ilo.org/global (31.07.2021).
Information Commissioner's Office (UK). Consent. – https://ico.org.uk/ (25.08.2021).
Inness, J. C. Privacy, Intimacy, and Isolation. Oxford University Press 1992.
International Labour Organisation, Non-Standard Employment around the World: Understanding Challenges, Shaping Prospect. Geneva: International Labour Office 2016.
Introna, L. D., Pouloudi, A. Privacy in the information age: Stakeholders, interests and values. – Journal of Business Ethics 1999/22 (1).
Ivask, E.-L. The Use of Facebook as Evaluation Method for Job Candidates in Service Sector Organizations. Bachelor Thesis. University of Tartu 2013.
Jeffrey, B., Ludlow, K., Testa, L., Herkes, J., Augustsson, H., Lamprell, G., McPherson, E., Zurynsk, Y. Built to last? The sustainability of healthcare system improvements, programmes and interventions: a systematic integrative review. – BMJ Open 2020/10 (6).
Johnson, E. School custodian refuses to download phone app that monitors location, says it got her fired. – CBC News 12.04.2021.
van den Joven, M. J., Weckert, J. Information Technology and Moral Philosophy. Cambridge University Press 2008.
Kanarbik, L. Võtmed naha all ehk Miks Ülemiste linnaku töötajad end kiibistada lasevad [The keys under the skin, i.e. Why the employees of Ülemiste City let themselves be implanted with a microchip]. – Eesti Päevaleht 11.10.2018.
Kanngieser, A. Tracking and tracing: geographies of logistical governance and labouring bodies. – Environment and Planning D: Society and Space 2013/31.
Kaplan, A. M., Haenlein, M. Users of the world, unite! The challenges and opportunities of Social Media. – Business Horizons 2010/53 (1).

Karyda, M., Gritzalis, S., Park, J. H., Kokolakis, S. Privacy and fair information practices in ubiquitous environments: Research challenges and future directions. – Internet Research 2009/19 (2).
Kędzior, M. The right to data protection and the COVID-19 pandemic: the European approach. – ERA Forum 2021/21.
Kinni, T. Monitoring Your Employees' Every Emotion. – MITSloan 15.09.2016.
Kitchin, R. Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of COVID-19. – Space & Polity 2020/24 (3).
Kitchin, R. The data revolution: Big data, open data, data infrastructures & their consequences. London 2014.
van Kolfschooten, H., de Ruijter, A. COVID-19 and privacy in the European Union: A legal perspective on contact-tracing". – Contemporary Security Policy 2020/41 (3).
Kollewe, J. Alarm over talks to implant UK employees with microchips. – The Guardian 11.11.2018.
Koops, B.-J. The trouble with European data protection law. – International Data Privacy Law 2014/4 (4).
Koops, B.-J. On decision transparency, or how to enhance data protection after the computational turn. In Hildebrandt, M., de Vries K (Eds.) Privacy, Due Process and the Computational Turn. Abingdon Routledge 2013.
Kretzschmar, M. E. *et al*. Impact of Delays on Effectiveness of Contact Tracing Strategies for COVID-19: A Modelling Study. – The Lancet Public Health 2020/5 (8).
Kuner, C. European Data Protection Law: Corporate Compliance and Regulation. Oxford University Press 2007.
Köffer S. Designing the digital workplace of the future – what scholars recommend to practitioners. International Conference on Information Systems 2015.
Landers, R. N., Schmidt, G. B. Social Media in Employee Selection and Recruitment: An Overview. In Landers, R. N., Schmidt, G. B. (Eds.) Social Media in Employee Selection and Recruitment. Theory, Practice, and Current Challenges. Springer International Publishing Switzerland 2016.
Lamoureux, S. Implementing the General Data Protection Regulation. The experiences of three Finnish organizations. Master's thesis in Governance of Digitalization. Åbo Akademi 2020.
Lasprogata, G., King, N. J., Pillay, S. Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada. – Stanford Technology Law Review 2004/4.
Lo, B., Sim, I. Ethical Framework for Assessing Manual and Digital Contact Tracing for COVID-19. – Annals of Internal Medicine 2021/174 (3).
Luca, B., Schwartz, M., Louzada, L. Selling Your Soul While Negotiating The Conditions: From Notice And Consent To Data Control By Design. – Health and Technology 2017/7 (4).
Lynskey, O. The Foundations of EU Data Protection Law. Oxford University Press 2015.
Mascheroni, G., Siibak, A. Datafied childhoods: data practices and imaginaries in children's lives. New York: Peter Lang 2021.
Managing human resources is about to become easier. – The Economist 28.03.2018.
Mangan, D., Gramano, E., Kullmann, M. An unprecedented social solidarity stress test. – European Labour Law Journal 2020/11 (3).

Mangan, D. Online Speech and the Workplace: Public Right, Private Regulation. – Comparative Labour Law & Policy 2018/39.
Marks, A., Briken, K., Chillas, S., Krzywdzinski, M. The New Digial Workplace: How New Technologies Revolutionise Work. Macmillan Publishers Limited 2017.
Mathiason *et al*. The Transformation of the Workplace Through Robotics, Artificial Intelligence, and Automation. Littler reports January 2016. – https://www.littler.com (19.08.2021).
McConville, M., Chui, W. H. Introduction and Overview. In McConville, M., Chui, W. H. (Eds.) Research Methods for Law. UK: Edinburgh University Press 2017.
McKinsey & Company. How COVID-19 has pushed companies over the technology tipping point – and transformed business forever. Survey 2020. – https://www.mckinsey.com (31.07.2021).
McNall, L. A., Stanton, J. M. Private eyes are watching you: Reactions to location sensing technologies. – Journal of Business and Psychology 2011/26.
MHI. Automatic Identification and Data Collection. – https://www.mhi.org/fundamentals/automatic-identification (30.07.2021).
Miller, A. More Companies Are Using Technology to Monitor Employees, Sparking Privacy Concerns. – ABCNEWS 10.03.2018.;
Mitrou, L. Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'? – SSRN 2018.
Moore, A. D. Employee Monitoring and Computer Technology: Evaluative Surveillance v. Privacy. – Business Ethics Quarterly 2000/10 (3).
Moore, P., Upchurch, M., Whittaker, X. (Eds.) Humans and Machines at Work. Monitoring, Surveillance and Automation in Contemporary Capitalism. Palgrave Macmillan 2018.
Moreham, N. A. Privacy in the Common Law: A Doctrinal and Theoretical Analysis. Law Quarterly Review 2005/121.
Nadeem, A. *et al*. A Survey of COVID-19 Contact Tracing Apps. – IEEE Access 2020/8.
Newlands, G., Lutz, C., Tamo'-Larrieux, A. Villaronga, E. F., Harasgama, R., Scheitlin, G. Innovation under pressure: Implications for data privacy during the Covid-19 pandemic. – Big Data & Society 2020/7 (2).
Nissenbaum, H. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press 2009.
Non-tech business are beginning to use artificial intelligence at scale. – The Economist 28.03.2018.
Office of the Privacy Commissioner of Canada. Radio Frequency Identification (RFID) in the Workplace: Recommendations for Good Practices 2008. – https://www.priv.gc.ca/en (30.07.2021).
Oliver, H. E-mail and Internet Monitoring in the Workplace: Information Privacy and Contracting-Out. –Industrial Law Journal 2002/31.
Olson, P. Fitbit Data Now Being Used in the Courtroom. Forbes 16.11.2014 – https://www.forbes.com (24.08.2021).
Organic Law 3/2018, of December 5, Protection of Personal Data and Guarantee of Digital Rights. ECIJA 11.12.2018. – https://ecija.com (25.08.2021).
Oswald, M., Grace, J. The COVID-19 Contact Tracing App in England and 'Experimental Proportionality'. – Public Law 2021.
Otto, M. The Right to Privacy in Employment: A Comparative Analysis. Oxford, UK: Hart Publishing 2016.

Padi, J. Big data analytics, consent and the European Union (EU) General Data Protection Regulation 2016 (GDPR) – The fallacy of consent and control. Dissertation, Keele University 2018.
Pangrazio, L., Selwyn, N. 'Personal data literacies': A critical literacies approach to enhancing understandings of personal digital data. – New Media & Society 2019/21 (2).
Paresh, D. Companies bet on AI cameras to track social distancing, limit liability. – Reuters 27.04.2020.
Patil D., Mason, H. Data Driven. Creating a Data Culture. O'Reilly Media 2015.
Pedersen, I., Iliadis, A. (Eds.) Embodied computing. Wearables, implantables, embeddables, ingestibles. The MIT Press 2020.
Peruffo, E., Rodriguez Contreras, R., Mandl, I., Bisello, M. Game-changing technologies: Transforming production and employment in Europe. Eurofound 2020.
Peyton, A. The Connected State of Things: A Lawyer's Survival Guide in an Internet of Things World. – Catholic University Journal of Law and technology 2016/24.
Poullet, Y. Data protection legislation: What is at stake for our society and democracy? – Computer Law & Security Review 2009/25 (3).
Prassl, J. What If Your Boss Was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work. – Comparative Labor Law & Policy Journal 2019/41 (1).
Purtova, N. Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver in European Data Protection Rights. – Netherlands Quarterly of Human Rights 2010/28 (2).
Raley, R. Dataveillance and Countervailance. In Gitelman, L. (Ed) 'Raw Data' is an Oxymoron. Cambridge, MA: MIT Press 2013.
Raskar, R. *et al*. Apps Gone Rogue: Maintaining Personal Privacy in an Epidemic. 2020. – arXiv:2003.08567 [cs.CR].
Riemer, K., Ciriello, R., Peter, S., Schlagwein, D. Digital contact-tracing adoption in the COVID-19 pandemic: IT governance for collective action at the societal level. – European Journal of Information Systems 2020/29 (6).
Roagna, I. Protecting the right to respect for private and family life under the European Convention on Human Rights, Council of Europe human rights handbooks. Council of Europe Strasbourg 2012.
Robinson, N., Graux, H., Botterman, M., Valer, L. Review of the European Data Protection Directive, Santa Monica, Calif.: RAND Corporation 2009.
Robitzski, D. How A.I. Exoskeletons Could Make People Super-Human. INVERSE 22.06.2017. – https://www.inverse.com (19.08.2021).
Rodrigues, M. G., Bairrão, I. New Portuguese Data Protection Act. Garriues – Lexology 13.08.2019.
Rogers, A. We Try a New Exoskeleton for Construction Workers. – WIRED 28.04.2015.
Roosendaal A. P. C., Kosta, E. A study on ICT implants. FIDIS Deliverables; No. D12.6). FIDIS 2008. – http://www.fidis.net (30.07.2021).
Ropes&Grey. Going Back to Work: Employer Use of 'Apps' on Employee PDAs/Smart Phones for COVID-19 Contact Tracing". Ropes&Grey 01.05.2020. – https://www.ropesgray.com (25.08.2021).
Rouvroy., A., Poullet, Y. The right to informational self-determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In Gutwirth S., Poullet Y., De Hert P., de Terwangne C., Nouwt S. (Eds.) Reinventing Data Protection? Springer 2009.

Sadeghian, P., Abdollahian, F., Hamidi, K. Workplace surveillance: review of surveillance and control of workplace. – Advanced Social Humanities and Mangement 2017/4 (1).
Sahinyilmaz, T. Worldwide: Biometric Authentication In The Workplace In Terms Of Employee Privacy. Mondaq 16.03.2021. – https://www.mondaq.com (25.08.2021).
Scassa, T. COVID-19 Contact Tracing: From Local to Global and Back Again. – International Journal of E-Planning Research, IGI Global 2021/10 (2).
Scassa, T., Chiasson, T., Deturbide, M., Uteck, A. An Analysis of Legal and Technological Privacy Implications of Radio Frequency Identification Technologies. Report Prepared under the Contributions Program of the Office of the Privacy Commissioner of Canada 2005. – https://libraries.dal.ca (30.07.2021).
Schmidt, G., O'Connor, K. W. Social Media, Data Privacy, and the Internet of People, Things, and Services in the Workplace: A Legal and Organizational Perspective. In Simmers, C., Anandarajan, M. (Eds.) The Internet of People, Things and Services. Workplace Transformations. Routledge 2018.
Shemer, S. Could A New Israeli App Help Tackle COVID-19 Tracing In the Workplace? – NoCamels 24.01.2021.
Simits, S. Reconsidering the Premises of labour Law. – European Law Journal 1999/5 (1).
Singhal, A. K., Malik. I. Doctrinal and socio-legal methods of research: merits and demerits. – Educational Research Journal 2012/2 (7).
Solove, D. J. Privacy Self-Management and the Consent Dilemma. – Harvard law Review 2013/126.
Solove, D. J. A Taxonomy of Privacy. – University of Pennsylvania Law Review 2006/154.
Solove, D. J. Conceptualizing Privacy. – California Law Review 2002/90 (4).
Spears, J. L., Padyab, A. Privacy risk in contact tracing systems – Behaviour & Information Technology 2021.
Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union. TNS Opinion & Social 2011.
Sprague, R. Survey of (Mostly Outdated and Often Ineffective) Laws Affecting Work-Related Monitoring: The Piper Lecture. – Chicago-Kent College of Law Review 2018/93.
Sprague, R. Invasion of the Social Networks: Blurring the Line between Personal Life and the Employment Relationship. – University of Louisville Law Review 2011/50.
Stack, M. B. Wearable Technology in Workers' Compensation. AMAXX 27.07.2017. – https://blog.reduceyourworkerscomp.com (02.08.2021).
Suemo. J. 12 most asked questions on EU employee monitoring laws. Worktime 13.10.2020. – https://www.worktime.com (25.08.2021).
Sugarman, S. D. Lifestyle Discrimination in Employment. – Berkeley Journal of Employment and Labor Law 2003/24 (2).
Swaya M. E., Eisenstein, S. R. Emerging Technology in the Workplace. – The Labor Lawyer 2005/21 (1).
Zuboff, S. The age of surveillance capitalism: The fight for a human future at the new frontier of power. New York: PublicAffairs 2019.
Tagvoryan, A., Iley, B. T., Oberly, D. J. Learn the Rules on Employers' Use of Biometric Data. SHRM 01.04.2019. – https://www.shrm.org (25.08.2021).
Tene, O. Privacy: The New Generations. – International Data Privacy Law 2011/1 (1).
There will be little privacy in the Workplace of the Future. – The Economist 28.03.2018.
Thiesse, F. RFID, privacy and the perception of risk:A strategic framework. – The Journal of Strategic Information Systems 2007/16 (2).

Thomas, L. France Continues to Focus on Use of Biometrics. SheppardMullin 2.04.2019. – https://www.eyeonprivacy.com (25.08.2021).
Tikkinen-Piri, C EU General Data Protection Regulation: Changes and implications for personal data collecting companies. – Computer law & security review 2017/34 (1).
Topo, A., Razzolini, O. The Boundaries of the Employer's Power to Control Employees in the ICTs Age. – 39 Comparative labour Law & Policy, 2018/39.
Torpey, J. Through thick and thin: Surveillance after 9/11. – Contemporary Sociology 2007/36 (2).
Tran, A. H. The Internet of Things and Potential Remedies in Privacy Tort Law. – Columbia Journal of Law and Social Problems 2017/50 (2).
Troiano, A. Wearables and Personal Health Data: Putting a Premium on Your Privacy. – Brooklyn Law Review 2017/82.
Tsao, C. L., Haskins, K. J., Hall, B. D. The Rise of Wearable and Smart Technology in the Workplace, ABA National Symposium on Technology in Labor and Employment Law 2017.
Urs, G., Ienca, M., Scheibner, J., Sleigh, J., Vayena, E. Digital tools against COVID-19: Framing the ethical challenges and how to address them. 2020. arXiv:2004.10236.
Valentino-DeVries, J. Bosses May Use Social Media to Discriminate Against Job Seekers. – The Wall Street Journal 20.11.2013.
Valerio De S. Negotiating the algorithm. Automation, artificial intelligence and labor protection. – Comparative Labor Law & Policy Journal 2019/41 (1).
Vatcha, A. Workplace Surveillance Outside the Workplace: An Analysis of E-Monitoring Remote Employees. – iSCHANNEL 2020/15 (1).
Vick, D. W. Interdisciplinary and the Discipline of Law. – Journal of Law and Society 2004/31.
Vinson, K. E. The blurred boundaries of Social Networking in the Legal Field: Just 'Face' it. – University of Memphis Law Review 2010/41.
Visamaa, K. Veebipõhiste sotsiaalvõrgustike kasutamine töötajate värbamisel [The use of social networking sites in recruitment], Bachelor thesis. University of Tartu 2011.
Vogeler, W. Technology Is Quickly Reshaping Workers' Compensation Claims, FindLaw 24.02.2017. – https://blogs.findlaw.com (19.08.2021).
Voigt, P., Bussche, A. The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer International Publishing 2017.
Waas, B., van Voss, G. H. (Eds), Restatement of Labour Law in Europe: Volume I . Oxford: Hart Publishing 2017.
Wachter, S., Mittelstadt, B. D. A right to reasonable inferences: Re-thinking data protection law in the age of Big Data and AI. – Columbia Business Law Review 2019/1.
Warren, S. D., Brandeis, L. D. The Right to Privacy. – Harvard Law Review 1890/4 (5).
Watkins, K. Security and Privacy of COVID-19 Contact-Tracing Apps. Symantec Enterprise Blogs 2021. – https://symantec-enterprise-blogs.security.com (30.07.2021).
Watts, D. COVIDSafe, Australia's Digital Contact Tracing App: The Legal Issues. – SSRN 2020.
Weil, D. The Fissured Workplace: Why Work Became so Bad for so Many and What Can Be Done to Improve it. Harvard University Press 2014.
Weiss, M. The future of comparative labor law as an academic discipline and as a practical tool. Comparative Labor Law and Policy Journal 2003/25.
Westerlund, M. A Study of EU Data Protection Regulation and Appropriate Security for Digital Services and Platforms. Åbo: Åbo Akademi University Press 2018.
Westin, A. F. Privacy and Freedom. – Washington and Lee Law Review 1968/25 (1).

Whelan, E., McDuff, D., Gleasure, R., Brocke, J. How Emotion-Sensing Technology Can Reshape the Workplace. – MITSloan 05.02.2018.
Wilhelm, E. O. Bărbulescu ruling: Workplace privacy is alive and kicking, IAPP Privacy Tracker 2017. – https://iapp.org.
Williams, A., Georgopoulou, S. France: CNIL standard on processing personal data for the purpose of human Resources. DataGuidance June 2020. – https://www.dataguidance.com (25.08.2021).
Wilson, G. Comparative Legal Scholarchip. In McConville, M., Chui, W. H. (Eds.) Research Methods for Law. UK: Edinburgh University Press 2017.
Williams, S. P., Schubert, P. Designs for the Digital Workplace. – Procedia Computer Science 2018/138.
Wilson, H. J. Wearables in the Workplace. Harvard Business Review September 2013. – https://hbr.org (25.08.2021).
Workplace Monitoring: What Are Your Employees' Rights? GDPRinformer 20.09.2017. – https://gdprinformer.com (25.08.2021)
World Health Organization. Contact tracing in the context of COVID-19: interim guidance. 2020. – https://apps.who.int (31.07.2021).
Yang, X. Workforce Survival: Tracking Potential COVID-19 Exposure Amid Socio-economic Activities Using Automatic Log-Keeping Apps. – Population Health Management 05.04.2020.
Yasaka, T. M., Lehrich, B. M., Sahyouni, R. Peer-to-peer contact tracing: Development of a privacy-preserving smartphone app. – JMIR Mhealth Uhealth 2020.
Yeginsu, C. If Workers Slack Off, the Wristband Will Know. (And Amazon Has A Patent For It.). – The New York Times 01.02.2018.

Legal Acts

Charter of Fundamental Rights of the European Union. – OJ L 2012/C 326/02.
Convention for the Protection of Human Rights and Fundamental Freedoms. Rome 4.11.1950.
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Union. – L 281, 23.11.1995, 31–50.
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). – OJ L 119 4.5.2016, p. 1.

National Laws

Australia
Privacy Amendment (Public Health Contact Information) Act 2020, No. 44, 2020.

Finland
Act on the Protection of Privacy in Working Life (759/2004). – http://ilo.org/dyn/natlex (18.08.2021)

France
Data Protection Act, Law 2018-493 of 20 June 2018.

Portugal
Data Protection Act law no 58/2019 of 8 August. Diário da República n.º 151/2019, Série I de 2019-08-08.
Labour Code 7/2009. Diário da República n.º 30/2009, Série I de 2009-02-12.

Spain
Organic Law 3/2018 of December 5, on Data Protection and Guarantee of Digital Rights.

Case law

ECtHR 5856/72, Tyres v. The United Kingdom.
ECtHR 13710/88, Niemietz v. Germany.
ECtHR 27798/95, Amann v Switzerland.
ECtHR 6959/75, Bruggemann and Scheuten v. Federal Republic of Germany.
ECtHR 20605/92, Halford vs The United Kingdom.
ECtHR 420/07, Köpke v Germany.
ECtHR 61496/08, Bărbulescu v Romania.
ECtHR 62617/00, Copland v. the United Kingdom.
ECtHR 70838/13, Antović and Mirković v Montenegro.
ECtHR 1874/13 López Ribalda and Others v Spain.
ECtHR 32792/05, Pay v UK.

US case law
Katz v. United States, 389 U.S. 347 (1967).
Gonzales v. Uber Techs., Inc., 305 F. Supp. 3d 1078 (N.D. Cal. 2018).
U.S. v Simons, 206 F.3d 392 (4th Cir. 2000).
City of Ontario, California *et al*. vs Quon *et al*., 560 U.S. 746 (2010).

Court of Justice of the European Union
CJEU C-101/01, Bodil Lindquist.
CJEU C-582/14, Patrick Breyer v Bundesrepublik Deutschland.
CJEU C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.

Canada
Eastmond v. Canadian Pacific Railway (11.06.2004). The Judgement of the Federal Court of Australia. No FC852.

Italy
The Cassazione 10955/2015. – www.iusexplorer.it.

Germany
Bundesarbeitsgericht [The German Federal Labor Court] 27.07.2017, case no. 2 AZR 681/16.

ABBREVIATIONS

AI – artificial intelligence
ECHR – European Convention for the Protection of Human Rights and Fundamental
ECtHR – European Court of Human Rights
EDPB – European Data Protection Board
GDPR – General Data Protection Regulation
RFID – radio frequency identification

ACKNOWLEDGEMENTS

I would like to thank my supervisors Professor Merle Erikson and Professor Andra Siibak for their feedback, support, and discussions. I would like to express my gratitude to Merle for giving me comprehensive guidance throughout my doctoral studies. I would like to thank Andra who inspired, encouraged, and helped me both to generate and to carry out my ideas. Without their support I could not have completed this dissertation.

I am also grateful to Professor Irene Kull for her encouragement and constructive criticism, that enabled me to sharpen the focus of my thesis.

I would like to thank the research project "Conceptualisations and experiences with public and private in technologically saturated society" PUT44, financed by Estonian Research Council, and Archimedes Foundation for allowing me to make various research visits during the course of my PhD studies.

And last, but definitely not least, I would also like to thank my colleagues and friends for their reassurance, and my deepest gratitude goes to my loving and caring family members who have always encouraged me to pursue my goals.

SUMMARY IN ESTONIAN

Töötaja privaatsuse kaitse digitaalsel töökohal

1. Eesmärk ja uurimisküsimused

Tänapäeva töökohad digitaliseeruvad üha enam.[394] Digitaliseerumine on loonud tööandjatele ja töötajatele mitmeid majanduslikke ja ühiskondlikke eeliseid, sealhulgas on suurenenud paindlikkus ja autonoomia töösuhetes ning tekkinud paremad võimalused töö- ja eraelu ühildamiseks. Teisalt on tehnoloogia areng töö kontekstis tekitanud ka mitmeid eetilisi ja õiguslikke probleeme. Üheks väljakutseks on töötajate jälgimine ja nende kohta andmete kogumine digitaalsete tehnoloogiate abil. Digitaalseid jälgimistehnoloogiaid arendatakse järjepidevalt ja nende funktsioonid muutuvad aina mitmekülgsemaks. Uued rakendused ja nutiseadmed võimaldavad tööandjatel koguda hulgaliselt töötajate isikuandmeid paljudest erinevatest allikatest, tehes seda tööandja jaoks mõistliku aja jooksul ja taskukohase hinnaga. Taoliste tehniliste võimaluste olemasolu võib kergelt viia töötaja isikuandmete kaitse reeglite rikkumise ja privaatsust riivava käitumiseni. Tuues näiteid erinevatest digitaalsel töökohal kasutatavatest tehnoloogiatest uurib käesolev doktoritöö, kuidas Euroopa Liidu privaatsus- ja andmekaitseraamistik tuleb antud väljakutsega toime ning kuivõrd suudab kaitsta töötajat privaatsust riivava jälgimise eest töökeskkonnas.

Doktoritöö põhineb viiel eelretsenseeritud teadupublikatsioonil ja keskendub privaatsuse ning andmekaitse küsimustele, mis käsitlevad kolme digitaalset jälgimistehnoloogiat – töötaja sotsiaalmeedia jälgimine (publikatsioonid I–II), mikrokiibistatud töötajate jälgimine (publikatsioon III) ja kontaktide tuvastamist võimaldavate rakenduste abil töötajate jälgimine COVID-19 leviku ajal (publikatsioon IV–V). Publikatsioonid hõlmavad eeltoodud jälgimispraktikaid nende uudsuse tõttu ja seetõttu, et need võimaldavad koguda hulgaliselt andmeid, sealhulgas eraelulisi andmeid töötaja kohta ning teha seda varjatult. Viidatud tehnoloogiad lisavad vaieldamatult täiendava mõõtme töösuhetele, tuues esile tööandja ja töötaja vastuolulised huvid, näiteks tööandja kontrolliõiguse ja töötajate õiguse privaatsusele ning andmekaitsele. Publikatsioonid IV ja V käsitlevad töötajate jälgimist COVID-19 leviku ajal. Pandeemia tõi paljudes töökohtades ohutuse tagamiseks kaasa töötajate jälgimise intensiivistumise ja uute tehnoloogiate

[394] Digitaalse töökoha kontseptsioon pärineb 1990ndatest. Viimastel aastatel on digitaalse töökoha mõiste pälvinud uut tähelepanu tulenevalt tehnoloogia kiirest arengust ning olles osana laiemast teemaderingist, mis käsitleb tulevikutööd. Digitaalset töökohta on näiteks selgitatud kui integreeritud tehnoloogiaplatvormi, mis sisaldab digitaalseid tööriistu ja teenuseid võimaldamaks töökohta paindlikult kontrollida ja tehtavat tööd tõhustada. Vt näiteks Williams, S. P., Schubert, P. Designs for the Digital Workplace. – Procedia Computer Science 2018/138; Köffer S. Designing the digital workplace of the future – what scholars recommend to practitioners. International Conference on Information Systems 2015; Marks, A., Briken, K., Chillas, S., Krzywdzinski, M. The New Digial Workplace: How New Technologies Revolutionise Work. Macmillan Publishers Limited 2017.

kasutuselevõtu, mis omakorda tekitas küsimusi tööandja kontrolliõiguse ja töötaja privaatsuse kohta.

Olgugi et Euroopa Liit omab ühte kõige hiljutisemat ja olulisemat privaatsuse ja andmekaitse raamistikku maailmas, ei ole töötajate jälgimine selgesõnaliselt ning üheselt reguleeritud, mistõttu on Euroopa Liidu riikides tekkinud hulgaliselt erinevaid siseriiklikke norme ja praktikaid. Käesolevas doktoritöös analüüsitud põhiprobleem seisnebki selles, et privaatsuse ja andmekaitse regulatsioon Euroopa Inimõiguste ja põhivabaduste kaitse konventsioonis (EIÕK) ja isikuandmete kaitse üldmääruses (IKÜM) ei sisalda selgeid ja konkreetseid reegleid digitaalsete jälgimistehnoloogiate kasutamise kohta.

Doktoritöö eesmärk on kindlaks teha, kas Euroopa Liidus on vaja kehtestada õigusakt (nt direktiiv või määrus), mis reguleerib töötaja privaatsust ja andmekaitset juhul, kui tööandja rakendab digitaalseid jälgimistehnoloogiaid, ning uurida millistel tingimustel peab olema lubatud nimetatud tehnoloogiaid töökeskkonnas kasutada. Doktoritöös on kasutatud meetoditena dogmaatilist ning võrdlevat ja sotsiaal-õiguslikku lähenemist.

Doktoritöös otsin vastust järgmistele uurimisküsimustele:

1) Millist kaitseb pakub EIÕK töötajale, kui tööandja kasutab digitaalseid jälgimistehnoloogiaid?
2) Millistel tingimustel kuulub IKÜM kohaldamisele, kui tööandja kasutab digitaalseid jälgimistehnoloogiaid? Millised tööandja jälgimispraktikad digitaalses töökeskkonnas on kooskõlas IKÜM-iga, kuid võivad rikkuda töötaja privaatsus- ja andmekaitseõigust? Millised tööandja poolt kasutatavad jälgimispraktikad ei kuulu IKÜM-i reguleerimisalasse, kuid mille korral tuleks ette näha reeglid töötaja privaatsuse kaitsmiseks?
3) Millised IKÜM-ist tulenevad õiguslikud alused, mida tööandja kasutab digitaalsel töökohal töötaja jälgimiseks, võivad rikkuda töötaja privaatsus- ja andmekaitseõigusi?
4) Millist kaitset pakuvad IKÜM-ist tulenevad andmekaitse põhimõtted töötajale digitaalses töökeskkonnas toimuva jälgimise eest?

2. Järeldused

2.1 Laiendades töötaja privaatsuse kaitset

EIÕK artikkel 8 näeb ette privaatsuse kaitse ja selle reguleerimisalasse kuulub ka Euroopa Inimõiguste Kohtu (EIK) praktika kohaselt töötajate privaatsuse riivete tuvastamine. Sellest hoolimata on EIK kohtupraktikast tuleneva kaitse ulatus küllaltki piiritletud, kuna tugineb teatud jälgimistehnoloogiatel (nt e-kirjade jälgimine ja kaamerate kasutamine), keskendub konkreetsetele kaasustele ja paneb paljuski töötaja privaatsusõiguse sõltuma formaalsetest kriteeriumitest (ennekõike töötaja eelnev teavitamine). Seetõttu ei ole seni EIK kohtupraktika raames väljakujunenud põhimõtted piisavad, et tagada töötajate privaatsus digitaalsete jälgimistehnoloogiate kasutamisel.

EIK kohtuasjas Bărbulescu vs Rumeenia vähendab kohus töötajate jälgimisega seonduvat ebaselgust ja kaalub töötaja ning tööandja huvisid erinevatele kriteeriumitele tuginedes, et välja selgitada, kas töötaja privaatsust on rikutud. Kohtu selgitustest hoolimata ei ole Bărbulescu kohtuasjas leitud kriteeriumid alati sobivad ja selged otsustamaks, kas tööandja ja töötaja huvid on tasakaalus ning töötaja õigused kaitstud, kui töökeskkonnas kasutatakse digitaalseid jälgimistehnoloogiaid. Antud kaasuses tõstab EIK ühe peamise kriteeriumina esile töötaja eelneva teavitamise, kaalumaks, kas tööandja poolt läbiviidav jälgimine on privaatsust rikkuv või mitte. Doktoritöös toon esile, et kuigi tööandja kontrollimeetmete korral on selged põhimõtted ja juhised vajalikud, ei tohiks töötaja jääda privaatsuse kaitseta seetõttu, et tööandja on teda võimalikust jälgimisest teavitatud. Eelnev teavitamine (nt töölepingu, teatise vormis) ei tohi õigustada invasiivsete jälgimistehnoloogitate kasutamist, mis võimaldavad varjatud ja pidevat jälgimist (nt mikrokiibid, kontaktide jälgimiseks mõeldud rakendused, kaasaskantavad tehnoloogiad nagu nutikellad/käevõrud/kiivrid). Eelneva teavitamise roll tulevastes EIK kohtuasjades jääb kahjuks ebaselgeks – kas tegemist on vaid ühe kriteeriumiga, mida kasutatakse poolte huvide kaalumisel või mõjutab see ikkagi märkimisväärselt kohtu otsust. Eelnev teavitus ei õigusta töötaja privaatsuse riivet digitaalse jälgimistehnoloogia kasutamisel, mistõttu peab vastav kriteerium tulevikus kaotama oma olulisuse tööandja ja töötaja huvide kaalumisel.

Lisaks võtab kohus Bărbulescu kaasuses kriteeriumina arvesse järelevalvemeetme invasiivsust ja seda, kas tööandjal on muid samavõrd tõhusaid viise töötajate jälgimiseks. Hoolimata kohtu selgitustest jääb ebaselgeks, kuidas peab tööandja tegema kindlaks digitaalsete jälgimistehnoloogiate (nt mikrokiibid) invasiivsuse. Samuti tekitab küsimusi, kuidas võrrelda uusi tehnoloogiaid võtmete, juurdepääsukaartide või muude sarnaste seadmetega. EIK üldised suunised ja digitaalsetest tehnoloogiatest tulenevad võimalused toovad siinkohal esile vajaduse reguleerida töötajate jälgimist täpsemalt ja põhjalikumalt Euroopa Liidu tasandil. Euroopa Liidu õigusakt suurendaks töötajate võimalusi keelduda invasiivsete jälgimistehnoloogiate kasutamisest ja annaks selgust, millistel tingimustel on töötajate jälgimine digitaalses töökeskkonnas lubatud.

Kusjuures murettekitav on kahju, mis võib ilmneda digitaalsete jälgimistehnoloogiate kasutamisel ja seda paljuski ka seetõttu, et tööandjad saavad toetuda andmete töötlemisel tehisintellekti pakutavatel võimalustel (nt andmete alusel töötajate kategoriseerimine, ülesannete jagamine ja isikuomaduste ning võimete tuvastamine). Üheks kriteeriumiks, mis aitaks tuvastada töötaja privaatsuse riivet pean seetõttu võimalikku kahju, mis võib tekkida digitaalsete jälgimisviiside kasutamisel. Näiteks tuleks kaaluda, kas jälgimine hõlmab informatsioonilist ebaõiglust, st ühes kontekstis esitatud teavet kasutatakse teises, kas digitaalseid jälgimistehnoloogiaid kasutatakse niivõrd ulatuslikult, et need võivad esile tuua tööga mitteseotud teavet (nt suhted kolleegidega, käitumismustrid) või kas jälgimine võib olla töötajate osas erinev ning tuua esile ebatäpset informatsiooni. Samuti peaks digitaalsete jälgimistehnoloogiate puhul panema põhilise rõhu küsimusele, kas selliste tehnoloogiate kasutamine on ettevõttes vajalik ning arutlema ennekõike selle üle, kas digitaalsest jälgimistehnoloogiast saadav teave on

töö tulemuslikkuse seisukohast oluline või mitte. Eeltoodud põhimõtted peaksid selguse huvides olema reguleeritud õigusakti tasandil.

2.2 Erireeglid töötaja andmete töötlemisele

Doktoritöös toon esile, et tööandjad saavad täna kasutada jälgimisviise, mis on küll kooskõlas IKÜM-iga, kuid kahjustavad töötajate privaatsus- ja andmekaitseõigust. IKÜM ei erista olukordi, kus andmete kogumine töötaja jälgimise käigus on piiratud, nendest olukordadest, kus üha võimsamad digitaalsed jälgimistehnoloogiad töötlevad ja analüüsivad teavet töötajate kohta, märgates ning luues andmetest mustreid ning korrelatsioone. Kuna tehisintellekti levik võimaldab töötajate algoritmilist juhtimist, laguneb kiiresti traditsiooniline piir töökoha ja üksikisiku eraelu vahel ning uued teabeallikad paljastavad tavapärastest jälgimismeetoditest palju enam informatsiooni. Lisaks on levimas üha kasvav trend, kus inimesed jälgivad enda tervist, heaolu ja muid näitajaid digitaalsete vahendite abil, laadides selleks näiteks telefoni erinevaid rakendusi. Taolisi enda jälgimise võimalusi saab ühendada digitaalsel töökohal kogutud andmetega, mõjutades seeläbi tööandja ja töötaja vahelist suhtlust. Digitaalsete jälgimistehnoloogiatega seonduvad andmete kogumise võimalused, näiteks töötajate asukohaandmete kogumine, töötajate käitumismustrite koostamine, töötajate eraelu puudutava teabe kogumine ja tehisintellekti abil loodud andmekogumite haldamine kuuluvad IKÜM reguleerimisalasse ja on seetõttu põhimõtteliselt lubatud, kui tööandjal on töötlemiseks õiguspärane alus. Eeltoodud praktikate valguses on oluline kaitsta töötajaid tarbetu ja liigse jälgimise eest. Seejuures on küsitav, kas taoline andmete kogumine töökeskkonnas peab olema lubatud.

Doktoritöös väidan, et invasiivsete jälgimispraktikate tõttu tuleb Euroopa Liidu tasandil täpsustada töötajate andmetöötluse ja jälgimise võimalusi. Õigusaktiga tuleb ette näha, et tööandja ei tohi töötajat jälgida ja tema andmeid töödelda, kui selleks puudub vajadus. Sellest reeglist võib erandi teha näiteks kuriteo, tõsise väärkäitumise või muude õigusaktis üheselt esitatud põhjuste korral (nt tööõnnetuste ärahoidmine). Üks võimalus on õigusaktis eristada jälgimistegevusi lähtuvalt nende invasiivsusest ning kehtestada rangemad reeglid jälgimismeetmetele, mis sekkuvad tugevalt töötajate õigustesse (nt mikrokiibid, biomeetrilisi andmeid töötlevad seadmed, kontaktide jälgimiseks kasutatavad rakendused).

Digitaalsete jälgimistehnoloogiate kasutamisel on sageli keeruline tuvastada, millal tööandjad töötlevad töötaja isikuandmeid ja millal mitte. Tänapäeval on võimalik eristada esmaseid ja teiseseid digitaalseid identifikaatoreid. Esmased identifikaatorid on kergesti mõistetavad, kuna need on inimesega otseselt seotud teave (nt nimi, aadress, mobiiltelefoni number, parool). Teisesed identifikaatorid on palju varjatumad, kuna need on kaudsed (nt veebibrauseri küpsised, IP-aadressid, RFID[395]-märgendite numbrid). Teisesed identifikaatorid ei ole töötajale

[395] RFID (Radio Frequency Identification) on raadiolainetel töötav identifitseerimistehnoloogia, mis võimaldab esemete või objektide automaatset tuvastust (nt kasutusel mikrokiipides).

tingimata teada, kuid neid saab seostada töötaja ja töökohaga või konkreetse objektiga, mis on omakorda töötajaga seotud. Kontaktide jälgimise rakendused, mikrokiibid ja muud tehnoloogilised lahendused, mis taolisi identifikaatoreid kasutavad, võivad töödelda ka mitmesuguseid muid andmeid (nt terviseandmed, asukohaandmed, samuti andmed, mis ilmestavad kontakte ja suhtlust töötajate vahel) ning teha seda varjatult. Kuivõrd tehnoloogiad, mis taolisi identifikaatoreid kasutavad, võivad muuta jälgimise läbipaistmatuks ja salajaseks, tuleks kaaluda Euroopa Liidu õigusakti loomist, mis võimaldab töötajatel kindlaks teha, millal ja kuidas jälgimine toimub. Jälgimise läbiviimisel peab tööandjale panema senisest rangemad kohustused. Näiteks peab tööandja andma töötajatele üksikasjalikud juhised jälgimise läbiviimise kohta ja töökohal, kus jälgimine toimub, peavad olema vastavad märgised. Samuti võiks teatud jälgimisviisid keelata, nt keelata salajase jälgimise või liikumisandmete kogumise töökohal. Lisaks peab töötajal olema võimalus valida nii „uute" kui ka „traditsiooniliste" jälgimismeetodite vahel. Näiteks peab töötajal olema võimalik töökohale sisse- ja väljapääsu saamiseks valida erinevate rakenduste vahel, st kasutada mikrokiibi asemel uksekaarti. Samuti ei tohiks tööandja kombineerida erinevaid digitaalsetest jälgimistehnoloogiatest saadud andmeid ühte mahukasse andmebaasi, mis sisaldab hulgaliselt teavet töötajate kohta ning võimaldab töötajaid tuvastada isegi juhul, kui andmed on algselt anonüümiseeritud.

Tööandjad kasutavad ka jälgimistegevusi, mis ei kuulu IKÜM-i reguleerimisalasse, kuid mida tuleks ikkagi reguleerida, et kaitsta töötajate privaatsust. Täna ei ole töötaja kaitstud olukorras, kus tööandja ei kasuta veebibrauseri küpsiste või RFID-märgiste abil saadud andmeid töötaja tuvastamiseks, vaid loob profiili arvuti, töövahendi, ruumi või kiibi omaniku kohta, et tema suhtes tegevusi rakendada (nt töötajate puhkeruumi kasutuse jälgimise andmete põhjal kõigile töötjatele juhiste koostamine). Kuna töötajad jäävad sellises olukorras õigusteta, mida pakub IKÜM, peaks Euroopa Liidu õigus reguleerima tööandja jälgimismeetodeid, kus töötaja kohta koostatakse profiil ilma tema isikut tuvastamata. Näiteks tuleb õigusaktis üheselt sätestada, et tööandjatel on üldjuhul keelatud töötajate käitumismustrite jälgimine ilma konkreetse eesmärgita (nt tervis ja ohutus) ja seda ka juhul, kui töötaja ei ole tuvastatav.

Digitaalsete jälgimistehnoloogiate korral ei pruugi isikuandmete kogumine olla alati tööandja korraldada. Näiteks võib andmete töötlemisega tegeleda ka kolmas isik, mistõttu ei pruugi tööandja olla andmete vastutavaks töötlejaks, kellel lasuvad IKÜM-ist tulenevad kohustused. Tööandja võib kontrollida andmeid ainult osaliselt või üldse mitte ja töötaja andmeid käitleb näiteks lepingupartner teenusedisainerina või tarkvara arendajana. Vastutava töötleja roll võib tekitada segadust ka olukorras, kus tööandja kasutab või suunab töötajaid kasutama enese jälgimisvahendeid (nt tervise jälgimiseks mõeldud rakendus) või kolmanda osapoole omandis olevaid tehnoloogiaid (nt valitsuste või ettevõtete poolt COVID-19 ajal laialdaseks kasutamiseks välja töötatud kontaktide jälgimise rakendused). Tööandja vastutuse ulatus selliste rakenduste suhtes sõltub tööandja rollist. Juhul kui tööandja loodab, et töötajad edastavad talle vabatahtlikult näiteks valitsuse käivitatud rakendustest saadud asjakohast teavet, ei ole ta

vastutav töötleja IKÜM tähenduses, kuna ta ei otsusta töötlemise eesmärke ja vahendeid. Tööandja roll muutub aga paratamatult ebaselgemaks, kui ta nõuab, et töötajad laeksid alla ja kasutaksid valitsuse loodud rakendusi töökohal ohutuse tagamiseks. Sellisel juhul on tööandjatel aktiivsem roll, kuid on küsitav, kas nad määratlevad töötlemise eesmärgi ja vahendid. Nendel juhtudel ei pruugi tööandja saada rakenduselt mingeid andmeid (nt tööandja jälgib ainult rakenduse olemasolu töötaja või ettevõtte telefonis) ja seetõttu ei peeta teda IKÜM kohaselt andmete vastutavaks töötlejaks. Doktoritöös toon esile, et taolist jälgimistegevust tuleks reguleerida, et kaitsta töötajate privaatsust. Nõue, et töötaja kontrolliks iseenda tervist, töökiirust ja tööle kuluvat aega rakenduste abil, rikub tõsiselt töötaja privaatsust. Tööandjal ei tohi olla õigust nõuda töötajatelt ilma olulise põhjuseta (nt õnnetuste vältimine ohtlikus töökeskkonnas või nakkushaiguse leviku tõkestamine) enesekontrolli teostamist digitaalsete jälgimistehnoloogiate (nt telefoni rakendused, nutikellad ja -käevõrud) kaudu. Euroopa Liidu õigusakt peab täpsustama, millistes olukordades ja millistel tingimustel võib tööandja nõuda töötajalt digitaalse jälgimistehnoloogia, näiteks rakenduste või nutikellade kasutamist. Ebaselguste vältimiseks tuleb Euroopa Liidu õigusaktis selgelt sätestada, et andmete kogumine töötaja omandis olevatest allikatest (nt enesejälgimise rakendused) on keelatud.

2.3 Töötaja jälgimiseks kohased õiguslikud alused

Kuigi tööandjad saavad kasutada mitut IKÜM-is sätestatud õiguslikku alust (nt andmete töötlemine töölepingu täitmiseks, seadusjärgse kohustuse täitmiseks, töötaja nõusolekul või tööandja õigustatud huvi korral), võivad need õiguslikud alused riivata töötaja privaatsus- ja andmekaitseõigust.

Tööandja võib IKÜM-i kohaselt töödelda töötaja andmeid töölepingu täitmiseks. Doktoritöös toon esile, et tööandja ei tohi seda õiguslikku alust töötajate jälgimisel rakendada. Ainuüksi asjaolu, et tööleping on sõlmitud, ei anna alust töötajate jälgimiseks, eriti juhul kui tööandja kasutab digitaalset jälgimistehnoloogiat. Töötaja jälgimine ei ole töölepingu täitmiseks hädavajalik ja seetõttu ei saa töölepingust tulenevad kohustused õigustada andmete kogumist. Seda ka juhul kui andmetöötlus toimub lihtsate ja igapäevaste jälgimistoimingute raames, nt arvutite sisselülitamisel, töökohta sisenemisel. Seetõttu ei tohi jälgimine nt mikrokiipide, nutikäevõrude ja töötaja telefonis olevate rakenduste kaudu põhineda ainuüksi töölepingulise kohustuse olemasolul. Taolisel jälgimisel põhinevad otsused (nt töösuhte ülesütlemine, töötaja hoiatamine) peavad olema ebaseaduslikud. Doktoritöös toon esile, et Euroopa Liidu õigus peab tulevikus selgelt sätestama, et töötaja jälgimine ei ole lubatud töölepingu täitmiseks.

Tööandja võib IKÜM-i kohaselt töödelda töötaja andmeid seadusjärgse kohustuse täitmiseks. Seejuures ei ole üheselt arusaadav, millal võib tööandja sellele õiguslikule alusele tugineda, kui soovib koguda töötaja andmeid digitaalsete tehnoloogiate vahendusel. Tööandja võib seda õiguslikku alust kasutada juhul, kui töötlemine on seadusjärgse kohustuse täitmiseks vajalik ja vältimatu.

Samas ei ole selge, kuidas peab seadusjärgne kohustus olema kehtestatud, et õigustada jälgimist. Näiteks, on küsitav, kas üldine töötervishoiu ja -ohutuse tagamine õigustab töötaja jälgimist ja andmete kogumist või tuleb konkreetsete andmete kogumiseks kehtestada täpsemad reeglid. Digitaalsete jälgimistehnoloogiate kasutamise vajalikkust ja asendamatust on sageli raske põhjendada üldiste seadusjärgsete kohustuste alusel (nt tööle kandideerijate kvalifikatsiooni ja väärtuste kontrollimine sotsiaalmeedias, rääkimata jälgimismeetmetest nagu mikrokiibid või kontaktide jälgimise rakendused). Seega, kuigi seadusjärgsed kohustused õigustavad IKÜM-i alusel töötajate andmete töötlemist, tuleb seda õiguslikku alust kohaldada ainult juhul, kui siseriiklik õigus on konkreetne ja reguleerib selgelt töötajate jälgimist. Ainuüksi asjaolu, et õigusaktide kohaselt peavad tööandjad täitma arvukalt kohustusi, ei õigusta digitaalsete jälgimistehnoloogiate kasutamist.

Töötajate andmete töötlemine võib toimuda ka nõusoleku alusel. Samas võib see õiguslik alus rikkuda töötajate privaatsust, kui seda kasutatakse digitaalsel töökohal jälgimise õigustamiseks. Nõusolek ei kaitse töötajaid jälgimise korral peamiselt teabe ebasümmeetria tõttu töötaja ja tööandja vahelistes suhetes ning töötaja võimetuse tõttu täiel määral hinnata, millega ta nõustub ning mõista nõusoleku andmise tagajärgi. Osapoolte ebavõrdsus töösuhetes muudab nõusoleku andmise sisutühjaks tegevuseks, kuivõrd töötaja võimalused sisulisteks läbirääkimisteks on piiratud. Doktoritöös toon esile, et tööga seonduv (edutamine, tasustamine, ülesütlemine jne) ei tohi sõltuda sellest, kas töötaja on nõus telefoni rakendust alla laadima või mikrokiipi siirdama.

Töösuhetes on raske eristada, millal toimub andmete töötlemine tööandja soovide tõttu ja millal töötaja vabal tahtel. Tehnoloogia võib veelgi piirata töötaja valikuvõimalusi, raskendada nõusoleku tagasivõtmist või nõusolekust keeldumist. Töötaja nõusoleku kvaliteeti võivad mõjutada erinevad tegurid, näiteks tehnoloogia kasutuselevõtt kolleegide seas ja sellega kaasnev sotsiaalne surve tehnoloogia aktsepteerimiseks.

Töötaja peab andma informeeritud nõusoleku, kuid tööandja katsed töötajat mõtestatult teavitada võivad olla ebapiisavad, kuivõrd ülimalt tehnilised, pikad ja keerulised töökorralduse reeglid ja lepingupunktid ei anna töötajale piisavat ja sisulist infot digitaalse töökoha andmetöötluse tegelikust olemusest. IKÜM-is töötaja nõusolekuga seotud keerukate ja ebamääraste reeglite tõttu võetakse digitaalseid jälgimistehnoloogiaid (näiteks mikrokiipe) töökohtadel kasutusele ilma selge suuniseta, mis võib omakorda halvendada töötajate privaatsuse kaitset.

Doktoritöös toon välja, et töötajad ja tööandjad vajavad selget ja konkreetset lähenemisviisi digitaalsete tehnoloogiate kasutamisel. Väidan, et tööandja ja töötaja vahelise alluvusvahekorra ja digitaalsetest jälgimistehnoloogiatest tulenevate võimaluste tõttu tuleb Euroopa Liidu õigusaktiga tugevdada töötaja õigusi nimetatud tehnoloogiatest keelduda. Samuti tuleb jälgimistehnoloogiate kasutusele töökeskkonnas kehtestada konkreetsed reeglid. Euroopa Liidu õigus peab keelama eraldiseisvalt nõusoleku kasutamise õigusliku alusena, mis võimaldab töötajaid jälgida. Samas võib endiselt kaaluda nõusoleku kasutamist koos muu õigusliku alusega, näiteks koos tööandja õigustatud huviga. Teisalt ei tohi eirata

ka asjakohase teabe vajalikkust, kuivõrd selle kaudu saavad töötajad oma isikuandmete töötlemist kontrollida. Seetõttu peab töötlemise õigusliku alusega kaasnema tööandja kohustus töötajaid juhendada ning töötajate ja nende esindajatega konsulteerida, kui töökohal võetakse kasutusele digitaalsed jälgimistehnoloogiad. Samuti peab Euroopa Liidu õigus nõudma, et tööandja rakendab lahendusi, mis toetavad erinevate tehnoloogiate kasutamist töökeskkonnas, jättes sellega töötajale valikuvõimalused.

Tööandjal on soovitav töötajate jälgimisel tugineda õigusliku alusena õigustatud huvile. Samas kaasnevad ka selle õigusliku alusega teatavad probleemkohad. Õigustatud huvi on IKÜM-is sõnastatud laialt ja mitmetähenduslikult. Tööandja peab selle õigusliku aluse rakendamiseks viima läbi huvide kaalumise testi, mis võimaldab hulgaliselt tõlgendamisruumi. Huvide kaalumise test koosneb mitmest komponendist ja kaalutlusest, näiteks võimalikud tagajärjed töötajale, võimalikud privaatsusriskid ja nende realiseerumise tõenäosus, jälgimise intensiivsus, töötaja põhjendatud ootus privaatsusele. Kahjuks ei ole need testi osised ja kaalutlused IKÜM-is sätestatud vaid neid on selgitatud Artikli 29 töörühma[396] üldistes juhistes ning analüüsitud liikmesriikide kohtupraktikas. Ei ole üheselt selge, kas nimetatud elementide loetelu on ammendav või avatud ja kuidas neid elemente tuleks digitaalsete jälgimistehnoloogiate kasutamisel tõlgendada. Huvide kaalumise testi keerukus seisneb selles, et õiguste kaalumine ei ole kunagi üheselt tõlgendatav ja sõltub paljuski juhtumi eripärast. Kuna huve kaalub tööandja, on küsitav, kas testi läbiviimisel saavutatakse õiglane tasakaal töösuhte osapoolte vahel, kuna võib eeldada, et test on läbi viidud eelkõige tööandja huve arvestades.

Huvide kaalumise test vajab ranget ja sisulist analüüsi, mida võib tööandjal olla keeruline läbi viia. Parema mõistmise eesmärgil tuleb huvide kaalumise testi elemendid õigusaktis selgelt määratleda. Näiteks peab tööandja digitaalsete jälgimistehnoloogiate kasutamisel arvestama jälgimise vajalikkuse, konkreetsete jälgimismeetodite, tehnoloogia eripärade ja nende kasutamisega kaasneva kahjuga (erinevad andmed töötajate lõikes, andmete ebatäpsus, teabe käsitlemine vales kontekstis). Euroopa Liidu õiguses tuleb reguleerida, millised üksikisiku õigused kaaluvad üle tööandja huvid, muutes andmete töötlemise ebaseaduslikuks või teise võimalusena võib õigusaktiga reguleerida, millised tööandja huvid või eesmärgid õigustavad töötajate jälgimist. Täiendavalt tuleb analüüsida, kuidas õigluse roll, sotsiaalsed õigused tööl, heausksus, õigus töötervishoiule ja -ohutusele (nt töötaja õigus töötada sobivas töökeskkonnas, mis arvestab tema vaimse tervisega), sõnavabadus (nt töötaja õigus avaldada arvamust internetis ja sotsiaalmeedias) ning vajadus austada töötaja väärikust mõjutavad huvide kaalumise testi. Lisaks peavad sektori eripära ja tehtav töö mängima olulist rolli otsustamaks jälgimismeetme invasiivsuse ja seetõttu nende lubatavuse üle. Digitaalsed jälgimistehnoloogiad leiavad eelduslikult rohkem aktsepteerimist ohtlikel töökohtadel, kus on suurem õnnetusoht. Samuti tuleb Euroopa Liidu õiguses sätestada, millised

[396] Artikkel 29 töörühm oli Euroopa sõltumatu töörühm, mis kuni 25. maini 2018 (kuni isikuandmete kaitse üldmääruse jõustumiseni) käsitles eraelu puutumatuse ja isikuandmete kaitse küsimusi.

on tööandja kohustused enne jälgimist. Näiteks peab tööandja teavitama töötajaid digitaalsetest jälgimismeetoditest ja kuulama ära nende arvamused seoses jälgimisega. Töötajate esindajad peavad olema kaasatud privaatsust riivava jälgimistehnoloogia rakendamisse töökohal.

2.4 Täiendatud andmetöötluse põhimõtted

Andmetöötluse põhimõtted, täpsemalt eesmärgikohasus, õiglus ja läbipaistvus on sõnastatud üldiselt, võimaldades tööandjal rakendada digitaalsel töökohal jälgimist, mis on küll kooskõlas IKÜM-iga, kuid rikub töötajate andmekaitseõigusi ja privaatsust.

Eesmärgikohasuse põhimõte jääb liiga üldiseks, et kaitsta töötaja õigusi jälgimise korral. Tehnoloogiliste lahenduste areng koos COVID-19 levikuga on suurendanud töötajate jälgimist digitaalsetes töökohtades ja tõstnud töökeskkonnas kogutud andmete hulka. Taolised trendid võivad omakorda tuua esile tööandja soovi kasutada jälgimistehnoloogiaid muul otstarbel kui algselt kavandatud ja viia isikuandmete ebaseadusliku edasise töötlemiseni algsest erinevatel eesmärkidel. COVID-19 levikuga võitlemiseks kasutatud jälgimistegevused ja isikuandmete kogumine tuleb lõpetada, kui see ei täida enam algset eesmärki ega kaitse töötajate tervist. Seejuures peab arvestama, et pandeemia ning viiruse leviku lõpp on ebamäärased terminid, mistõttu on andmete töötlemise aega ja eesmärki kohati keeruline määrata. Lisaks võivad tööandjad varjata teiseseid andmete töötlemise eesmärke privaatsuspoliitika pikkades ja keerukates tekstides, mis pole üheselt mõistetavad.

Paljuski puuduvad konkreetsed teadmised, mis juhtub töökohal kasutatavate tehnoloogiatega pärast viiruse taandumist, kuna eesmärgikohasuse põhimõte läheb vastuollu andmemajanduses kasutusel oleva ideega, milleks on andmete taaskasutamine. Digitaalses töökeskkonnas valitseb suur tõenäosus andmete uuesti kasutamiseks, mistõttu võib väita, et eesmärgikohasuse põhimõte on liiga laialt sõnastatud, kaitsmaks töötajaid invasiivsete jälgimistehnoloogiate kasutamise eest. Doktoritöös toon välja, et Euroopa Liidu õiguses tuleb reguleerida eesmärke, mis võimaldavad töötajaid jälgida. Näiteks on mõned liikmesriigid lubanud kasutada tööl digitaalseid jälgimistehnoloogiaid vaid juhul, kui nende tehnoloogiate kasutamine on lubatud õigusaktides või kollektiivlepingutes sätestatud eesmärkidel. Sarnaseid põhimõtteid võib kasutada ka Euroopa Liidu õiguses.

IKÜM-ist tulenev õigluse põhimõte peab kujundama andmete õiglast töötlemist, kuid keskendub pigem menetluslikule õiglusele kui sisulisele õiglusele. Õiglase andmete töötlemisega on tegemist juhul, kui töötlemine on läbipaistev ja sellel on õiguslik alus. Samas ei peaks andmete töötlemise läbipaistvus ja õiguslik alus olema ainsad tegurid, mis määratlevad, kas andmete töötlemine on käsitletav õiglasena. Digitaalsed jälgimistehnoloogiad toovad esile vajaduse hinnata õiglust sisulisemalt. Andmete töötlemist tuleb pidada õiglaseks vaid juhul, kui andmeid hinnatakse asjakohases kontekstis, mis tähendab, et tööandja võib töötajat jälgida viisil, mida töötaja mõistlikult ootab ega tohi andmete töötlemisega tekitada töötajale põhjendamatult negatiivset mõju. Näiteks ei tohi tööandja tutvuda töötaja

sotsiaalmeedia profiilidega, kui selleks ei ole olulist põhjust (töötaja käitumine sotsiaalmeedias rikub teise isiku õigusi või ta avaldab seal ettevõtte ärisaladusi). Õiglast andmete töötlemist võib mõjutada ka see, kui digitaalsed jälgimistehnoloogiad võimaldavad teatud töötajate andmete põhjal teha järeldusi erinevate töötajate gruppide kohta, omistades ühele töötajale hoiakuid, mis pole temaga seotud. Taoliste järelduste tegemine võib kaasa tuua konkreetse töötaja eripärasid mitte arvestavaid lahendusi, mis on lõpptulemusena ebaõiglased.

Sarnaselt eelmiste põhimõtetega on ka andmete läbipaistvuse põhimõte laialt sõnastatud, võimaldades invasiivseid jälgimispraktikaid. IKÜM-ist tulenevalt ei saa töötaja õigel ajal piisavat teavet digitaalsete jälgimistehnoloogiate kohta, kuna tööandjalt nõutakse töötaja informeerimist jälgimise alguses, kui töötajal pole veel selge, kuidas jälgimine teda reaalselt mõjutab. Samuti ei konsulteeri tööandja töötajaga digitaalsete jälgimistehnoloogiate kasutusele võtmisel ja seetõttu ei pruugi töötaja täielikult mõista, kuidas jälgimist teostatakse.

Digitaalsed jälgimistehnoloogiad võivad tuua kaasa varjatud jälgimise sulandudes sujuvalt tööga seotud tegevusteks (nt võimaldades andmete kogumist kui töötaja käivitab tööriistu ning siseneb töö- või puhkeruumidesse). Seejuures ei pruugi töötaja olla teadlik toimuvast jälgimisest või isegi võimalikust profileerimisest. Teisalt, kui töötaja ongi teadlik jälgimisest, võib ta tunda ärevust ja ebamugavust ning tsenseerida oma käitumist asjatult ja ebaõiglaselt. Varjatud jälgimise välistamiseks ja selleks, et töötajad ei tunneks ennast töökeskkonnas halvasti, tuleb Euroopa Liidu õigusaktiga panna tööandjale kohustus töötajate regulaarseks teavitamiseks. Kui jälgimine on pidev, peab tööandja enne sellise meetme rakendamist küsima töötajate esindajate nõusolekut ja korraldama enne jälgimismeetme kasutuselevõttu konsultatsioone töötajate ja nende esindajatega. Andmete töötlemise ja jälgimise tavad ei tohi ettevõttes sisalduda üksnes formaalsetes dokumentides. Tööandja peab viima läbi koolitusi jälgimisest teavitamiseks ja visualiseerima töökeskkonnas, kus jälgimine toimub. Samuti tuleb töötajale anda lisateavet, näiteks selgitada jälgimise spetsiifikat ja seda, kas tööandja poolt antud tehnoloogiat võib kasutada isiklikeks tegevustes ning millises ulatuses (nt arvuti või nutikella kasutamine eraelulisteks tegevusteks), millised kaitsemeetmed on ettevõttes kehtestatud ja mis on jälgimise tagajärjed. Juhul kui tööandja kasutab digitaalseid jälgimistehnoloogiaid, peab töötaja olema teadlik sellest, millal ja kuidas tema kohta andmeid koguti. Näiteks mikrokiipide jälgimisel peab töötaja olema teadlik, kus asuvad töötajat seiravad andurid ning mis on nende jälgimisraadius (seda saab ilmestada vastav märgistus töökeskkonnas). Kui tööandja lähtub oma otsustes (nt tulemustasud, töösuhte ülesütlemine) jälgimistulemustest, peavad töötajal olema üksikasjalikud teadmised, kuidas võib jälgimine teda mõjutada ja milliseid andmeid otsuse tegemiseks töödeldakse.

PUBLICATIONS

CURRICULUM VITAE

Name: Seili Suder
Date of birth: 4 December 1982
E-mail: seili.suder@sm.ee

Career

2014–…	Ministry of Social Affairs, Head of work environment
2010–2014	Ministry of Social Affairs, Head of employment relations
2007–2010	Ministry of Social Affairs, Working life development apartment, Specialist
2005–2007	Labour Inspectorate, labour inspector

Education

2012–…	Doctoral studies, School of Law, University of Tartu
2005–2007	MA in Law, Faculty of Law, University of Tartu
2002–2005	BA in Social Sciences (law), Faculty of Law, University of Tartu

Publications

Suder, S. Pre-Employment Background Checks on Social Networking Sites – May Your Boss Be Watching? – Masaryk University Journal of Law and Technology 2014/8 (1).

Suder, S., Siibak, A. Employers as Nightmare Readers: An Analysis of Ethical and Legal Concerns Regarding Employer-Employee Practices on SNS – Baltic Journal of Law & Politics 2017/10 (2).

Suder, S., Erikson, M. Microchipping Employees – Unlawful Monitoring Practice or a New Trend in the Workplace? In Ebers, M.; Cantero Gamito, M. (Eds.). Algorithmic Governance and Governance of Algorithms. Legal and Ethical Challenges. Springer International Publishing. Data Science, Machine Intelligence, and Law 1 2020.

Suder, S. Processing employees' personal data during the Covid-19 pandemic. – European Labour Law Journal 2021. DOI: 10.1177/2031952520978994.

Suder, S., Siibak, A. Proportionate response to a COVID-19 threat? Use of apps and other technologies for monitoring employees under the EU data protection framework. – Special issue 'COVID-19 and the world of work'. – International Labour Review 2021.

Suder, S. Töötaja isikuandmete töötlemine COVID-19 leviku tõkestamiseks [Processing of employee's personal data to prevent the spread of COVID-19]. – Juridica 2020/7.

ELULOOKIRJELDUS

Nimi: Seili Suder
Sünniaeg: 4. detsember 1982
E-post: seili.suder@sm.ee

Töökogemus

2014–… Sotsiaalministeerium, töökeskkonna üksuse juht
2010–2014 Sotsiaalministeerium, töösuhete poliitika juht
2007–2010 Sotsiaalministeerium, tööelu arengu osakonna peaspetsialist
2005–2007 Tööinspektsioon, tööinspektor

Hariduskäik

2012–… doktoriõpe, õigusteaduskond, Tartu Ülikool
2005–2007 õigusteaduse magister, õigusteaduskond, Tartu Ülikool
2002–2005 sotsiaalteaduste bakalaureus (õigus), õigusteaduskond, Tartu Ülikool

Publikatsioonid

Suder, S. Pre-Employment Background Checks on Social Networking Sites – May Your Boss Be Watching? – Masaryk University Journal of Law and Technology 2014/8 (1).

Suder, S., Siibak, A. Employers as Nightmare Readers: An Analysis of Ethical and Legal Concerns Regarding Employer-Employee Practices on SNS – Baltic Journal of Law & Politics 2017/10 (2).

Suder, S., Erikson, M. Microchipping Employees – Unlawful Monitoring Practice or a New Trend in the Workplace? In Ebers, M.; Cantero Gamito, M. (Eds.). Algorithmic Governance and Governance of Algorithms. Legal and Ethical Challenges. Springer International Publishing. Data Science, Machine Intelligence, and Law 1 2020.

Suder, S. Processing employees' personal data during the Covid-19 pandemic. – European Labour Law Journal 2021. DOI: 10.1177/2031952520978994.

Suder, S., Siibak, A. Proportionate response to a COVID-19 threat? Use of apps and other technologies for monitoring employees under the EU data protection framework. – Special issue 'COVID-19 and the world of work'. – International Labour Review 2021.

Suder, S. Töötaja isikuandmete töötlemine COVID-19 leviku tõkestamiseks [Processing of employee's personal data to prevent the spread of COVID-19]. – Juridica 2020/7.

DISSERTATIONES IURIDICAE UNIVERSITATIS TARTUENSIS

1. **Херберт Линдмяэ**. Управление проведением судебных экспертиз и его эффективность в уголовном судопроизводстве. Тарту, 1991.
2. **Peep Pruks**. Strafprozesse: Wissenschaftliche “Lügendetektion”. (Instrumentaldiagnostik der emotionalen Spannung und ihre Anwendungsmöglichkeiten in Strafprozess). Tartu, 1991.
3 **Marju Luts**. Juhuslik ja isamaaline: F. G. v. Bunge provintsiaalõigusteadus. Tartu, 2000.
4. **Gaabriel Tavits**. Tööõiguse rakendusala määratlemine töötaja, tööandja ja töölepingu mõistete abil. Tartu, 2001.
5. **Merle Muda**. Töötajate õiguste kaitse tööandja tegevuse ümberkorraldamisel. Tartu, 2001.
6. **Margus Kingisepp**. Kahjuhüvitis postmodernses deliktiõiguses. Tartu, 2002.
7. **Vallo Olle**. Kohaliku omavalitsuse teostamine vahetu demokraatia vormis: kohalik rahvaalgatus ja rahvahääletus. Tartu, 2002.
8. **Irene Kull**. Hea usu põhimõte kaasaegses lepinguõiguses. Tartu, 2002.
9. **Jüri Saar**. Õigusvastane käitumine alaealisena ja kriminaalsed karjäärid (Eesti 1985–1999 longituuduurimuse andmetel). Tartu, 2003.
10. **Julia Laffranque**. Kohtuniku eriarvamus. Selle võimalikkus ja vajalikkus Eesti Vabariigi Riigikohtus ja Euroopa Kohtus. Tartu, 2003.
11. **Hannes Veinla**. Ettevaatusprintsiip keskkonnaõiguses. Tartu, 2004.
12. **Kalev Saare**. Eraõigusliku juriidilise isiku õigussubjektsuse piiritlemine. Tartu, 2004.
13. **Meris Sillaots**. Kokkuleppemenetlus kriminaalmenetluses. Tartu, 2004.
14. **Mario Rosentau**. Õiguse olemus: sotsiaalse käitumise funktsionaalne programm. Tartu, 2004.
15. **Ants Nõmper**. Open consent – a new form of informed consent for population genetic databases. Tartu, 2005.
16. **Janno Lahe**. Süü deliktiõiguses. Tartu, 2005.
17. **Priit Pikamäe**. Tahtluse struktuur. Tahtlus kui koosseisupäraste asjaolude teadmine. Tartu, 2006.
18. **Ivo Pilving**. Haldusakti siduvus. Uurimus kehtiva haldusakti õiguslikust tähendusest rõhuasetusega avalik-õiguslikel lubadel. Tartu, 2006.
19. **Karin Sein**. Ettenähtavus ja rikutud kohustuse eesmärk kui lepingulise kahjuhüvitise piiramise alused. Tartu, 2007.
20. **Mart Susi**. Õigus tõhusale menetlusele enda kaitseks – Euroopa Inimõiguste ja Põhivabaduste Kaitse Konventsiooni artikkel 13 Euroopa Inimõiguste Kohtu dünaamilises käsitluses. Tartu, 2008.
21. **Carri Ginter**. Application of principles of European Law in the supreme court of Estonia. Tartu, 2008.
22. **Villu Kõve**. Varaliste tehingute süsteem Eestis. Tartu, 2009.

23. **Katri Paas**. Implications of Smallness of an Economy on Merger Control. Tartu, 2009.
24. **Anneli Alekand**. Proportsionaalsuse printsiip põhiõiguste riive mõõdupuuna täitemenetluses. Tartu, 2009.
25. **Aleksei Kelli**. Developments of the Estonian Intellectual Property System to Meet the Challenges of the Knowledge-based Economy. Tartu, 2009.
26. **Merike Ristikivi**. Latin terms in the Estonian legal language: form, meaning and influences. Tartu, 2009.
27. **Mari Ann Simovart**. Lepinguvabaduse piirid riigihankes: Euroopa Liidu hankeõiguse mõju Eesti eraõigusele. Tartu, 2010.
28. **Priidu Pärna**. Korteriomanike ühisus: piiritlemine, õigusvõime, vastutus. Tartu, 2010.
29. **René Värk**. Riikide enesekaitse ja kollektiivse julgeolekusüsteemi võimalikkusest mitteriiklike terroristlike rühmituste kontekstis. Tartu, 2011.
30. **Paavo Randma**. Organisatsiooniline teovalitsemine – *täideviija täideviija taga* kontseptsioon teoorias ja selle rakendamine praktikas. Tartu, 2011.
31. **Urmas Volens**. Usaldusvastutus kui iseseisev vastutussüsteem ja selle avaldumisvormid. Tartu, 2011.
32. **Margit Vutt**. Aktsionäri derivatiivnõue kui õiguskaitsevahend ja ühingujuhtimise abinõu. Tartu, 2011.
33. **Hesi Siimets-Gross**. Das „Liv-, Est- und Curlaendische Privatrecht" (1864/65) und das römische Recht im Baltikum. Tartu, 2011.
34. **Andres Vutt**. Legal capital rules as a measure for creditor and shareholder protection. Tartu, 2011.
35. **Eneken Tikk**. Comprehensive legal approach to cyber security. Tartu, 2011.
36. **Silvia Kaugia**. Õigusteadvuse olemus ja arengudeterminandid. Tartu, 2011.
37. **Kadri Siibak**. Pangandussüsteemi usaldusväärsuse tagamine ja teabekohustuste määratlemine finantsteenuste lepingutes. Tartu, 2011.
38. **Signe Viimsalu**. The meaning and functioning of secondary insolvency proceedings. Tartu, 2011.
39. **Ingrid Ulst**. Balancing the rights of consumers and service providers in electronic retail lending in Estonia. Tartu, 2011.
40. **Priit Manavald**. Maksejõuetusõigusliku regulatsiooni valikuvõimaluste majanduslik põhjendamine. Tartu, 2011, 193 lk.
41. **Anneli Soo**. Remedies against ineffectiveness of defense counsel. Judicial supervision over the performance of defense counsel in Estonian criminal proceedings. Tartu, 2011, 282 p.
42. **Arnold Sinisalu**. Mõjutustegevuse piirid rahvusvahelises õiguses. Tartu, 2012, 277 lk.
43. **Kaspar Lind**. Käibemaksupettused ja nende tõkestamine. Tartu, 2012, 155 lk.
44. **Berit Aaviksoo**. Riigi otsustusruumi ahenemine: kodakondsus nüüdisaegses Euroopas. Tartu, 2013, 368 lk.
45. **Kai Kullerkupp**. Vallasomandi üleandmine. Õigusdogmaatiline raamistik ja kujundusvõimalused. Tartu, 2013, 398 lk.

46. **Iko Nõmm**. Käibekohustuse rikkumisel põhinev deliktiõiguslik vastutus. Tartu, 2013, 212 lk.
47. **Piia Kalamees**. Hinna alandamine õiguskaitsevahendite süsteemis. Tartu, 2013, 232 lk.
48. **Irina Nossova**. Russia's international legal claims in its adjacent seas: the realm of sea as extension of Sovereignty. Tartu, 2013, 205 p.
49. **Age Värv**. Kulutuste kondiktsioon: teise isiku esemele tehtud kulutuste hüvitamine alusetu rikastumise õiguses. Tartu, 2013, 273 lk.
50. **Elise Vasamäe**. Autoriõiguste ja autoriõigusega kaasnevate õiguste jätkusuutlik kollektiivne teostamine. Tartu, 2014, 308 lk.
51. **Marko Kairjak**. Keerukuse redutseerimine Eesti õiguses karistusseadustiku § 217^2 objektiivse koosseisu relatiivsete õigusmõistete sisustamise näitel. Tartu, 2015, 179 lk.
52. **Kadi Pärnits**. Kollektiivlepingu roll ja regulatsioon nüüdisaegsetes töösuhetes. Tartu, 2015, 179 lk.
53. **Leonid Tolstov**. Tort liability of the director to company's creditors. Tartu, 2015, 169 p.
54. **Janar Jäätma**. Ohutõrjeõigus politsei- ja korrakaitseõiguses: kooskõla põhiseadusega. Tartu, 2015, 242 lk.
55. **Katre Luhamaa**. Universal Human Rights in National Contexts: Application of International Rights of the Child in Estonia, Finland and Russia. Tartu, 2015, 217 p.
56. **Mait Laaring**. Eesti korrakaitseõigus ohuennetusõigusena. Tartu, 2015, 267 lk.
57. **Priit Kama**. Valduse ja kohtuliku registri kande publitsiteet Eesti eraõiguses. Tartu, 2016, 194 lk.
58. **Kristel Degener**. Abikaasade vara juurdekasvu tasaarvestuse varasuhe. Tartu, 2016, 242 lk.
59. **Olavi-Jüri Luik**. The application of principles of European insurance contract law to policyholders of the Baltic states: A measure for the protection of policyholders. Tartu, 2016, 228 p.
60. **Kaido Künnapas**. Maksukohustuse täitmise preventiivne tagamine enne maksukohustuse tuvastamist: ettevaatuspõhimõte maksumenetluses.Tartu, 2016, 388 lk.
61. **Eve Fink**. Õiguspärase ootuse kaitse põhimõtte eeldused ja piirid Euroopa liidu õiguses. Tartu, 2016, 245 lk.
62. **Arsi Pavelts**. Kahju hüvitamise nõue täitmise asemel ostja õiguste näitel. Tartu, 2017, 414 lk.
63. **Anna-Maria Osula**. Remote search and seizure of extraterritorial data. Tartu, 2017, 219 p.
64. **Alexander Lott**. The Estonian straits. Exceptions to the strait regime of innocent or transit passage. Tartu, 2017, 259 p.
65. **Dina Sõritsa**. The Health-care Provider's Civil Liability in Cases of Prenatal Damages. Tartu, 2017, 365 p.

66. **Einar Vene**. Ajaline faktor halduskohtumenetluses tühistamis- ja kohustamiskaebuse lahendamist ning rahuldamist mõjutava tegurina. Tartu, 2017, 294 lk.
67. **Laura Feldmanis**. Süüteokatsest loobumise instituudi põhjendus ja kohaldatavuse piirid kuritegelikule eeltegevusele. Tartu, 2017, 292 lk.
68. **Margit Piirman**. Inimese pluripotentsete tüvirakkudega seotud leiutiste patentimise piirangud vastuolu tõttu avaliku korra ja moraaliga (Eesti patendiõiguse näitel). Tartu, 2018, 246 lk.
69. **Kerttu Mäger**. The Taming of the Shrew: Understanding the Impact of the Council of Europe's Human Rights Standards on the State Practice of Russia. Tartu, 2018, 305 p.
70. **Tambet Grauberg**. Õiguse kuritarvitamise keelamise põhimõte: Euroopa Kohtu seisukohtade mõju liikmesriigi maksuõigusele. Tartu, 2018, 277 lk.
71. **Maarja Torga**. The Conflict of Conflict Rules – the Relationship between European Regulations on Private International Law and Estonian Legal Assistance Treaties Concluded with Third States. Tartu, 2019, 252 p.
72. **Liina Reisberg**. Semiotic model for the interpretation of undefined legal concepts and filling legal gaps. Tartu, 2019, 232 p.
73. **Mari Schihalejev**. Debtor-Related Creditors' Claims in Insolvency Proceedings. Tartu, 2019, 137 p.
74. **Ragne Piir**. Mandatory Norms in the Context of Estonian and European International Contract Law: The Examples of Consumers and Posted Workers. Tartu, 2019, 117 p.
75. **Madis Ernits**. Constitution as a system. Tartu, 2019, 201 p.
76. **Kärt Pormeister**. Transparency in relation to the data subject in genetic research – an analysis on the example of Estonia. Tartu, 2019, 184 p.
77. **Annika Talmar**. Ensuring respect for International Humanitarian Law 70 years after the adoption of the Geneva Conventions of 1949. Tartu, 2020, 286 p.
78. **Liliia Oprysk**. Reconciling the Material and Immaterial Dissemination Rights in the Light of the Developments under the EU Copyright *Acquis*. Tartu, 2020, 397 p.
79. **Katrin Sepp**. Legal Arrangements in Estonian Law Similar to Family Trusts. Tartu, 2020, 163 p.
80. **Taivo Liivak**. Tort Liability for Damage Caused by Self-driving Vehicles under Estonian Law. Tartu, 2020, 206 p.
81. **Anne Veerpalu**. Regulatory challenges to the use of distributed ledger technology: Analysis of the compliance of existing regulation with the principles of technology neutrality and functional equivalence. Tartu, 2021, 365 p.
82. **Maren Krimmer**. Protecting Property Rights through International Treaties but With Constitutional Brakes: The Case of Contemporary Russia. Tartu, 2021, 153 p.