HUNGARIAN LABOUR LAW
E - J O U R N A L

The fragmented protection of privacy and data in labour law

David Mangan*

Abstract

The premise of this article is: act now regarding privacy law in general, and in particular its application to labour, or be complicit in its slow degradation. The indications of activity, such as legislation and case law, do not support the argument that privacy is being addressed. Satisfaction has grown with a simple easily surpassed threshold of notice. There must be a good, supported reason for intruding upon an individual's privacy. The ambition of this contribution is to identify the fragmented treatment of privacy, and then to offer points for recalibrating privacy at work.

Keywords: privacy at work, privacy protection, data protection

1. Introduction

We have a crisis. We are speaking vaguely about topics that themselves are complicated and layered. The 21st century has given us language without meaning. What is the digitalisation of work? What is personal data? (Or more precisely, perhaps, what is not included in the GDPR's definition of personal data?) What does artificial intelligence do when it comes to work? What is a co-bot? And then there is the focus of the present discussion: what is workplace privacy?[1]

* Maynooth University (Ireland); Osgoode Hall Law School (Professional Development) (Canada); (at the time of presentation) Global Professor KU Leuven Faculty of Law & Criminology (Belgium).
I wish to thank Tamás Gyulavári for his invitation to the conference "Decent Work in the Digital Age" at Pázmány Péter Catholic University, and to the Friedrich Ebert Stiftung Budapest Bureau for funding the keynote presentation upon which this article is based.

1 Where even the concept of the 'workplace' is debateable given the extent to which there is remote working, and the rise of digital nomads. For discussion of the latter see Stan Bruurs: Digital Nomads and the Rome I Regulation: An Overview. *Global Workplace Law & Policy,* 14 December 2022. https://tinyurl.com/w3vu3sw3

Regarding the last question, there is blame to go around for the absence of clarity in our discussions. We can blame the European Union to some extent. The EU Charter of Fundamental Rights (CFREU)[2] protects a right to privacy which is broad, as well as a right to data protection which seems more particularised. How do these two rights intersect? We can also blame courts. The European Court of Human Rights told us that workplace privacy cannot be reduced to zero. The phrase carries a weight that sounds profound. But, consider how it may be practically applied to a workforce. Mostly, however, we must blame ourselves. We have been thinking about privacy since the 19th century (at least).

Security of privacy and data have not been at the top of the plan. The International Labour Organization's Decent Work Agenda contains four pillars: employment creation, social protection, rights at work, and social dialogue. These have been embedded within Goal 8 of the United Nations 2030 Agenda for Sustainable Development (Promote sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all).[3] Security of privacy and data (that is, the capacity to monitor workers as well as to collect, analyse, and use data about them) is a sub-topic in this discussion. It may be said that this topic would fall within the breadth of the social protection and/or rights at work pillars. An examination of Goal 8, however, reveals that its essence touches lightly upon the challenges posed by technology (save for consideration of upskilling of digital literacy which is a significant issue for the European Union[4]). Instead, there is apt and legitimate focus on sustainability of work, including the potential for jobs to support workers and their families, with the ambition of eliminating poverty. Nevertheless, this focus subscribes to the idea that we can only attend to a few items at any one time. Of these priorities, continuing the line of thought, we should address the most critical first. And so, security of worker privacy and data emerges as an issue that does not critically affect the same range of people as the concern for decent work. The omission, though, is an emblem of the attention given towards the influence of technology on work. By omitting these technological issues from this important discussion, engagement with these matters has been relegated to a later time. As will be argued in this article, issues surrounding privacy have been left for far too long. The present must be the moment for taking the fledgling steps towards setting out a general framework for addressing these matters.

In the first section below, the example of privacy in Canada is used to show how even in this century there has only been a willingness to deal with privacy in a particularised manner, but not in a more generalised way that would facilitate an overarching agenda for privacy in law. The Canadian decision of *Jones v Tsige*[5] illustrates this point well. The court recognised a new tort of intrusion upon seclusion. The treatment of this decision by later courts exhibits the kind of hesitation which

2 *Charter of Fundamental Rights of the European Union,* 2012/C 326/02.

3 https://sdgs.un.org/2030agenda

4 See the DIGITAL Europe program which aims to augment the digital skills of the existing workforce: https://digital-strategy.ec.europa.eu/en/activities/skills-digital-programme

5 2012 ONCA 32. (Foreinafter: *Jones*)

has marked the discussion of privacy in the common law system. This example demonstrates that the disinclination to engage more widely with privacy (than just particularised instances) affects other jurisdictions, and other legal disciplines. It also illustrates how both the courts and legislatures seem to be waiting for each other to take the first step along the lines of an all-encompassing approach to privacy.

In the second section, labour law's engagement with privacy and data protection is discussed. The intersection of privacy and data protection with labour law is a classic example of the fragmented engagement with the area. European Union law creates some level of confusion in addition to facilitating the disparities inherent to the law within this area across the EU. The final section proposes some considerations in devising a generalised framework for privacy and data security within the labour setting.

2. The lethargic recognition of a right to privacy

Samuel Warren and Louis Brandeis' often-quoted 1890 article offered the retrospectively optimistic prognostication that the development of privacy was "inevitable".[6] Some instruction must be taken from the long-established arguments surrounding privacy in private law and the recognition of only particularised instances of privacy protection. What has been the reason for the delay with the law moving beyond this article? We have specific laws that have developed. But, we have long been lacking an organising set of principles that guide our approach to a wider concept in law of privacy.

Canada will be used as an example of this legthargy.[7] In Canadian common law, privacy has been protected incidentally. Along the way, the Supreme Court of Canada has made some distinctions.[8] A few provinces have passed statutes that offer some level of protection in certain instances.[9] Although precedent-setting, *Jones* continued the pattern of protecting privacy in discrete instances. To the legal issue "[d]oes Ontario law recognize a right to bring a civil action for damages for the invasion of personal privacy?"[10], the Court responded with a deliberate, incremental step: "it is appropriate for this court to confirm the existence of a right of action for intrusion upon seclusion."[11] *Jones* confirmed the existence of a right of action for intrusion upon seclusion,[12] with Sharpe JA adopting the definition

6 S. D. Warren – L. D. Brandeis: The Right to Privacy. *Harvard Law Journal,* Vol. 4, No. 5. (1890) 195.

7 It may be argued that what is called lethargy here, another would classify as deliberative. The response to that assessment is that we should be coming to the close of deliberations sometime soon so that we may effect a path.

8 *R* v. *Dyment,* [1988] 2 SCR 417 being one example.

9 See for example, Privacy Act*,* R.S.B.C. 1996 c.373, s 1(1); Privacy Act, C.C.S.M. c.P125, s 2; Privacy Act, R.S.N.L. 1990, c.P-22, s 3; Privacy Act, R.S.S. 1978, c.P-24, s 2.

10 *Jones* op. cit. [1].

11 *Jones* op. cit. [65].

12 Ibid.

found in the American Law Institute's *Restatement*: "One who intentionally intrudes, physically or otherwise, upon the seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the invasion would be highly offensive to a reasonable person."[13] The key features of this tort are: "the defendant's conduct must be intentional" [including being reckless];[14] the defendant "invaded, without lawful justification, the plaintiff's private affairs or concerns"; "a reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish".[15] The plaintiff is not required to demonstrate "proof of harm to a recognized economic interest". Damages would be "measured by a modest conventional sum" because of the "intangible nature of the interest protected".[16] Claims for intrusion upon seclusion were limited to situations of "deliberate and significant invasions of personal privacy."[17] Sharpe JA added a further limiting description to the tort by identifying examples of these significant invasions: "such as one's financial or health records, sexual practices and orientation, employment, diary or private correspondence that, viewed objectively on the reasonable person standard, can be described as highly offensive.[18] The court classified these intrusions as "highly offensive" without much discussion. It may be argued that accessing a financial database (as in *Jones*) to view the aforementioned information constitutes highly offensive conduct. Accessing of personal health records was found to constitute the subject matter for a claim in intrusion upon seclusion, as discussed in *Hopkins v Kay.*[19] However, the absence of further treatment of this list remains unfortunate. With online profile platforms such as LinkedIn, employment history may be of more debatable inclusion in this list. Presumably, the list was not exhaustive given the careful discussion of the court's "incremental step"; to avoid an "unmanageable legal proposition [that could] breed confusion and uncertainty".[20] A further point for consideration is Sharpe JA's identification of "competing claims", namely freedom of expression and freedom of the press.[21] Perhaps fortuitously, a competing freedom of expression claim was not an issue in *Jones.*

The Ontario Court of Appeal's 2012 decision in *Jones* has increased the number of claims regarding a compensable right of privacy.[22] And yet, anticipation of further development since then has been

13 Ibid. [19].

14 The Ontario Court of Appeal, in *Demme v. Healthcare Insurance Reciprocal of Canada*, 2022 ONCA 503, discussed recklessness as being very close to intentional conduct. The extent to which reckless conduct may fall within this tort remains to be canvassed.

15 Ibid. [71].

16 Ibid.

17 Ibid. [72].

18 Ibid.

19 *Hopkins v. Kay* 2015 ONCA 112. This decision was also authored by Sharpe J.A.

20 *Jones* op. cit. [21] and reiterated in R. J. Sharpe: *Good Judgment: Making Judicial Decisions.* Toronto, University of Toronto Press, 2018. 197.

21 On the collection of private information for journalistic purposes where intrusion upon seclusion may be claimed see the obiter in *Chandra v CBC* 2015 ONSC 5305, [59].

22 See the discussion of cases in D. Mangan: "Jones v Tsige". In: P. Wragg – P. Coe (eds.): *Landmark Cases in Privacy Law.* Oxford, Hart, 2023.

equivocal, some endorsement[23] and some reticence.[24] It may be that *Jones*' restrained impact is attributable, in part, to the absence of a clear notion of privacy protection at common law. The opinion remains that a general right of privacy should not be set out,[25] and that in Canada there is no common law tort of breach of privacy.[26] *Jones* does not venture beyond the specific facts in that case. Instead, it continues the purpose-driven approach to privacy: "Conceptualizing privacy is about understanding and attempting to solve certain problems."[27] Technological innovations, though, suggest the need for a more thorough outline of how the law may protect privacy. There must be engagement in law with an overarching idea of privacy, coupled with an elaboration on what is being protected in law.[28] That we seem little further along from 1890 in determining what is meant by privacy than a "right to be let alone" should be a source of consternation. Further factors in the limited development of *Jones* include some courts blurring any distinction by giving an impression of equivalence,[29] as well as continued reticence due to the action's relative youth.[30]

With intrusion upon seclusion being one of the few recognised privacy torts in Canadian common law, *Jones* has been relied upon by many plaintiffs. Plaintiffs, counsels continue to compel further consideration in Canadian courts by attempting to expand intrusion upon seclusion. Pleadings have included "invasion of privacy based on the tort of intrusion upon seclusion".[31]

Jones is an emblem of privacy law generally: it is a landmark decision, but not as an orthodox precedent. Although the decision has prompted much academic and judicial discussion of privacy, it has not resulted in significant and lasting development in the area. Still, there should be an appreciation for the decision's direct engagement with Canadian common law's tentativeness with privacy. *Jones* is the "incremental step"[32] the Court of Appeal intended it to be.

---

23 Such as the Federal Court of Appeal interpreting *Jones* as opening the door to a common law actionable tort in privacy: *Canada v. John Doe* 2016 FCA 191.

24 See *Owsianik v. Equifax Canada Co.* 2021 ONSC 4112.

25 One example is *Wainwright v Home Office* [2003] UKHL 53.

26 *Pinder v. Canada (Minister of the Environment)* 2015 FC 1376, [107], aff'd on other grounds, 2016 FCA 317; *Al-Ghamdi v. Alberta* 2017 ABQB 684, [160], aff'd 2020 ABCA 81. The Federal Court in *Pinder* specifically noted there is no common law tort aside from that set out by provincial statutes.

27 D. Solove: Conceptualizing Privacy. *California Law Review,* Vol. 90. (2002) 1078, 1129.

28 D. Mangan: Situating Canadian defamation and privacy law in comparative context. In: A. Koltay – P. Wragg (eds.): *Research Handbook on Comparative Privacy and Defamation Law.* Cheltenham, Edward Elgar, 2020. 379.

29 "In *Jones* the Court made an award based on the tort of invasion of privacy, or intrusion upon seclusion": *Marson v. Nova Scotia* 2017 NSCA 17, [27]. See also *Patel v Steth* 2016 ONSC 6964, [104] where a husband surreptitiously set up a camera to record his wife in the bedroom and bathroom. Claims involving the recording of individuals in intimate settings are likely to increase according to the authors of one leading Canadian tort casebook: R. Solomon – M. McInnes – E. Chamberlain – S. Pitel: *Cases and Materials on the Law of Torts.* Toronto, Carswell, 2019. 115.

30 "The tort of intrusion upon seclusion was defined authoritatively only nine years ago": *Owsianik v Equifax Canada Co.* 2021 ONSC 4112, [54].

31 See, e.g. *Del Giudice v. Thompson* 2020 ONSC 2676. The intrusion upon seclusion claim was dismissed in *Del Giudice v. Thompson* 2021 ONSC 5379, [137], based upon the binding authority of the Divisional Court in *Owsianik v. Equifax Canada Co.* 2021 ONSC 4112.

32 *Jones* op. cit. [65].

3. The fragmented protection of privacy and data

Fragmentation has emerged as a concern within the EU framework for data protection. The CJEU's decision in *Meta Platforms Ireland*[33] illustrates fragmented enforcement. The case arose due to the ambiguity surrounding Article 80(2) of the General Data Protection Regulation,[34] specifically whether it precluded national legislation from allowing consumer protection associations to bring legal proceedings for alleged infringement of personal data protection law. The Court determined that a consumer protection association may launch a claim against Meta Platforms Ireland for alleged violation of data protection rules which additionally (arguably) violated consumer protection rules.[35] For the Court, this interpretation "ensur[es] effective protection" of rights.[36] This effective protection, though, comes in the form of an additional path for GDPR enforcement. *Meta Platforms Ireland* also facilitates, what AG de la Tour calls, "the risk of a new fragmentation of the arrangements for the protection of personal data within the European Union".[37] This risk is even more evident in the labour setting where Art.88 provides for Member States to legislate in this area. As can be seen from discussions of other Member States regarding privacy at work,[38] there is a notable lack of harmony across EU countries.

Fragmentation within the EU framework for security of privacy and data is accompanied by a confusing framework. EU law has set out rights to privacy and data protection. Article 16(1) of the Treaty on the Functioning of the European Union (TFEU)[39] provides for a right for "everyone" to the protection of personal data "concerning them". Privacy and data protection are difficult to separate. Take for example the EU Charter of Fundamental Rights (CFREU).[40] Case law from the CJEU often combines the more general right to privacy (Article 7) with the specific right to data protection (Article 8). These Articles, furthermore, are derived from Article 8 European Convention on Human Rights (ECHR)[41] which confers a general right of privacy on individuals. Article 52(3) CFREU requires that "the meaning and scope" of Article 7 CFREU "shall be the same" as that set out in Article 8 ECHR.[42]

---

33 C-319/20, ECLI:EU:C:2022:322. (Foreinafter: *Meta Platforms Ireland*)

34 Regulation (EU) 2016/679.

35 The Federal Union of Consumer Organisations and Associations, Germany, launched this action as an umbrella organisation for the 41 German consumer organisations.

36 *Meta Platforms Ireland* op. cit. [73].

37 Opinion of Advocate General Richard de la Tour of 2 December 2021, C-319/20, *Meta Platforms Ireland*, ECLI:EU:C:2021:979, [55]. AG de la Tour drew from E. Mišćenić – A-L. Hoffmann: The Role of Opening Clauses in Harmonisation of EU Law: Example of the EU's General Data Protection Regulation (GDPR). *EU and Comparative Law Issues and Challenges Series (ECLIC),* Vol. 4., No. 44. (2020) 50–51.

38 See further the outlines of privacy at work in Member States as set out in F. Hendrickx – D. Mangan – E. Gramano (eds.): *Privacy@Work.* Deventer, Wolters Kluwer, 2023.

39 *Treaty on European Union and the Treaty on the Functioning of the European Union.* 2012/C 326/01.

40 *Charter of Fundamental Rights of the European Union.* 2012/C 326/02.

41 Convention for the Protection of Human Rights and Fundamental Freedoms. *Council of Europe Treaty Series 005*, 1950.

42 There is a change in wording between the two instruments; where the ECHR referenced correspondence, the CFREU uses communications to "take account of developments in technology": *Explanations relating to the Charter of Fundamental Rights* (2007/C 303/02).

Decisions of these courts could be treated as aligned.[43] It remains unclear, though, whether there is such harmony or if there are differences in approach between the two relevant courts.[44]

Further fragmenting the framework, enforcement has also been parcelled out to employers. Articles 24(1) and (2) GDPR[45] require employers to implement data protection policies "to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation."[46] These provisions have also been viewed as imposing "accountability obligations, alongside Article 5(2) GDPR."[47] This is a shift from the Data Protection Directive because employers are now assigned responsibility for data protection, with enforcement coming in the form of the possibility of being asked to establish compliance.

Article 88 GDPR is another example of fragmentation because it permits Member States to adopt specific rules for processing of personal data in the work context. It may be that Article 88 facilitates consistency from the Data Protection Directive.[48] However, the implementation of the GDPR within the employment setting across Member States remains varied,[49] thereby ensuring the continuity of this situation.

There is also fragmentation in case law based upon technology. In *López Ribalda and Others v Spain*[50] the ECtHR objected to overt surveillance through cameras which monitored employees at work. Still, in this instance, the Grand Chamber was satisfied that the employer's decision to install the surveillance equipment constituted a "reasonable suspicion that serious misconduct has been committed and the extent of the losses identified in the present case may appear to constitute weighty justification."[51] It is wondered why there was (at best) muted concern for covert GPS (Geolocation Positioning System) monitoring of an individual twenty-four hours a day for a period of three years in *Florindo de Almeida Vasconcelos Gramaxo v Portugal*.[52] A majority of the Fourth Section of the ECtHR ruled that the employer's tracking of Florindo using both overt and covert means in a company car that tracked him 24 hours a day, seven days a week for three years was permissible. Florindo was found to have known about the existence of GPS, and that disciplinary measures could have arisen in

43 See the discussion in F. Hendrickx: Article 7 – Protection of Private and Family Life. In: F. Dorssemont – K. Lörcher – S. Clauwaert – M. Schmitt (eds.): *The Charter of Fundamental Rights of the European Union and the Employment Relation.* Oxford, Hart, 2019. 229.

44 D. Mangan: Article 7 – Respect for Private and Family Life (Private Life, Home and Communications). In: S. Peers – T. Hervey – J. Kenner – A. Ward (eds.): *The EU Charter of Fundamental Rights: A Commentary.* Oxford, Hart–Bloomsbury–Nomos, 2021.

45 Regulation (EU) 2016/679. The GDPR was listed as part of EU Law in *Nowak* C-434/16, EU:C:2017:994, [11]–[13].

46 Recital 78 GDPR adds "the controller should adapt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default."

47 C. Docksey: Article 24 Responsibility of the Controller. In C. Kuner – L. Bygrave – C. Docksey – L. Drechsler (eds.) *The EU General Data Protection Regulation (GDPR): A Commentary.* Oxford, OUP, 2020. 557.

48 P. Van Eecke – A. Šimkus: Article 88: Processing in the Context of Employment. In: Kuner–Bygrave–Docksey–Drechsler (eds.) op. cit. 1230.

49 See the chapters on implementation of the GDPR in the labour setting in Hendrickx–Mangan–Gramano (eds.) op. cit.

50 Applications nos. 1874/13 and 8567/13 (Grand Chamber, 17 October 2019).

51 Ibid. See also the factors in assessing the proportionality of video surveillance at *López Ribalda* [116].

52 *Florindo De Almeida Vasconcelos Gramaxo v. Portugal* [2022] ECHR 1073. See further the discussion in M. Mole – D. Mangan: 'Just more surveillance': The ECtHR and workplace monitoring. *European Labour Law Journal*, Vol. 14, Iss. 4. (2023) 694.

response to his misreporting of his work activities. And so, Florindo's right to private life had been proportionately reduced to protect the employer's interests.[53] Certainly this form of surveillance was not the least intrusive available, as the dissent noted.[54]

4. Recalibrating privacy at work

A pessimistic perspective has been laid out to this point. In this final section, several factors are listed as important considerations in developing a framework for privacy at work that better addresses contemporary issues. Primary amongst these is setting out a general framework that facilitates substantive rights to privacy within the work context that exceed the procedural entitlement of notice.

Labour law tends to be swept away with 'new' issues. Frank Hendrickx has reminded that "it should be clear that the right to privacy has a much more broad scope than these "new" issues related to AI and data protection."[55] Adding to this point, there must be recognition that the concept of privacy has not been adequately mapped out. We are mired as we deal with privacy because the pace of developments in information technology continues far more rapidly. This is not to overlook that it is "likely that AI will create new case law in relation to various privacy and data protection principles."[56] Harmonisation in the context of privacy and data protection at work does not necessarily mean that there must be homogeneity. But, the current disparities across the EU must also be recognised as a matter of some urgency.[57]

4.1. Clarity about the applicability of laws

A key facet to developing a substantive law of privacy at work in the EU is to clarify the applicable laws. Adjudication relating to Articles 7 and 8 of the Charter of Fundamental Rights demonstrates this point. What is the difference between the two? If privacy is a collective term (set out in the broadly worded Article 7), does data protection (Article 8) fall under the collective term of privacy? Moreover, what is protected within these articles? Koen Lenaerts wrote of the essence of a fundamental right placing an "absolute limit on the limitations that may be imposed on the exercise of that fundamental right".[58] For Lenaerts, the Safe Harbour agreement between the US and the EU regarding transatlantic

53 Ibid. [119]–[125].

54 Ibid. [81].

55 Hendrickx (2023) op. cit. 1.

56 Ibid. 17.

57 "[…] there is a specific role for worker involvement mechanisms (through workplace representatives or trade unions), through information, consultation, or even co-decision procedures, and there are some strong national practices of collective bargaining in relation to privacy and data protection." Ibid. 55.

58 K. Lenaerts: Limits on Limitations: The Essence of Fundamental Rights in the EU. *German Law Journal,* Vol. 20. (2019) 779–793.

data transfers which was litigated in the first *Schrems* decision[59] "emptie[d] those rights of their content [and] call[ed] their very existence into question because, in terms of respect for private life, there was simply no privacy as [US] authorities could have unlimited access to the content of all the personal data transferred from the EU to the US." Lenaerts defined the essence as "a 'hard nucleus' that guarantees to each and every individual a sphere of liberty that must always remain free from interference. That nucleus is, in my view, absolute in so far as it may not be subject to limitations." In the second *Schrems* decision[60], though, the discussion of the essence of the Article 7 right seemed to shift to the right to redress in Article 47.[61] Further complicating the issue of applicable laws, in the employer setting, several instruments arguably apply. These include not only the General Data Protection Regulation, but also the EU Directive 2019/1152 on Transparent Working Conditions, as well as the proposed AI Act, and the proposed Platform Work Directive.

The above paragraph is not intended to be an exhaustive exploration of the absence of clarity when it comes to privacy and data protection law. Nonetheless, it suffices to ground follow-up questions such as how can lawyers advise clients (whether they are employers or workers), if the applicable law is itself a matter of confusion? If one was to advise an employer who seeks to be compliant, how does a lawyer go about properly informing that client? At least at a surface level, there appears to be a tremendous amount of regulation that seemingly overlaps. On top of these questions, we have those related to the operations of businesses, such as how can data be secured effectively, in an understandable manner, and still not unnecessarily impede day-to-day commercial operations?

4.2. The venue for adjudication

Another aspect of fragmentation is the venue for complaints alleging violation of workplace data protection. In Ireland, there is a question as to whether labour adjudicators have the competence to hear these matters, instead of sending them to the Data Protection Commissioner. In *Go Ahead Transport Services (Dublin) Ltd v Gifford*,[62] the Labour Court dismissed the complainant's argument about a violation of data protection rights because it was "outside the competence of this Court. Any alleged breaches of the Complainant's rights in this regard are a matter for a different forum."

---

59 Case C-362/14 *Maximillian Schrems v. Data Protection Commissioner* (CJEU, Judgment 6 October 2015).

60 Case C-311/18 *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems,* CJEU, Judgment 16 July 2020.

61 There is also the prospect of a challenge to the European Union-U.S. Data Privacy Framework (EU-U.S. DPF) This agreement is the successor to the Privacy Shield Agreement struck down by the CJEU in 202. US President Biden signed an Executive Order in October 2022 to implement US commitments under the DPF. See: *Fact Sheet: President Biden Signs Executive Order to Implement the European Union – U.S. Data Privacy Framework.* The White House, 7 October 2022. https://tinyurl.com/ehu6e2k3 Max Schrems has raised the possibility that he will challenge this new agreement: Chloe Kim: Privacy activists slam EU-US pact on data sharing. *BBC News,* 11 July 2023. https://www.bbc.com/news/world-us-canada-66161135

62 *Go Ahead Transport Services (Dublin) Ltd v Gifford* UDD2225 (24 March 2022).

This decision has been debated in Ireland. *Go Ahead Transport* has been characterised as an exceptional circumstance where further processing was permissible because it was "not considered to be disproportionate, and the employer has stringent procedures in place to limit abuse".[63] The decision could be confined to its facts insofar as the complainant was dismissed pursuant to a strict rule about safe driving of a bus where use of mobile phones while doing so was enforced. Still, the ruling suggests a lack of competence by labour adjudicators to apply data protection law to the employment setting. If this treatment of data protection issues at work remains, it poses further difficulties for the development of the area in Ireland. This would be an unfortunate situation, particularly considering the jurisdiction's role in data protection within the EU.

The fact of the Labour Court's diversion of these matters to the Data Protection Commission does not in itself raise a question. Other countries, such as Italy, have a similar separation. The Data Protection Act 2018 (which enacted the GDPR into Irish law) empowers the Data Protection Commission to, amongst other functions, "monitor the lawfulness of processing of personal data".[64] As such, the Commission would seem to be the venue to bring a data protection action against an employer who acts as the controller and/or processor of a worker's personal data.[65]

The diversion of data cases away from labour courts should prompt a question which recalls why employment tribunals (or similar such entities) were initially established. They were to be a less costly venue where experts in industrial relations could deliberate on work matters.[66] Do workers and employers lose that expertise when a data issue is shuttled to a data protection commission, instead of an industrial relations panel? DPAs offer guidance on the application of privacy and data protection rules in the employment context.[67] But, is there a uniform approach to this which integrates the data and work discussions?

The workplace is well-known to be a setting that incorporates different areas of law. The CJEU in 2018 ruled that the Workplace Relations Commission is a statutory body established for the purpose of adjudicating employment-related disputes in Ireland.[68] As such, it has the authority to disapply a rule of national law that is contrary to EU law where it is necessary to give full effect to EU law. In the 2022 *Go Ahead Transport* decision, the Labour Court shifted data-related employment disputes to the Data Protection Commission based on the latter's competence.

---

63 N. Cox – V. Corbett – M. Connaughton: *Employment Law in Ireland.* Dublin, Clarus Press, ²2022. [14–87].

64 Data Protection Act 2018, s.12. This is also the guidance derived from F. Meenan: *Employment Law.* Dublin, Round Hall, ²2023. Chapter 4 J.

65 Data Protection Act 2018, s.117.

66 See the discussion in *McGowan & Ors v Labour Court & Ors,* [2010] IEHC 501, though this was a decision that predated the establishment of the Workplace Relations Commission (through the Workplace Relations Act 2015). The Workplace Relations Commission has come under scrutiny, particularly through the Irish Supreme Court's decision in *Zalewski v WRC & Ors* [2021] IESC 24, and the resulting legislative changes set out in the Workplace Relations (Miscellaneous Provisions) Act, 2021.

67 Hendrickx (2023) op. cit. 54.

68 C-378/17 *Minister for Justice and Equality, Commissioner of An Garda Síochána v. Workplace Relations Commission and Ronan Boyle & Others* ECLI:EU:C:2018:979.

4.3. Reasonable expectation of privacy: a living concept

Hendrickx questions the reliance (perhaps dependence?) upon the concept of the reasonable expectations of privacy based upon technologies creating a greater sense of openness and transparency, particularly through monitoring technologies.[69] The relativity of the reasonable expectation should be easily identified as worrisome.

The reasonable expectation concept extends beyond differences between the EU and other jurisdictions.

It may be asserted that the reasonable expectation of privacy is an area of divergence between an American and a European approach to technologies. Many of the technologies in question are developed in the US where there is not as robust a discussion regarding privacy, let alone data protection. The *Schrems* litigation testifies to these differences. And yet, the reasonable expectation of privacy, as set out in the EU, and as it pertains to the work setting has a slight threshold that can be easily achieved by notifying employees. This threshold must be viewed as minimal because it exchanges notice for a basis to intrude upon worker privacy.[70] The reasonable expectation of privacy needs to be recalibrated so that it becomes a living concept, and not simply a snapshot of privacy at a moment in time (a moment which can easily pass). With the current law, we are creating new expectations (or the absence of them) regarding privacy. A concern voiced here is that the current snapshot in time approach sets a trajectory for the diminishing of privacy, let alone any reasonable expectation thereof.

The European Court of Human Rights in *Bărbulescu v. Romania*[71] provides a statement of sound and fury signifying nothing.[72] In this decision, the Grand Chamber wrote: "an employer's instructions cannot reduce private social life in the workplace to zero."[73] This sounds profound! But, what does it mean, when we look at its application to labour? Somewhere in between the reasonable expectation of privacy and a prohibition on employers reducing workplace privacy to zero we have a hint of a right to privacy at work. Employers cannot contract out of workplace privacy. They can tell workers about monitoring, and this suffices in fulfilling employers' obligations. Is this the extent of the right to privacy at work? *Bărbulescu* subscribes to the idea that informing individuals allows them to make informed decisions. What is overlooked, however, is the relationship of subordination. A choice to leave an employer once informed is as workable as a prohibition on reducing workplace privacy to

---

69 F. Hendrickx: From Digits to Robots: The Privacy-Autonomy Nexus in New Labor Law Machinery. *Comparative Labor Law & Policy Journal,* Vol. 40. (2019) 380.

70 D. Mangan: Beyond Procedural Protection: Information Technology, Privacy, and the Workplace. *European Law Review,* Vol. 44. (2019) 559.

71 ECtHR, Judgment 5 September 2017. (Foreinafter: *Bărbulescu*)

72 While the famous line from William Shakespeare's *Macbeth* is referenced here, there is no suggestion the ECtHR is an "idiot" as the earlier part of this passage from the play states.

73 *Bărbulescu* op. cit. [80].

zero. Subordination is not simply about information. It is a situation in which workers' options are reduced to choices that may offer little choice at all.

5. Conclusion

This article argues that we must act now regarding privacy at work, or be complicit in its slow degradation. Satisfaction seems to be found with a simple easily surpassed threshold of notice. It is contended here that there must be a good supported reason for intruding upon an individual's privacy. The ambition of this contribution has been to take some careful steps towards that goal.