Stanford – Vienna
Transatlantic Technology Law Forum
A joint initiative of
Stanford Law School and the University of Vienna School of Law

TTLF Working Papers

No. 102

‘Quis Custodiet Ipsos Custodes’: Regulating AI-powered Workplace Surveillance in Europe and the United States

Christine Carter

2023

TTLF Working Papers

Editors: Siegfried Fina, Mark Lemley, and Roland Vogl

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology, and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Christine Carter holds both a BA (Double-First Class Honors) and a LLM (Distinction Honors) from the University of Cambridge, UK, where she has been awarded numerous academic prizes and scholarships for her legal work. She has worked in the International Arbitration practice group of Arnold & Porter LLP where she assisted the practice group in various cases involving the representation of sovereign States and multi-national corporations in investor-state arbitrations and international commercial arbitrations. She is currently a Prince of Wales Scholar at the Inns of Court in London. Christine has been a TTLF Fellow since August 2023. Her research interests lie in the areas of EU Law, Law & Economics, and Employment Law. Within these areas, she focuses on the regulatory, economic and technical implications of emerging technologies, particularly in relation to the regulation of Algorithmic Governance, Big Data, Digital Surveillance and Platform Economies.

General Note about the Content

The opinions expressed in this paper are those of the author and not necessarily those of the Transatlantic Technology Law Forum or any of its partner institutions, or the sponsors of this research project.

Suggested Citation

This TTLF Working Paper should be cited as:
Christine Carter, 'Quis Custodiet Ipsos Custodes': Regulating AI-powered Workplace Surveillance in Europe and the United States, Stanford-Vienna TTLF Working Paper No. 102, http://ttlf.stanford.edu.

Copyright

Abstract

AI-powered surveillance is a new norm in the modern workplace that monitors the performance of workers through advanced surveillance and data tracking technologies. Most are unaware of the fact that AI-powered surveillance can, among many other things, log keystrokes and mouse movements, activate webcams and microphones, and in some cases even track the facial expressions and body movements of the general workforce. With these technologies, employers are able to reach performance-driven assessments of workers' activity and productivity levels, motivation and success chances, as well as predict emotions, mood and stress levels. Against this background, the paper will conduct a comparative review of worker privacy rights in Europe and the United States to examine how privacy laws respond to the emergence of AI-powered surveillance in the workplace. The aim is to assess where both legal systems draw the line between the fair use of productivity-enhancing technologies and the unfair use of privacy-eroding technologies. In the European context, the paper will focus on the general right to privacy in Article 8 of the European Convention of Human Rights, as well as the more specific privacy and data protection provisions that are set out in the General Data Protection Regulation. In the American context, the paper will assess the privacy protections found in the Fourth Amendment of the United States Constitution, the general privacy torts, as well as in relevant federal and state legislation.

'Quis Custodiet Ipsos Custodes': Regulating AI-Powered Workplace Surveillance in Europe and the United States

1. Introduction

Originally rooted in 18th century Fordism[1], workplace surveillance has advanced leaps and bounds with the emergence of new AI analytics that process information on virtually all aspects of, and often beyond, the sphere of work. There are no theoretical or practical limits on the types of data that can be collected by AI-powered surveillance; it can include physical, emotional, sensory or visual data that is analyzed by advanced algorithmic and machine learning processes. In addition, these processes often utilize inferential analytics, as well as extensive data mining and profiling techniques, that can make data-driven predictions and automate managerial and organizational decisions in the workplace. Together, these AI-powered processes constitute advanced and sophisticated surveillance measures that are deployed as a pseudo-electronic management system in the modern workplace to observe, supervise and sometimes even manage the workforce[2].

The proliferating use of AI-powered surveillance systems in the modern workplace exposes workers to unprecedented privacy invasions. Employers gather, process and utilize workforce data for all kinds of purposes, regardless of whether such are anticipated or foreseeable. The workforce are often unaware of the fact that they are subject to strict AI-powered surveillance, and have no control over the ultimate usage of their data; they lack the opportunity to challenge, review, or meaningfully consent to the ultimate use of the data retrieved by AI-powered surveillance. With the increasing amount and variety of personal data that is collected and subsequently processed by these systems, the distinction between

[1] *See generally* David Landes, *The Unbound Prometheus: Technological Change and Industrial Development in Western Europe from 1750 to the Present* (first published 26 June 2003 Cambridge University Press 2nd edition); *see further,* Michael C. Jensen, William H. Meckling, 'Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure' (1976) 3(4) Journal of Financial Economics 305-360

[2] European Fundamental Rights Agency, *Data Protection in the European Union: The Role of National Data Protection Authorities* (2010) (Publications Office of the European Union 2010) paras 4.3.4-4.3.5 https://fra.europa.eu/en/publication/2010/data-protection-european-union-role-national-data-protection-authorities

productivity-enhancement and privacy-erosion becomes exceedingly illusive and difficult to maintain.

Accordingly, such poses three particular challenges to the basic privacy, data autonomy, and moral control of the workforce in Europe and the United States. *First*, AI-powered surveillance is more intrusive than traditional methods of workplace surveillance. Its frequent usage of inferential analytics allows employers to discover hidden patterns and trends within the available workforce data that can be used to generate new, and previously undiscoverable, insights into their workers' identity and private lives. *Second*, AI-powered surveillance is also more pervasive than traditional methods of workplace surveillance. It often involves the continuous and remote monitoring of workers through open-source operating systems that are able to instantaneously intercept and exchange much greater volumes and varieties of workforce data. *Third*, the complexity and sophistication of AI-powered surveillance, including its potential as a system of algorithmic management, grants employers the power to use the data to their ultimate pleasing; whether as performance-indicators, success predictors, or other.

These challenges contribute to the so-called commodification and datafication of the employment relationship, and create an inevitable trade-off between the need to protect and preserve privacy in a densely digitized and information-based society, against the need to maintain and support productivity and innovation in labor and capital-driven economies. Consequently, the question arises whether the law should perceive privacy as relative to technological progress and industrial development, or as an invariable and core aspect of the protection of individual rights and freedoms.

This paper will analyze the impact of AI-powered workplace surveillance on worker privacy rights in EU and US law. In particular, the paper will focus on the technological competence of the contemporary privacy law frameworks in Europe and the United States and determine whether these are able to govern the introduction of these technologies in the modern workplace.

The introduction is followed by four sections. *Section 2* demonstrates how AI-powered surveillance systems differ from traditional surveillance systems, and illustrates how such affects the ways in which the law should respond to these workplace technologies. *Section 3* then examines the regulation of these technologies in European law, and particularly focuses on the general protection of privacy rights under the European Convention of Human Rights ("ECHR"), and European Charter of Fundamental Rights ("CFREU") as well the specific protection conferred through the General Data Protection Regulation ("GDPR")[3]. *Section 4* assesses how the equivalent rights are protected in the United States where workers seeking redress for privacy intrusion may seek relief under the Fourth Amendment of the United States Constitution where the violation has occurred in a public sector office, whilst private sector workers may rely on the analogical operation of the tort of intrusion upon seclusion. The section will also consider how these privacy laws are aided by piecemeal state privacy legislation and the Electronic Communications Privacy Act ("ECPA")[4]. *Section 5* will address what can be learnt from the comparative assessment of privacy laws in Europe and the United States and assess what this means for legal reform.. *Section 6* concludes.

2. Distinguishing AI-powered from Traditional Surveillance

In order to assess the technological competence of privacy laws in Europe and the United States, it is first necessary to consider the reasons why AI-powered surveillance differs from

[3] 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 2016 L 119/1

[4] Electronic Communications Privacy Act of 1986 (ECPA) (18 U.S.C.) §§2510-2523

traditional surveillance systems, as well as understand what this means for the protection and safeguarding of privacy in the modern workplace. There are several ways in which AI-powered surveillance systems distinguish themselves from more traditional surveillance systems, both in the way in which they collect and analyze data, as well as reach evidence-based decisions thereon.

2.1. Data Discovery and Generation

First, with the scientific and technological advancement of AI analytics, data may be collected at a much larger scale and with granular precision. For instance, data can be sourced from the live monitoring of workers' computer screens[5], keystrokes[6], social messages[7] and emails[8]. Similarly, biometric, sociometric, or GPS data can collected from wearable health and fitness to radio-frequency ID (bio-RFID) tracking devices, smart glasses or phone sensors[9]. Through the use of algorithmic correlations, these technologies generate limitless inferences about some of the most personal, and private elements, of the lives of the workforce [10]; they evaluate social interactions on messaging platforms and emails to prognose an individual's emotions, feelings or behaviour patterns of workers, or estimate their social affiliation or

[5] Peter Walker, 'Call centre staff to be monitored via webcam for home-working infractions' (Guardian News, 26 March 2021) <https://www.theguardian.com/business/2021/mar/26/teleperformance-call-centre-staff-monitored-via-webcam-home-working-infractions> accessed 15 March 2023

[6] Johnathan Keane, 'Bosses putting a digital leash on remote workers could be crossing a privacy line' (CNBC News, 27 May 2021) <https://www.cnbc.com/2021/05/27/office-surveillance-digital-leash-on-workers-could-be-crossing-a-line.html> accessed 15 March 2023

[7] Reid Blackman, 'How to monitor your employees while respecting their privacy' (Harvard Business Review, 28 May 2020) <https://hbr.org/2020/05/how-to-monitor-your-employees-while-respecting-their-privacy> accessed 15 March 2023

[8] Kate Morgan and Delaney Nolan, 'How worker surveillance is backfiring on employers' (BBC News, 30 January 2023)<https://www.bbc.com/worklife/article/20230127-how-worker-surveillance-is-backfiring-on-employers> accessed 15 March 2023

[9] Christopher Rowland, 'With fitness trackers in the workplace bosses can monitor your every step and possibly more' (Washington Post, 16 February 2019) <https://www.washingtonpost.com/business/economy/with-fitness-trackers-in-the-workplace-bosses-can-monitor-your-every-step--and-possibly-more/2019/02/15/75ee0848-2a45-11e9-b011-d8500644dc98_story.html> accessed 15 March 2023

[10] Ifeoma Ajunwa, Kate Crawford,and Jason Schultz 'Limitless worker surveillance' (2017) 105(735) California Law Review 101-143 https://ssrn.com/abstract=2746211 accessed 5 Mar 2023

propensity to join a particular group or culture[11]. To give an example, sociometric badges can process oral data through voice-pitch analysis software to determine the mood of workers[12]. Similar can be achieved with facial recognition software and natural language processing systems that analyse physical expressions of workers and assess concentration levels, as seen in Amazon's use of AI-powered cameras in delivery trucks that monitor whether a driver yawns during their route of delivery to compute their levels of drowsiness or distraction. Such imposes significant burdens on the drivers' welfare, health and safety. Drivers feel the need to skip breaks, maintain constant high levels of activity and occasionally even take short-cuts in attempts to meet the performance targets of these AI-powered surveillance systems. This has been associated with increased levels of road traffic accidents and speeding, as well as general heightened feelings of stress and anxiety[13].

2.2. Data Exchange and Processing

Second, the interoperable exchange of data within linked-up devices generates an unprecedented volume of data of workers' personal lives and grants AI- powered surveillance the ability to monitor workers beyond the sphere of work[14]. These type of data exchanges often consist of complex intra-systems communications that contribute to the instantaneous and exponential proliferation of data between multiple operating systems. Data collected is therefore permanently retrieved by the employer for unlimited review and scrutiny. Workforce data is consequently left more exposed and vulnerable to data leaks, unwarranted access and

[11] Sandra Wachter, Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) 2019(2) Columbia Business Law Review 494-620 https://doi.org/10.7916/cblr.v2019i2.3424 accessed 10 March 2023

[12] Kai Fischbach et al 'Analyzing the Flow of Knowledge with Sociometric Badges' (2009) Science Direct http://www.ickn.org/documents/COINs2009_Fischbach_Gloor_Lassenius_etc.pdf

[13] Karen E.C. Levy, '*The Contexts of Control: Information, Power, and Truck-Driving Work*' (2015) 31(2) Information Society Journal 160-174 https://karen-levy.net/wp-content/uploads/2016/08/The-Contexts-of-Control-Information-Power-and-Truck-Driving-Work.pdfAccessed 7 March 2023

[14] *See for general explanation* Viktor Mayer-Schönberger & Kenneth Cukier, *Big Data: A revolution that will transform how we live, work and think* (Houghton Mifflin Harcourt, 2013)

unlimited sharing by both the employer as well as third-parties. This has to be viewed together with the fact that AI-powered surveillance is far less overt and far more encompassing than traditional workplace surveillance systems. The reality of these technologies is to provide employers with unlimited access to data sources that permit them to monitor workers' behaviour patterns at all times of the day through advanced accelerometers, triangulation algorithms and Bluetooth devices[15]. Surveillance is therefore no longer tethered to the physical workplace but often portable, remote and interoperable. The non-physical characterisation of these type of privacy intrusions, that often do not take place in the real but digital domain of the modern world, creates new frontiers for the law of privacy, which historically originate in the privacy traditions of a physical world in a time where technology and digital concepts were alien to mankind[16]. These more subtle and less visible forms of surveillance make it exceedingly difficult, if not impossible, to impose effective data limitations on algorithmic processing[17]. This is particularly evident in the use of AI analytics in monitoring and evaluating public communications made by workers on social media and other online forums. The same also applies to the use of AI-powered web cameras in remote working arrangements that capture and process data retrieved from the images of the worker's home and family[18]. Provided that these devices are installed on a relevant device, there is no limit as to the duration,

[15] Alan Kohll, A, '8 Things You Need to Know about Employee Wellness Programs' (Forbes News, 16 April 2016) https://www.forbes.com/sites/alankohll/2016/04/21/8-things-you-need-to-know-about-employee-wellness-programs/?sh=6290411d40a3 accessed 4 March 2023

[16] Patricia Sánchez Abril, 'Recasting Privacy Torts in a Spaceless World' (2007) 21(1) Harvard Journal of Law & Technology, 2-47 http://jolt.law.harvard.edu/articles/pdf/v21/21HarvJLTech001.pdf accessed 28 February 2023

[17] Michael Veale, Reuben Binns, Lillian Edwards, 'Algorithms that remember: model inversion attacks and data protection law' (2018) 376(2133) Philosophical Transactions of Royal Society Publishing Journal https://royalsocietypublishing.org/doi/10.1098/rsta.2018.0083 accessed 20 February 2023

[18] Shikun Zhang et al '"Did you know this camera tracks your mood?": Understanding Privacy Expectations and Preferences in the Age of Video Analytics. Proceedings on Privacy Enhancing Technologies' (2021) 2(1) 282–304
https://users.ece.cmu.edu/~lbauer/papers/2021/popets2021-video-prefs.pdf accessed 29 February 2023

frequency and time of monitoring and data processing, with the possibility that workers may be monitored around the clock, irrespective of whether they are on or off-duty[19].

2.3. Data Usage and Decision-Making

Third, AI-powered surveillance technologies increase the risk of a so-called 'function creep' where employers use the data collected by AI-powered surveillance for an unwanted, unspecified or unforeseen purpose. The autonomy of workers over their own data is not only challenged by the invasive nature of these technologies but by the way in which they use the data; data acquired for one purpose may be potentially used for an unspecified amount of other reasons. This is due to the general versatility of data and the multifaceted potential of AI analytic tools that are capable of drawing infinite correlations and inferences from both current and historical data sets[20]. Data may also be retained on file by the employer for unduly long periods of time where the AI-powered surveillance is used to create pools of training data that are subsequently used by the employer for an unlimited and unspecified amount of decision-making needs, including organisational and managerial determinations that relate to past, present and future issues in the workplace[21]. For instance, corporate wellness tracking programmes provide employers with access to the raw health data of their workers that can be used to determine whether a worker is fit to work or suitable for a physical task. However, it can equally be used to calculate the possibility of sickness, pregnancy, or time-off requests by the workforce[22]. Not only do such practices raise significant issues of algorithmic discrimination, they also make workers vulnerable to data leaks and the possibility of third-

[19] Brishen Rogers, 'The law and political economy of workplace technological change' (2020) 55(1) Harvard Civil Rights-Civil Liberties Review 531-583 https://harvardcrcl.org/wp-content/uploads/sites/10/2020/10/Rogers.pdf accessed 1 March 2023

[20] Sandra Wachter et al Supra 11, at pp. 505-512

[21] Michaele Veale supra 17, see 'storage data discussion' at pp.1-12

[22] *See for instance* Frank Hendrickx 'Employment Privacy' (2014) Comparative labour law and industrial relations in industrialized market economies, Alphen aan den Rijn, *Kluwer Law International*

parties acquiring confidential and private information[23]. Similar is true with the use of happiness metrics in Emotion AI[24]. Although the algorithm may process data in a way that services to monitor the morale levels of workers, the data could equally be used to create personality profiles that determine a worker's future in a particular company or their suitability for a particular position[25]. This touches on the fact that it is often not the strict collection of the raw data itself that is intruding on privacy rights but the actual use of the data and the potential inferences and predictions that can be drawn from it[26].

3. The Privacy Framework of European law

The language of privacy in Europe, as generally expressed by the WP29 in its Opinion 2/2017, is that the advancement of AI technologies makes it more, not less, necessary that the privacy is preserved and maintained in the employment context[27]. To date, European law expressly provides for privacy rights in Article 8 ECHR as well as in Articles 7 and 8 CFREU respectively. These general rights-based frameworks must be read against the technical provisions of the GDPR. Together, these regimes create a patchwork of regulatory safeguards, consisting of a mixture of general rules, principles and policy opinions that seek to balance the employer's legitimate business interests against the worker's fundamental rights and freedoms relating to data autonomy and privacy.

[23] Moriz Büchi et al, 'The chilling effects of algorithmic profiling: Mapping the issue' (2020) 36(105367) Computer Law & Security Review https://doi.org/10.1016/j.clsr.2019.105367accessed 20 March 2023

[24] Kat Roemmich, Florian Schaub, and Nazanin Andalibi, 'Emotion AI at Work: Implications for Workplace Surveillance, Emotional Labor, and Emotional Privacy' *ACM Conference on Human Factors in Computing Systems,* 23-28 April 2020, Hamburg, Germany https://doi.org/10.1145/3544548.3580950

[25] Phoebe Moore, *The Quantified Self in Precarity: Work, Technology and What Counts* (2017 Routledge) p. 6

[26] Article 29 Data Protection Working Party, *Opinion 03/2013 on Purpose Limitation*, 00569/13/EN, WP203 (2 April2013)https://ec.europa.eu/justice/article29/documentation/opinionrecommendation/files/2013/wp203_en.pdf accessed 10 March 2023, p. 47

[27] Art 29 Working Party, 'Opinion 2/2017 On Data Processing at Work' (WP 249 8 June 2017), pp.4-5

3.1. European Convention of Human Rights

Article 8 of the ECHR provides a *'right to respect for private and family life, home and correspondence'*. The application of this right in the workplace has been endorsed by the European Court of the Human Rights ('ECtHR') in *Yonchev v Bulgaria*[28], as well as in *Antović and Mirković v. Montenegro*[29]. In *Bärbulescu v Romania* the ECtHR has examined the extent of the application of the privacy right and noted that it is not an absolute but qualified right that applies with the proviso that privacy laws are fluid and relative to the contemporary standards of society in determining what exactly amounts to a reasonable expectation of privacy of workers[30]. In *López Ribalda v Spain*[31] and *Köpke v Germany*[32] the ECtHR ruled that the use of video surveillance did not amount to an intrusion into a person's private affairs. The same conclusion has been reached on the basis of data acquired through GPS tracking in *Florindo v Portugal*[33]. Tracking workers is *prima facie* compliant with privacy rights, except where such amounts to an unreasonable interference that neither pursues a legitimate aim, is necessary or proportionate. Such intrusion could be established in *Halford v United Kingdom*[34] where the police force unlawfully intercepted an officer's personal telephone calls. This is consistent with *Copland v United Kingdom*[35] and suggests that the law looks for some distinguishing feature in the collection of information. The question then, is whether the particular use of AI processing can constitute this distinguishing feature that enables courts to resolve the conflict between the business needs of the employee and the freedoms and privacy of the worker?

[28] *Yonchev v Bulgaria* (2017) (Application no. 12504/09), paras 45-47
[29] *Antović and Mirković v Montenegro* (2017) (Application no. 70838/13) paras 40-45
[30] *Bärbulescu v Romania* (2016) IRLR 235, paras 52-54, 78, 80, 133, 140, 141
[31] *López Ribalda v Spain* (2018) ECHR 14
[32] *Köpke v Germany* (2010) ECHR 1725
[33] *Florindo de Almeida Vasconcelos Gramaxo v. Portugal* (2022) (Application no. 26968/16)
[34] *Halford v United Kingdom* (1997) 24 E.H.R.R 523
[35] *Copland v United Kingdom* (2007) ECHR 253

The Dutch Civil Court in *NCJM et al. and FNV v The State of the Netherlands* ('SyRi')[36] recently found such a distinguishing feature that constituted an infringement of the data subject's privacy rights where the Dutch government made use of a 'System Risk Indication' algorithm to create risk-profiles of citizen's propensity to commit fraud. Although there was no use of deep learning or data mining algorithms in SyRi, the court did not hesitate to find that the use of advanced probabilistic analytics within the risk-assessment were equivalent to deep learning and data mining technologies[37]. This in the court's view, coupled together with the long-lasting effects of the risk-profile created by SyRi amounted to a serious intrusion of the data subject's right to private life[38]. This decision will have significant implications for AI-powered workplace surveillance, particularly where advanced machine learning algorithms are used in predictive analytics to obtain data on workers and create success profiles for future careers prospects or to generally evaluate the performance of the workforce.

The lawfulness of AI-powered surveillance under Article 8(2) of the ECHR will significantly depend on the objective of its use[39]. In *Libert v France,* the ECtHR was persuaded by the fact that an employer wished to examine the personal files of a worker on their work computer to determine whether or not that individual was using the computer provided to them for proper purposes and pursuant to their contractual obligations[40]. The case exemplifies the desire of the court to strike a balance between the employers commercial needs and the workers personal interests and suggests that courts will be cognizant of the productive potential of AI analytics in generating efficiency amongst workers. The employer may alternatively rely on organizational needs, health and occupational needs, or security needs to justify the use of AI-powered surveillance. That does not necessarily mean that this economic rationale will take

[36] *NCJM et al. and FNV v The State of the Netherlands (SYRI),* District Court of the Hague, 6 March 2020, ECLI:NL:RBDHA:2020:865
[37] SyRi, supra 36, paras 6.50-6.51
[38] SyRi, supra 36, paras 6.59-6.60
[39] See further Articles 16 and 17 CFREU, Article 1 Protocol to the ECHR
[40] *Libert v. France* (2018) (application no. 588/13), para 46

greater precedence than the privacy interests, particularly so where the employer cannot give a compelling rationale for the use of AI-powered surveillance. For instance, whilst it may be reasonable to analyze facial movements on webcams for remote workers to track productivity, such will most likely not suffice as a sufficient reason for analyzing the worker's mood. Accordingly, the legality of AI-powered surveillance will to a greater extent depend on the purpose of the data processing and whether such contributes to a reasonable objective: is it merely to protect company property or ensure proper interaction with customers or is it to carry out covert investigations of the behavior and character of workers. The former will likely be considered a more satisfiable objective than the latter. It will also depend on the type of data collected by the AI-powered technology and how such relates to task performance. Whilst it may be possible to rationalize the collection of GPS data to compute routes, logistics and performance evaluations of delivery drivers, it is more difficult to argue that the collection of biometric data from wearable wrist badges serves a legitimate purpose of evaluating the general behavior and motivation of delivery drivers. Such principle, and the need for heightened legal scrutiny in these contexts, was expressly recognized by the ECtHR in *Gaughran v United Kingdom*[41] where it was held that the indefinite detention of biometric data and photographs of a convicted person amounted to a breach of Article 8 of the ECHR.

Article 8(2) imposes a further requirement on the use of surveillance and requires any such measures to be necessary and proportionate to the aim it seeks to achieve. The distinguishing features of AI-powered surveillance challenge the conventional reading of privacy jurisprudence amongst courts and commentators alike[42]. In these instances, courts will have to be meticulous in their analysis of issues of transparency, proportionality, consent and data minimization by analogy to the main data principles in Article 5 of the GDPR.

[41] *Gaughran v United Kingdom* (2020) (Application no. 45245/15)

[42] Jeremias Adams-Prassl, *'What if Your Boss Was an Algorithm?* The Rise of Artificial Intelligence at Work' (2019) 41(1) Comparative Labor Law & Policy Journal 123-124

Regarding the issue of transparency, consideration will have to be given to Articles 12-15 of the GDPR that provide basic transparency rights that regulate data processing. Courts will regard these in the determination of whether the particular AI is opaque, or otherwise subjects the workforce to an unaccountable process, which will influence whether the given AI-powered surveillance measure is compliant with Article 8(2) of the ECHR.

In relation to the issue of consent, Article 29 WP and the European Data Protection Board note that workers are only seldom able to provide free and informed consent due to their contractual subordination to their employers[43]. Workers may therefore risk social or organizational pressure to opt-in or not opt-out from AI-powered surveillance[44]. This was expressly recognized by the Dutch Data Protection Authorities in their landmark decision to shut down a company's pilot scheme that required workers to wear Fitbits for data processing purposes[45]. Free and informed consent will also not be possible where vague and opaque algorithmic processing techniques are used. Such was recently decided by the Italian Supreme Court who found that a data subject's ability to consent is premised on there being sufficient transparency in the algorithmic decision-making process[46]. The decision, although not originally based on, echoes the general conditions for consent laid out in Article 7 and Recitals 32-33 of the GDPR.

This stage of the legal enquiry also relates to issues of data minimization that call for consideration of Article 5(1)(c) of the GDPR. Workplace surveillance should be designed to be as minimally intrusive to the worker's privacy rights as possible to achieve its objective. In

[43] European Data Protection Board Guidelines 05/2020 on consent under Regulation 2016/67, pp.9-10 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

[44] Frank Hendrickx, Aline Van Bever, 'Article 8 ECHR: Judicial Patterns of Employment Privacy Protection' in Filip Dorssemont, Klaus Lörcher, Isabelle Schömann, *The European Convention on Human Rights and the Employment Relation* (Hart Publishing 2013) p.185

[45] Autoriteit Persoonsgegevens (Dutch data protection authority), *AP: Verwerking gezondheidsgegevens wearables door werkgevers mag niet* (March 8, 2016), https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-verwerking- gezondheidsgegevens-wearables-door-werkgevers-mag-niet.

[46] Corte di Cassazione, sez. I Civ. – 25/05/2021, n. 14381

contrast to traditional surveillance, where the data minimization principle only needs to be balanced against the need for security and good conduct in the workplace, AI-powered surveillance risks the additional trade-off that needs to be met between data accuracy and data minimization. This is due to the fact that the use of inferential and predictive analytics requires high volumes of training data. Any minimization to input data will therefore not only impact the reliability of the algorithm but have serious repercussions for those who are subject to the review of the AI-powered surveillance. In circumstances where AI-powered surveillance is used to monitor worker behavior and make informed predictions about their performance, this risks increasing the likelihood of the AI making ill-informed decisions. In SyRi, the court considered the issue of data minimization in conjunction with that of purpose limitation when examining the limitless categories of data that were subject to the processing of the fraud prediction algorithm[47]. This demonstrates a functional approach to resolving the trade-off between accuracy and privacy by reference to the overall purpose and objective of data privacy laws. It also suggests that a court will not only carefully scrutinize the relevant AI application in question but consider its interaction with the overall social, economic and cultural interests of the data subject. In doing precisely such in the related context of *Gaughran v United Kingdom,* the ECtHR rejected the Respondent Government's utilitarian argument that the greater data retention would lead to a greater reduction in crime rates as a slippery slope[48]. A similar outcome was also reached by the ECtHR in *Szabó and Vissy v. Hungary* where the court found that the enhancement of technological inception in advanced surveillance technologies, makes it more, not less, imperative for courts and legislators to develop adequate legal protections to uphold individual rights[49].

[47] *SyRI* supra 36, at paras 6.99–6.102.

[48] *Gaughran,* supra 41, para 89

[49] *Szabó and Vissy v. Hungary* (2016) (Application no. 37138/14) para 68

3.2. General Data Protection Regulation

The GDPR provides an alternative route for workers to rectify the inherent information asymmetry that is introduced into the employment relationship through the use of AI-powered surveillance. The main provisions within the GDPR that are of assistance are Articles 17 and 22 respectively.

Pursuant to Article 17 and Recital 65 of the GDPR, workers have the so-called right to be forgotten, which entitles them to request the erasure of their personal data or abstain from their data being processed. *Prima facie,* such right would prevent AI-powered surveillance from overreaching into the worker's personal data. However, the right to be forgotten has serious deficiencies in its application to the AI-powered surveillance context.

For one, the right is in theory applicable to a closed information system but does not operate as effectively in an open or cloud-based information system[50]. Given that the majority of AI analytics systems are open sourced, it will prove an impossible task to constrain the flow of information that has already been exchanged and processed between multiple interconnected systems. The vast proliferation of the so-called 'Internet of Things'[51] only perpetuates the advancing spread of personal information among different integrated systems that challenges the viability of Article 17 in this multisystemic digital reality even further.

Second, the right also fails to capture the fact that data can't simply be deleted from the relevant code of the algorithmic process but must be overwritten. Accordingly, even if it were in theory possible to remove the relevant data of an individual without any trace, it would endanger the integrity of the remaining data of all other individuals who are subject to the same

[50] Bernd Malle, Peter Kieseberg, Edgar Weippl, and Andreas Holzinger, 'The Right to Be Forgotten: Towards Machine Learning on Perturbed Knowledge Bases' (2016), Workshop on Privacy Aware Machine Learning

[51] *See for general introduction on the Internet of Things and the regulatory responses of law*
Giedo Noto La Diega, *Internet of Things and the Law: Legal Strategies for Consumer-Centric Smart Technologies* (Routledge Research in the Law of Emerging Technologies. London: Routledge 2022)

AI-powered data processing sequence[52]. Particularly with self-learning and machine learning algorithms, the removal of one part of a particular data set risks corrupting the outcome of the overall analysis. This not only frustrates the equal treatment all other workers who are subject to the same data sample, but risks leading to unfair results where the data obtained from AI-powered surveillance is then used to reach evidence-based management decisions

Providing workers with an effective right to be forgotten from the AI-powered surveillance would lead to two practical hurdles where AI-powered surveillance systems make use of such machine learning technologies. First, for the right to be meaningfully applied, it would require the historical training data set to be amended to ensure that the disputed data has been properly erased and that the remaining data remains viable. This is a time-consuming activity that would impose significant costs and require advanced coding skills, as well as general access to the relevant program. This is not likely achievable in many employment contexts. Second and alternatively, the machine learning model could be amended to adopt a different training method that does not implicate the disputed data. The outcome in this scenario would be equal to changing the input data. However, this is also not feasible in many employment contexts where machine learning programs, such as facial recognition or natural language software in webcams to screen interview candidates, are not something that are quickly remodeled without teams of dedicated computer scientists or engineers[53]. It would, however, ensure the continuing relevance of data that is sourced by AI-powered surveillance. Particularly in contexts where algorithms are used to evaluate worker's performance or conduct, it is questionable whether there should be a limitation on the extent of scrutiny that workers should be subjected to by these analytical processes. From this perspective, the right

[52] Tiffany Li, Eduard Fosch Villaronga, Peter Kieseberg 'Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten' (2018) 34(304) Computer Law & Security Review https://scholarship.law.bu.edu/faculty_scholarship/817

[53] Michael Veale et al, supra 17, at pp.9-10

to be forgotten would ensure that all data is relevant, up to date, and consistent with current performance standards.

The alternative is to rely on Article 22 of the GDPR as a more targeted solution for AI-powered surveillance systems, specifically for those that make use of algorithmic and automated decision-making technologies. Article 22 overcomes the technological deficit of Article 17 and is generally applicable in the employment context[54]. Not all types of AI-powered surveillance, however, will be captured by this provision, but only those that involve a solely automated decision. For instance, the use of AI analytics to scan worker communications and provide real-time updates on matters such as whether the worker has committed a violation of a company policy, may not be captured by Article 22. By contrast, using AI analytics to scan worker communications and provide a report on their general behavior and conduct at work that is then used to make recommendations to the employer on who should be promoted, demoted, let go, or fired, will in contrast be captured by Article 22[55]. This distinction is based on the degree of automation involved and therefore on the issue of whether algorithm is autonomously reaching the decision or merely processing data that leads up to a human decision-making process. The protection afforded by Article 22 in the workplace surveillance context is therefore not absolute but contingent upon the degree of sophistication and autonomy of the algorithmic decision-making process[56]. These legal distinctions can be hard to apply to the practical realities of computer science and human labor: if there is human intervention in any of the decision-making elements, Article 22 will not apply[57], even if such only amounts to a mere formality or 'rubber-stamping' process[58]. The latter is exceedingly likely in light of the

[54] *See e.g.* Three applicants v Ola Netherlands B.V. C/13/689705 / HA RK 20-258 ("Ola Netherlands"), District Court, Amsterdam (11 March 2021) para 4.37

[55] *See Ola Netherlands,* supra 53, paras 4.37-4.43

[56] *See* Michael Veale, Lilian Edwards, 'Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling' (2018) 34(2) Computer Law & Security Review 398-404

[57] *See generally* Garante per la protezione dei dati personali (Italy) – 9675440 https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9675440

[58] Michael Veale and Lilian Edwards, supra 17, p. 10

nature of algorithmic management in the workforce, especially where such is concerned with people analytics. In such a context, the algorithm may be, despite performing the substantial amount of decision-making, not the sole decision-maker. In these situations, Article 22 will not be of much use. Particularly in cases where the AI-powered surveillance operates on predictive analytics to profile the potential behavior, success or liabilities of certain workers, the technology may not reach a solely automated decision but a supporting decision that is then affirmed or denied by a human agent[59], which will subsequently elide the protective ambit of Article 22.

4. The Privacy Framework of American law

The notion of privacy occupies a more precarious position in American jurisprudence, particularly in the employment context. Privacy rights are historically taxonomized by the seminal writings of Dean Prosser as four distinct torts that exist alongside the Fourth Amendment of the United States Constitution[60]. The latter, however, only offers protection to public workers and will be of little, or no avail, to private sector workers[61]. Private sector workers are therefore dependent on the technological competence, and workplace proficiency, of the general privacy torts and individual state legislation. Although there are legislative provisions that confer a degree of privacy protection in the workplace, such as the ECPA, as well as individual state legislation, these are less encompassing than the protection conferred under the GDPR. They do not confer a catch-all solution to the use of AI-powered surveillance

[59] Michael Veale and Irina Brass, ‘Administration by Algorithm? Public Management Meets Public Sector Machine Learning’ in Karen Yeung and Martin Lodge (eds), *Algorithmic Regulation* (OUP 2019) 123–25

[60] William L. Prosser ‘Privacy’ (1960) 48(3) California Law Review 383-389

[61] *Skinner v. Railway Labor Executives Association* (1989) 489 U.S. 602, 623, 614; *see further* Lin Elbert ‘Prioritizing Privacy: A Constitutional Response to the Internet’ (2002) 17(3) Berkeley Technology Law Journal 1150

but only apply in a very specific set of circumstances. This reflects the overall degree of caution of the United States towards the concept of privacy and data autonomy, and its ultimate hesitation to establish such as a concrete set of legal rights.

4.1. Fourth Amendment of the United States Constitution

The Fourth Amendment regulates against unreasonable searches and seizures in public sector workplaces. The United States Supreme Court affirms its earlier decision in *O'Connor v. Ortega*[62] in the landmark decision in *City of Ontario v. Quon*[63] that the Fourth Amendment will protect privacy interests in the employment context where a worker can establish two legal requirements: (i) the employer possesses a subjective expectation of privacy that society is prepared to recognize as "*reasonable*"[64], and (ii) was the employer's intrusion into the privacy interests reasonably justified[65].

This balancing doctrine is of particular interest to the regulation of AI-powered surveillance because it suggests that there is no clear cut approach on what constitutes a lawful or unlawful inception of privacy interests. Rather, it will depend on a case-by-case basis and require a court to ask itself the following questions: how much surveillance is too much, what data is too private, what data processing methods are used, how reliable are the algorithmic results, and what business interests are more important than fundamental freedoms that cannot be attained without the help of AI-powered surveillance? These issues will be assessed holistically and in their entirety rather than as separated isolated issues. The pragmatism of this approach is further evident in the introduction of the mosaic theory by the United States Supreme Court in *United States v. Jones*[66]. Under this theory, courts will not only consider the

[62] *O'Connor v. Ortega* (1987) 480 U.S. 709, 717
[63] *City of Ontario v. Quon* (2010) 130 S. Ct. 2619, 2628–29
[64] *O'Connor* supra 61, at 715
[65] *O'Connor* supra 61, at719
[66] *United States v. Jones* (2012) 565 U.S. 400; see generally Orin S. Kerr 'The Mosaic Theory of the Fourth Amendment' (2012) 111(3) Michigan Law Review 312-353https://repository.law.umich.edu/mlr/vol111/iss3/1

intrusion of surveillance technologies in isolated steps but in their totality[67]. This approach is crucially significant for the workplace context where it is often not the use of artificial intelligence *per se*, but the total usage of such over a long period of time, that crosses the threshold between a permissible and impermissible practice.

There are, however, significant privacy loopholes in the Fourth Amendment that emerge from the recognition of the so-called third-party[68] and public availability defence[69]. These defences imply a careful distinction between personal and private data in the employment context. The loopholes create a serious flaw for the protection of the former type of data[70]. This is due to the fact that personal data may not necessarily be private in the sense of being isolated or unknown. Rather, it can include data that is just not work-related or relevant to the worker's job performance. This can include the worker's personal interests and activities outside of work, religious and political beliefs or general online presence. When such kinds of are concerned, the Fourth Amendment will not provide any protection or relief to workers. Consequently, the use of AI-powered surveillance to pre-screen candidates on the basis of their social media profiles, or monitor their general workplace performance or behaviour thereon, will be left unregulated by the law.

In contrast, the Fourth Amendment will apply where the AI analysis concerns inherently private data or operates in a way that could otherwise be achieved through less invasive measures. The latter could apply where remote AI-powered surveillance is used to monitor the webcam activity of workers in their private homes, since the courts have endorsed somewhat of an elevated status of privacy rights in this context[71]. It may also potentially assist

[67] *United States Jones* supra 65, 956 and 963-64

[68] *Smith v. Maryland* (1979) 442 U.S. 735, 743–45

[69] *California v. Greenwood (*1988) 486 U.S. 35, 40–41

[70] Bridget Dempsey 'Band-Aid on a Bullet Wound: Why the Email Privacy Act Is Necessary Triage in Federal Technology Law' (2014) 24(2) DePaul Journal of Art, Technology & Intellectual Property Law 339 https://via.library.depaul.edu/jatip/vol24/iss2/4

[71] *Kyllo v. United States* (2001) 533 U.S. 27, 35, 40

workers who are looking for avail from continuous location tracking outside of working hours or seeking relief from having their physical activity tracked, monitored and evaluated by wearable AI smart gadgets[72].

Such reflects the general judicial hesitation towards regulating technological progress through the Fourth Amendment. In *City of Ontario v. Quon*, Justice Kennedy famously explained that *"[t]he Court must proceed with care . . . . The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.*[73]*"* That is not to say that the courts do not recognize a distinction *per se* between privacy in the digital and the real sphere of life. Evidently, in *Riley v. California,* Justice Roberts aptly suggested that failing to distinguish between the two different spheres is akin to claiming that *" a ride on horseback is materially indistinguishable from a flight to the moon.*"[74] This recognition can be seen in the Supreme Court's decision not to extend the third-party doctrine to cell-site location information in *Carpenter v. United States*[75]. In delivering its judgement, the court recognized that participation in such information exchanges is no longer a purely voluntary choice but *"indispensable to participation in modern society."*[76]

4.2. Tort of Intrusion upon Seclusion

The law of the United States recognizes four distinct torts that may constitute a violation of privacy in its Restatement[77]. These are where privacy rights are violated by unreasonable intrusion on the seclusion of another; appropriation of the other's name or likeness;

[72] *See for further discussion*, Lisa Schmidt 'Social Networking and the Fourth Amendment: Location Tracking on Facebook, Twitter, and Foursquare' (2012) 22(2) Cornell Journal of Law and Public Policy 516-326 http://scholarship.law.cornell.edu/cjlpp/vol22/iss2/7

[73] *City of Ontario* supra 62, at 2629

[74] *Riley v. California* (2014) 573 U.S. 373, 2488

[75] *Carpenter v. United States* (2018) 138 S. Ct. 2206, 2220

[76] Ibid at 2220

[77] Restatement (Second) of Torts 652A-E (1977)

unreasonable publicity given to the other's private life; or publicity that unreasonably places the other in a false light before the public. The tort of intrusion upon seclusion is most relevant to the protection of privacy interests from AI-powered surveillance in the employment context[78]. Unlike the other three privacy torts, the tort of intrusion upon seclusion does not require the element of publicity to be established for a plaintiff wishing to bring a cause of action. This is due to the fact that the tort is primarily concerned with what was described by the District Court in *Russell v. ABC* as the offence of "*prying into the private domain of another*"[79]. Even so, there are several difficulties in applying this right to an employment context, yet alone a digital employment context.

The first reason is due to the fact that courts balance the tort of intrusion against the employer's reasonable business interests. Surveillance is therefore allowed where such can be rationalized on appropriate commercial reasons[80]. In this capacity, American courts have even gone so far to find that medical information, collected for the ordinary business needs of a company, does not violate a worker's privacy rights[81]. This parallels the approach of EU regulators in Article 8(2) of the ECHR in perceiving privacy as a qualified, as opposed to absolute, right that needs to be balanced against the commercial realities of everyday life and business. In terms of AI-powered surveillance, the employer can easily negate liability by arguing that ordinarily surveillance will not suffice without the use of AI analytics to not only ensure safety and compliance amongst workers, but also improve business efficacy and general workplace performance. Thus, setting up a high threshold for claimants to meet if they wish to illustrate an interference of their privacy rights within the workplace context, even in situations where the AI-powered surveillance has collected information, that does not *prima facie* seem or appear particularly relevant to the discharge of work-related duties. This will be particularly

[78] Restatement (Second) of Torts 652B (1977)

[79] *Russell v. ABC* (1995) U.S. Dist LEXIS 7528, 1995 WL 330920, at 8 (N.D. Ill.)))

[80] *Smyth v. Pillsbury Co.* (1996) 914 F. Supp. 97, 101

[81] *See Fletcher v. Price Chopper Foods of Trumann, Inc.* (2000) 220 F.3d 871, 879

problematic for those wishing to challenge the collection of raw health data from wearables or other biometric gadgets, where such can be argued to be necessary for productivity targets or activity tracking.

This relates in part to the second reason why it is difficult to find sufficient privacy protection from AI-based intrusion under the tort, which is due to the high bar set by courts in the United States who limit the application of the tort to personal data that is highly sensitive in nature[82]. This is problematic for AI-powered surveillance. Unlike more traditional systems of surveillance, the data collected by the surveillance system may itself not necessarily be deemed highly sensitive. Rather, it is once this data is subsequently processed through advanced data mining methods or processed through correlative and inferential AI analysis techniques that it acquires sensitive characteristics. Prior to this stage, the data collected by the AI-powered surveillance may be deemed innocuous and unworthy of special legal protection[83]. This will defeat the application of the tort to any instance where the data has been sourced and processed from the online activity of workers, or their social media activity, or even where they can be said to have voluntarily disclosed the information to their employer, even if such data is ultimately then used by the AI-powered surveillance technology to make a discovery about a worker that is sensitive or private in nature.

The third reason is due to the legal requirement that the intrusion is 'highly offensive'. Arguably, the use of Emotive AI that captures the wishes, feelings and emotions of workers may meet the legal threshold of this ground in certain circumstances where the use of such technologies leave workers feeling particularly distressed, anxious or upset. The same may also be true for illicit uses of biometric data that has a discriminatory effect on persons with

[82] *See e.g. Blackwell v. Harris Chem. N. Am., Inc*. (1988) 11 F.Supp.2d 1302; *Guccione v. Paley, No.* (2006) LLICV054002943S, WL 1828363 at 1, 2-3

[83] Daniel J. Solove 'The Digital Person: Technology and Privacy in the Information Age' (2004) GWU Law School Public Law Research Paper 2017-5; GWU Legal Studies Research Paper 2017-5. https://ssrn.com/abstract=2899131

particular illnesses or health concerns that are unrelated to their work performance[84]. The ground, will, however not be met in many other circumstances where AI is used to process internal and external office communications or generally review workers for their overall performance in the workplace through automated decision-making[85].

4.3. Electronic Communications Privacy Act

The current legislative baseline for workplace surveillance in the United States can be identified in the ECPA. This act is, to date, the only federal law that regulates electronic surveillance in the workplace and builds on the aforementioned constitutional and common law protections. The central force of the ECPA is to prohibit employers from intentionally intercepting the oral, wire and electronic communications that are stored by workers[86]. But the legislation contains several loopholes that allow employers to justify intrusive surveillance practices. For instance, the business purpose exception allows employers to justify surveillance where they can show a legitimate business purpose for the practice[87]. These purposes include: monitoring productivity in the workplace, evaluating the due and proper usage of workplace material and equipment[88], preventing unauthorized intrusions or theft by employees or third parties[89], investigating internal or external complaints against employees[90]. Additionally, there is the consent exception that allows surveillance where such has been consented to by the

[84] Pauline Kim ‘Data Mining and the Challenges of Protecting Employees Privacy under U.S. Law’ (2019) 40 Comparative Labor Law & Policy Journal 405-420; See also Pauline Kim ‘Big Data and Artificial Intelligence: New Challenges for Workplace Equality’ (2019) 57 University of Louisville Law Review 313 (2019) (Carl A. Warns, Jr. Keynote Speech).

[85] ibid

[86] Supra 4, §2511(1)(a)-(e)

[87] Supra 4, §2511(2)(a)

[88] *Muick v. Glenayre Electronics* (2002) 280 F3d 741 743

[89] *See e.g. McLaren v. Microsoft Corp.* (1999) No. 05-97-oo824, 1999 WL 339015; *Bohach v. City of Reno*, (1996) 932 F Supp. 1232

[90] Paul E. Hash & Christina M. Ibrahim ‘E-Mail, Electronic Monitoring and Employee Privacy’ (1996) 37 Texas. Law Review 893-897; Mindy C. Calisti ‘You Are Being Watched: The Need for Notice in Employer Electronic Monitoring’ (2008) 96(4) Kentucky Law Journal 649-668 https://uknowledge.uky.edu/klj/vol96/iss4/5;

worker[91]. Although the law has been developed to include stored data on computers and online communications such as email, it is unclear whether the thrust of the act will prove useful to smart gadgets that operate on AI analytics.

4.4. State Privacy Legislation

The technological development of AI privacy laws operates in a piecemeal fashion by individual states, with states such as New York[92], Connecticut[93] and Delaware[94] enacting laws that require employers to notify workers when they are utilizing surveillance technologies in the workplace, including those that are AI-powered. In a similar vein, Maryland[95] has recently passed a law that prohibits employers from using facial recognition technology in interviews unless such has been expressly consented for by the applicant. As of yet, the closest to a comprehensive federal regulatory solution of AI-powered surveillance technologies, or of AI in general, can be identified in the recent Blueprint for an Artificial Intelligence Bill of Rights that was issued in October 2022 by the White House Office of Science and Technology[96]. The Blueprint marks a pivotal step forward in regulating AI technologies in general and specifically recognizes the importance of data privacy and the need for heightened sensitivity towards the regulation of such in the employment context. This expressly includes the fact that "*Continuous surveillance and monitoring should not be used in education, work, housing, or in other contexts where the use of such surveillance technologies is likely to limit rights, opportunities, or access.*[97]*"* What is interesting about this policy statement is that it starkly distinguishes

[91] Supra 4, §2511(2)(c)

[92] Int. No. 1894-2020, New York City, Law Restricting Use of Artificial Intelligence in Employment Decisions (effective Jan. 1, 2023)

[93] Substitute Senate Bill No. 6 Public Act No. 22-15 (effective as Connecticut Data Privacy Act 'CTDPA' from 1 July 2023)

[94] Delaware General Assembly (2022), *Title 19 General Provisions Chapter 7 Employment Practices*, https://delcode.delaware.gov/title19/c007/sc01/index.html (accessed on 17 June 2022).

[95] Md. Code, Lab. & Empl. § 3-717, Facial Recognition Services Law (effective Oct. 1, 2020)

[96] White House (2022) AI Blueprint https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf (last accessed 17 March 2023)

[97] Ibid, p. 6 and see further pp. 30, 34

itself in its contextualization of the workplace; rather than perceiving this context in the conventional sense as a setting that warrants a lesser degree of privacy expectations, it takes a meaningful shift in recognizing one where privacy interests are more, not less endangered, by technological intrusion. The change in regulatory attitude may potentially reflect the overall shift in the social reality of data privacy in the modern workplace, building on the exponential increase in litigation seeking recognition of workers privacy rights. This includes the contemporary BIPA litigation in *Sherman v. Brandt Industries*[98] and *Cothron v White Castle System*[99], and the litigation in *Dittmann v. UPMC*[100], that cumulatively signal this growing legal trend of seeking general privacy standards in the workplace in reaction to the growing overreach of workplace technologies.

5. The Way Forward: The Trade-Off between Productivity and Privacy

Do the existing privacy frameworks in Europe and the United States address the challenges of AI-powered surveillance or must they be updated to catch up with the rapidly progressing technological development of these surveillance systems? Answering this question rests in part upon the technological competence of the current regulatory frameworks and their ideological balance between the protection of privacy and the promotion of productivity in the increasingly digitized and computerized economies. The European legislator has opted for a clear and unambiguous policy framework that seeks to balance the protection of fundamental human rights against the development of a fair and efficient digital economy[101]. Privacy, in

[98] *Sherman v. Brandt Industries USA LTD*, (2022) No**.** 1:20-cv-01185-MMM-JEH (C.D. Ill. July. 26, 2022) (EFC No. 85, Final Approval of Settlement).
[99] *Cothron v. White Castle Sys., Inc*., (2021) No. 20-3202, 2021 WL 5998537, at *1 (7th Cir. Dec. 20, 2021)
[100] *Dittman v. UPMC,* (2018)No. 43 WAP 2017, 2018 WL 6072199, --- A.3d. ---- (Pa. Nov. 21, 2018)
[101] Sandra Seubert, Carlos Becker (2020) 'The Democratic Impact of Strengthening European Fundamental Rights in the Digital Age: The Example of Privacy Protection' German Law Journal 22(1)pp. 31 – 44 https://doi.org/10.1017/glj.2020.101

contrast, is less fiercely protected in the United States, due to the historical subordination of privacy to general principles of freedom of expression[102]. Despite the historical caution of the United States towards the recognition of privacy rights, both legal systems do unite in their policy agenda to regulate these novel technologies, particularly in the surveillance context, and the recognition of the new types of digital harms that can be generated through the use[103].

5.1. Applicability to Data Discovery and Generation

This concerns the applicability of current legal frameworks to the unique species of data that can be discovered and generated by AI-powered surveillance, which often includes data describing the emotions, physical whereabouts or activity, as well as the biological disposition and overall health of workers. Protecting privacy interests in these situations requires the law to look beyond the species of data that is gathered from the AI-powered surveillance system and distinguish this to the data that is produced through the inferences and predictions of its various constitutive algorithmic and automated processes. In other words, data that is neither intrinsically private nor personal at the time of collection, can gradually acquire such characteristics. Both legal systems struggle to recognize the changing realities of workplace data in this regard and often operate under the presumption that data sourced from the workplace must be work-related, unless such can be proven otherwise, as can be achieved with certain species of personal data. Both European and American law alike must go further and actively consider the multifaceted nature of data, as well as appreciate the fact that data, which may appear at first to be entirely workplace related, can prove to provide employers with

[102] Gail Lasprogata and Nancy J King, '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' (2004) 4 Stanford Technology Law Review; *see also for introduction to privacy rights in American law* Samuel Warren, Louis Brandeis 'The Right to Privacy' (1980) 4(5) *Harvard Law Review.* IV (5): 193–220

[103] OECD Social, Employment and Migration Working Papers No. 273 https://www.sipotra.it/wp-content/uploads/2022/07/Using-Artificial-Intelligence-in-the-workplace-What-are-the-main-ethical-risks.pdf

significant insight into non-work related aspects of their workforce. The law must also look at the issue holistically and consider the whole life cycle of data that is collected by AI-powered surveillance in order to ensure that any privacy intrusion resulting from such technologies are kept to their minimum possible. European law does recognize this issue by virtue of its proportionality and necessity assessment under Article 8(2) of the ECHR and its data minimization principle in the GDPR. In the United States, similar can be seen in the establishment of the mosaic theory in the fourth amendment challenge in *United States v. Jones.* Such encourages courts to look at the entire factual matrix of the data collection process and evaluate whether the totality of the exercise exceeds a tolerable legal threshold[104]. Both legal tools provide the courts with promising instruments to regulate the collection and accumulation of data in complex surveillance systems and should be used as much as possible in the AI-powered surveillance context. It is particularly noteworthy that both approaches do not prescribe rigid legal rules that define AI-powered surveillance as legal or illegal by nature but rather provide courts with the discretion to closely scrutinize the technology in question and make a factual determination of whether the technology, together with its specific uses, and impact on the affected humans, should be permissible, or not, on a case by case basis.

5.2. Applicability to Data Exchange and Processing

Related issues stem from the applicability of the law to the continuous, constant and instantaneous nature of data collection, which often additionally involves exchanges of data within, and between, AI-powered surveillance systems, particularly in context of those that are constituted through open rather than closed data structures. Within this context, both legal systems struggle to respond to the heightened risks to privacy rights. European privacy rights, such as the right to be forgotten under Article 17 of the GDPR, are unable to remedy the harms

[104] *United States v. Jones* supra 65

arising from the fact that data once imparted, may not all be permanently exhaustively erased where it has already been exchanged and shared with different systems. Erasing data from a single system will therefore not provide workers with a right to be forgotten where the law is unable to fully capture the proliferation of data that is exchanged between the different constitutive systems of AI-powered surveillance. For instance, erasing data from the AI-powered surveillance system will have little, or no, utility where the data has already been used by the algorithm to reach an automated decision on the worker's performance. Even if a worker would be able to ask for their data, or alternatively a certain class of their data, such as data collected outside of working hours, to be eliminated from the entire algorithmic process, such would in turn adversely affect the remaining data set. In context of workforce performance analytics, the erasure of one worker's personal data risks introducing issues of bias and discrimination for all other workers who are assessed by the same technology. Other sources of privacy law and data protection rights, such as the right not to be subject to a decision based solely on automated processing in Article 22 are likewise unlikely to resolve this issue due to their narrow scope of application and at most can provide workers with an assurance of basic human oversight. Despite this regulatory gap, European law does achieve more than the statutory legal protections of the United States. These laws currently provide a patchwork of different prohibitions on particular uses of AI technologies in the employment context and vary between the different states. Although various states do recognize certain rights to abstain from AI-powered surveillance or automated decision-making in certain instances, these are not absolute rights and always conditional upon the employer being able to request workers to consent. These laws also do not recognize any substantive equivalent to the right to be forgotten, either in statute, common law or in the constitution, that can be compared to either the conceptual or practical operation of Article 17 of the GDPR. This right is, although not perfect, an important part of regulating against unduly intrusive data surveillance and in enhancing the data autonomy of those who are subject to these practices.

5.3. Applicability to Data Usage and Decision-Making

Lastly, the law must also protect and promote the proper uses of data collected, and processed by AI-powered surveillance. In European law, this is where the transparency requirements of the GDPR are of significance, as well as the need for employers to generally demonstrate a 'legitimate objective' under Article 8(2) of the ECHR. Both these legal devices stabilize the power dynamics between the workforce and the employer in the use of AI-powered surveillance. They also help prevent algorithmic opaqueness and guard against unconscious bias in data processing. In the United States, similar does exist for public sector workers in the Fourth Amendment and the tort of intrusion upon seclusion, which are useful in safeguarding against strictly unreasonable or unjustified interferences with privacy, and therefore may capture situations where data is abstracted by AI-powered surveillance for improper purposes. The same is true for the ECPA. However, it remains unclear where both legal systems will draw the line between proper and improper uses of data collected by AI-powered surveillance. Whether biometric data collected from wearable sensors such as smart watches, that is then used to monitor an employee's heartbeat to evaluate workplace activity, would amount to an improper use is, for instance, still somewhat of a moot issue. Particularly in the United States, such may deemed to pursue a reasonable or commercially justifiable objective where such can be linked to potential productivity reasons, such as monitoring activity levels, time-off requests or other leave of absence requests. This will require both legal systems to consciously consider where they chose to draw the line between permissible privacy invasions that are justified measures of productivity, and impermissible privacy invasions that are interferences of basic human rights in the workplace. Such for instance, may be achieved through the enactment of targeted legislative solution, such as through the new Artificial Intelligence Bill of Rights in America and the forthcoming EU Artificial Intelligence Act[105], which will hopefully increase awareness of the particular legal nuances that exist with AI-powered technologies and help inform and shape the future reaction of the legal system to the risks they pose for human rights and freedoms, within and beyond the workplace.

6. Conclusion

AI-powered surveillance is more aptly described as an everyday occurrence in the modern workplace rather than as a futuristic innovation. With the vast proliferation of these sophisticated surveillance technologies arises the emergence of a series of new, unforeseen and unprecedented challenges for the law. These challenges affect the entire life cycle of data that is collated by AI-powered workplace surveillance and generate long-lasting consequences for the workforce, often extending to issues beyond the immediate sphere of employment. The law is therefore confronted with both data-centric issues that challenge its ability to safeguard the integrity of employee data as a core issue of privacy, as well as more general issues of fair and equal treatment, transparency and accountability, as well as issues concerning the assurance of social equity in the workplace context.

European law and the law of the United States approach these challenges from very different starting points. European law balances the protection of privacy through the symbiotic operation of a general human rights framework and a more specific and technologically orientated data protection framework. In contrast, the existing baseline of privacy protections is not as entrenched in the United States due to the different ideological starting point of its

[105] European Commission 'Proposal for a Regulation of Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' (2021) COM (2021) 206 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

corpus of privacy laws and the more difficult balance they face with the legal emphasis on freedom of expression. However, there has been a significant surge of piecemeal state legislative activity, which involves various targeted regulatory responses that are consolidating a growing baseline of privacy expectations against technological invasion. These legislative initiatives do conceptually recognize and respond to the specific challenges of AI-powered surveillance, but are practically limited through their territorial jurisdiction.

Despite the different starting points of the relevant laws in Europe and the United States, it therefore becomes apparent that both legal systems feature a gradual convergence in their responses against the growing challenges of AI-powered technologies, both as systems of surveillance, and as novel innovations more generally. This confirms the importance of regulating against digital harms and protecting humans against the potential perils of such powerful and novel technological innovations. Even with their growing technological competences, both systems are challenged by the important nuances that arise from the specific context of AI-powered surveillance and the the unique ways in which these technologies collate, process and compute data. It is precisely in this context that the law must go further in recognizing and responding to the challenges raised by AI-powered workplace surveillance.

.