

https://dspace.org/

Remote work and employee privacy in South Africa law

Sibanyoni, Aaron Bonginkosi

2024
University of the Witwatersrand, Johannesburg
https://hdl.handle.net/10539/45076
Sibanyoni, Aaron Bonginkosi . (2024). Remote work and employee privacy in South Africa law [Masters dissertation, University of the Witwatersrand, Johannesburg]. WIReDSpace.

Downloaded from a DSpace repository. https://dspace.org/

REMOTE WORK AND EMPLOYEE PRIVACY IN SOUTH AFRICAN LAW

By

1022725

Submitted in partial fulfilment of the requirements for the degree of Master of Laws by Coursework and Research Report at the University of the Witwatersrand, Johannesburg

Date: 30 0ctober 2023

DECLARATION

I, **1022725**, declare that this research report is my own unaided work. It is submitted in partial fulfilment of the requirements for the degree of Master of Laws (by Coursework and Research Report) at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

I have submitted my final research report through Turnitin and have attached the report to my submission.

Word Count: 10489 [Incl. the body of your report, footnotes BUT excl. title page, declaration, abstract, table of contents and bibliography]

ABSTRACT

In South Africa, the right to privacy is guaranteed in the Constitution, and is given effect by the Protection of Personal Information Act (POPIA) and protected by other pieces of legislation. This research looks at remote work and employee privacy under South African law. The right to privacy, which is a human right that employees must also enjoy. However, the right to privacy impacts the employer's right to manage the business enterprise in a remote working setting. Therefore, the research explores the concept of control and subordination, which are central to the employment relationship. The employee is subordinate to the employer; otherwise, there would not be a contract of employment. These characteristics of control and subordination are drastically diminished by the employee's right to privacy and consequently impact negatively on the employer's entrepreneurial control. Employers should take note that it is not the "activities" of the employee that matter but the "purpose" of monitoring, which must be balanced with the rights and interests of both parties in the employment relationship.[1] South African law does not adequately deal with the issue of employee privacy in the context of remote work. South Africa can draw lessons from jurisdictions where this aspect of the law has been significantly developed. These jurisdictions include EU countries such as Germany, France and the UK. In the US, protection of privacy is based on liberty which requires a person to prove the expectation of privacy to enjoy the protection and therefore individualistic in nature, while in the EU it is based on dignity as a fundamental right which gives the power of individuals to control information about themselves and therefore communal.[2] The research explores these two analytical approaches and argues that the South African Constitution elevates human dignity and has been confirmed by the Constitutional Court in *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services (Media Monitoring Africa Trust) and a related matter* 2021 (4) BCLR 349 (CC)(*Amabhungane*). Thus, it should be the yardstick as in the EU countries instead of the US culture. This research makes a proposal for South Africa to adopt legislation or a Code of Good Practice on remote work and employee privacy.

[1] Neil M. Richards, 'Why Data Privacy Law Is (Mostly) Constitutional' (2015) 56 Wm & Mary L Rev at 1507.

[2] Guy E. Carmi, 'Dignity Versus Liberty: The Two Western Cultures of Free Speech' (2008) 26 BU Int'l LJ at 300.

Keywords:

Remote work, employee privacy, control, subordination, right to human dignity, contract of employment

Table of Contents

ABSTRACT 3
Keywords: 4
1 INTRODUCTION AND BACKGROUND TO THE RESEARCH PROBLEM 6
1.1 Research question 9
1.2 Research methodology 10
2 ORIGIN AND RATIONALE OF THE RIGHT TO PRIVACY 10
3 WHAT DOES THE RIGHT TO PRIVACY ENTAIL? 12
4 THE CONCEPTS OF PERSONAL DATA AND PERSONAL INFORMATION 14
5 REMOTE WORK AND EMPLOYEE PRIVACY IN SOUTH AFRICAN LAW 15
5.1 Implication of POPIA relating to the US test of reasonable expectation of privacy applied by our courts given that it has been drafted in line with EU GDPR 19
5.2 Examples of activities that would be regarded as ‘’crossing the line’’ of control. 21
6 THE LEGAL POSITION OF THE RIGHT TO PRIVACY IN OTHER JURISDICTIONS 22
6.1 United States of America 22
6.2 Germany 26
6.3 France 29
6.4 United Kingdom 30
6.5 Has the European Union through its regulations changed the landscape of the right to privacy? 31
7 CONCLUSIONS 32
Bibliography 35

1 INTRODUCTION AND BACKGROUND TO THE RESEARCH PROBLEM

In the latter part of 2019, the virus SARS-CoV-2, which is accountable for COVID-19, was detected in Wuhan, China.[3] In the year 2020, it spread throughout the world because of its highly contagious nature.[4] It affected people's health, income, and well-being. [5] It changed the way we used to live and our behaviour.

The pandemic resulted in a hybrid work arrangement in which employees can work remotely and in the traditional workplace. Working from home, as known as remote working, was however not a new phenomenon, as it had been there even before COVID-19.[6] Remote working, particularly in the information technology communication era, may conflict with the employee's right to protection of personal information and employer's right of control of the business enterprise. The employer is not subordinate to the employee, otherwise there would not be a contract of employment if there was no element of control by the employer on how to run the business enterprise.[7]

The employment contract is the cornerstone of the employment relationship. Parties must enter into an agreement which will provide for rights and duties.[8] The employer has a greater degree of control in the employment relationship due to the subordinate status of the employee, which is inherent in the contract of employment.[9] The control element would inevitably lead to violation of the employee's privacy when the employer manages the business enterprise such as monitoring the employee's

[3]World Health Organization: https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it (Date of access 10 September 2022).
[4] United Nations: https://unstats.un.org/unsd/ccsa/documents/covid19-report-ccsa.pdf Date of access (10 September 2022).
[5] Ibid.
[6] Tammy Katsabian, 'The Telework Virus: How COVID-19 Has Affected Telework and Exposed Its Implications for Privacy' (2022) 44 Berkeley J Emp & Lab L at 148-149.
[7] Darcy du Toit The right to equality versus employer 'control' and employee 'subordination': Are some more equal than others? (2016) 37 ILJ at 7.
[8] J Grogan, *Workplace Law* (13th edn, Juta 2020) 23.
[9] Ibid (note 7) at 9.

productivity when working remotely.[10] The employer's control should, however, not trump this right.[11]

The general principles of contract law apply to employment contracts.[12] In that sense, employers would draft employment contracts which potentially would deprive employees of their right to privacy, couched in terms such as not to have the right of expectation of privacy amongst others.[13]

This research explores remote work and employee privacy in South African law. It focuses on what impact, if any, does workplace privacy laws have on employment or labour law. The research is not about camera surveillance in the workplace and personal data collected during employment. The research is about monitoring employee communication and other usage such as internet whereby an employee is expected to perform his or her duties but focuses on other activities which are not work related particularly when they work remotely and the employer's power of control and subordination which is central to the employment relationship to make sure that employees are productive.

Principles discussed in this research which emanates for example from Regulation of Interception of Communication and Provision of Communication-related Information Act 70 of 2002(RICA) cases such as *AmaBhungane* will be applicable to employee monitoring to the degree that is pertinent to the factual circumstances of the case and vice versa and to this end such authorities will be referred to. This is against the backdrop that the right to privacy is a human right and therefore cannot easily be derogated in the workplace other than under justifiable reasons.[14]

The *Amabungane* case as stated in the previous paragraph supports my argument that the right to privacy is the cornerstone of the right to human dignity, equality and freedom which form part of the founding values of the Constitution of the

[10] Ann C. Hodges, Bargaining for Privacy in the Unionized Workplace, 22 Int'l J. of Comp. Lab. L. & Indus. Rel. 147 (2006) p159 quoting a judgment in Colgate-Palmolive Co., 323 NLRB 515 (1997).
[11] Ibid (note 7) at 9.
[12] Ibid (note 8) at 24.
[13] See the discussion in other jurisdictions below.
[14] See s36 of the Constitution of the Republic of South Africa, 1996.

Republic of South Africa, 1996[15] and one of the ILO mandates to create a workplace which is conducive for the attainment of those values and human rights.[16]

The research essay will be structured as follows; background to the research which gives a comprehensive discussion on the centrality of the concept of control and subordination in the employment relationship which result in the encroachment of an employee's right to privacy when working remotely. Then it will be followed by the research questions which set the parameters of the research of remote work and employee privacy in South African law.

The research question will be followed by the methodology used to conduct this research. The right to privacy cannot be properly discussed without a detailed exposition of its origin and rationale and therefore it will be discussed after the research methodology. It is significant to dissect what the right to privacy entails and this is being catered for in the next section after the origin and the rationale of the right to privacy. There are different concepts used in legislation or guidelines relating to an individual's right to privacy such as personal data and personal information. This section explains why the South African legislature has chosen the concept of personal information rather than personal data.

Following the concepts of personal data and personal information, is the detailed exposition of remote work and employee privacy in South African law. There were few cases which reached our courts relating to this aspect of the law particularly after implementation of the POPIA. The right to privacy in South Africa is protected by other pieces of legislation such as RICA and Electronic Communications and Transactions Act 25 of 2002. The principles as articulated by the court's pieces of legislation will be referred to. A subsection on the implication of POPIA relating to the US test of reasonable expectation applied by our courts given that it has been drafted in line with EU GDPR form part of the discussion of the South African privacy law. Another subsection to this part which is titled examples of activities that would be regarded as ''crossing the line'' of control which I believe will serve as what would be an excessive encroachment by employers.

[15] See s1(a) of the Constitution of the Republic of South Africa,1996.
[16] International Labour Organisation: Homework Convention, 1996 (No. 177).

The legal position of the right to privacy in other jurisdictions will be next starting with the US which has a different culture, liberty, which requires a person to prove expectation of privacy to enjoy this right.[17] It will be followed by Germany, France and the UK. These jurisdictions are members of the EU except recently when the UK pulled out. Their culture is different from the US as they focus on dignity. Further to this is a subsection which gives an exposition of the EU as a continental body. The research will now start with the research question.

1.1 Research question

The research focuses on the following questions which are by their very nature endeavour to strike a balance between the conflicting rights or interests of the parties in the employment relationship.

- Is there a balance between the employee's right to privacy and the employer's right to productivity in the context of remote working or teleworking?
- If there is such a balance what informs the parties limitation to those rights?
- Is the employer's source of power which is central to the employment relationship such as control being diminished and thereby putting authority in the periphery?
- Is the right to privacy also applicable in the world of work?
- If the employee's right to freedom of expression does not provide him or her the right to tarnish the employer's right to good name does this axiomatically mean that the employer should also respect the employee's right to privacy?

The application of these rights is despite the fact of ownership of the device being used.

[17] Saby Ghoshray, 'Employer Surveillance versus Employee Privacy: The New Reality of Social Media and Workplace Privacy' (2013) 40 N Ky L Rev at 611.

1.2 Research methodology

The research focuses on both the primary and secondary research sources namely, legislation, case law, electronic sources, textbooks as well as journal articles. The research method will be desktop and thus be qualitative and doctrinal in nature.

2 ORIGIN AND RATIONALE OF THE RIGHT TO PRIVACY

The right to privacy is a legal concept that was first advocated by Louis Brandeis and Samuel Warren in an influential 1890 article in the Harvard Law Review.[18] The authors argued that the law must evolve to protect individuals from the invasion of their private realm by the press, the government, and other agencies and institutions, especially with the development of new technologies like photography and wiretapping. Brandeis later became a Supreme Court justice and defended the right to privacy as the foundation of individual freedom and the most comprehensive of rights in several cases, such as his famous dissent in *Olmstead v United States* (1928).[19]

Although Brandeis and Warren's article was not universally accepted at the time, it served as a catalyst for deliberations and a form of authority despite differing opinions for most courts in the US.[20] The authors argued that the right to privacy at that time protected one's reputation and did not go far enough in protecting the feelings of the person aggrieved by such actions.[21] They metaphorically referred to facts of private life as ''property'' belonging to that individual and therefore worthy of protection by law.[22]

This type of privacy has been dubbed "dignitary privacy"[23] which is part of South African law of delict and by extension common law. Privacy relating to personal information is referred to as "data privacy." This categorisation of the right to privacy is discussed further elsewhere in this research.

---

[18] Ben Bratman, 'Brandeis and Warren's the Right to Privacy and the Birth of the Right to Privacy' (2002) 69 Tenn L Rev 627 and infra (note 86) at 322.
[19] See discussion on US.
[20] Ibid (note 18) at 628.
[21] Ibid (note 18) at 630.
[22] Ibid (note18) at 631.
[23] Robert C. Post, 'Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere' (2018) 67 Duke LJ at 981.

In South Africa, the right to privacy is protected by the Constitution.[24] This right is given effect by the POPIA and other legislation. The POPIA has been drafted in line with the "fair information practices"[25] principles of the EU, with its main objective being to give data subjects control over their personal information[26] and harm should not be present in triggering resentment.[27] Although the right to dignity is not expressly stated that it is aligned with the right to privacy, it is implied because invasion of privacy can be an affront to human dignity.

The protection of personal information as personal property is justified by the fact that such information can be used for commercial gain.[28] In the workplace, prying into employees' personal lives can be an affront to human dignity and can cause psychological injury. Furthermore, prying on employees can influence their job security and future employment prospects if this information is divulged to third parties, making it potentially difficult for them to make a living.

This labelling of personal information as "property" aligns with those who refer to it as "product" in the commercial space.[29] The same principle may also hold true in the employment arena. Matthew T. Bodie argues that the collection of employee data can feel disturbing and threatening, as it gives employers an informational advantage. He believes that this practice is open to abuse and concludes that data collection must be regulated rather than left at the whim of employers.[30]

Analogizing personal information as property has led some writers to argue that it is subject to the law of contract, allowing for agreements such as employment contracts in which employees can waive their privacy rights through consent, allowing employers to monitor them.[31] This view is espoused by American culture, which

[24] Constitution of the Republic of South Africa, 1996.
[25] Ibid note 23.
[26] Ibid (note 23) at 998.
[27] Ibid (note 23) at 999.
[28] Da Veiga, A, Vorscer, R., Li, F., Clarke, N., and Furnell, S.M. (2019), "Comparing the protection and use of on-line personal information in South Africa and the United Kingdom in line with data protection requirements", Information and Computer Security, Vol. 28 No. 3, pp. 399-422.
[29] Ibid.
[30] Matthew T. Bodie, 'The Law of Employee Data: Privacy, Property, Governance' (2022) 97 Ind LJ at 723.
[31] Laura Evans, 'Monitoring Technology in the American Workplace: Would Adopting English Privacy Standards Better Balance Employee Privacy and Productivity' (2007) 95 Calif L Rev at 1139.

emphasizes concepts of liberty. The EU is based on dignity which is given to them by the community.

Other authors use different frameworks for analysis,[32] but it is beyond the scope of this research to delve further into these categorizations. However, it does provide insight into the approach adopted by different jurisdictions. Compared to the average European constitution, from the US standpoint, the right to privacy and other rights seem to offer less safeguarding for values and rights that are linked with the notion of human dignity.[33]

The encroachment of privacy can result in the accumulation of personal information, which some employers use as an algorithm to make favourable or unfavourable decisions about employees.[34] It is important to control this practice to prevent abuse, as it can have a detrimental effect on an individual's future employability. For example, if an employer obtains information about a life-threatening illness of an employee through clandestine communication with their physician, it can potentially affect their promotion prospects due to risk assessments.[35]

Technological advancements have blurred the boundaries between private and working life in terms of place and time.[36] These developments have prompted other jurisdictions, such as France and Germany, to recognise the need for comprehensive privacy regulations, a recommendation which I make in my conclusion. It is vital to recognise that no right is unrestricted.[37]

3 WHAT DOES THE RIGHT TO PRIVACY ENTAIL?

The Constitution guarantees every person has the right to privacy. The right is further given effect by the POPIA. One of the purposes of the POPIA as stated in its preamble

[32] Ibid (note 2) at 281.
[33] Ibid (note 2) at 289.
[34] Bart Custers & Helena Ursic, 'Worker Privacy in a Digitalized World under European Law' (2018) 39 Comp Lab L & Pol'y J at 325.
[35] Ibid.
[36] Ibid (note 34) at 323.
[37] Ibid (note 34) at 324.

is to harmonize South African privacy laws in line with international standards. The POPIA resembles the data protection of the European Union.[38]

It is against this background the comparative analysis of other jurisdictions will be made alongside the GDPR which give effect to Article 8 of the Charter of Fundamental Rights of the European Union hence the research will first discuss remote work and employee privacy in South African law followed by selected EU countries and the Continental perspective.

Some notable authors define the right to privacy as the 'right to be let alone'[39] and more precisely the 'primal right of man to be left alone'.[40] In the four invasions of privacy torts which is a delict in our law as recognised in American jurisprudence the relevant definition of privacy which is in line with the previous one is the 'unreasonable intrusion upon the seclusion of another'.[41]

The right to privacy is a basic human right which employees should also enjoy. In a professional setting, the entitlement to confidentiality is characterized as the entitlement of a worker to be exempt from undue interference by a manager who desires to acquire knowledge about their actions, convictions, and confidential correspondence.[42] This simply means in practice that an employer cannot encroach on an employee's privacy without justifiable reasons.

And similarly, the definition of Alan F Westin in which he reformulated what was 'the right to be let alone' as indicated earlier in line with technological development is for individuals to decide for everyone and entities to have control on their personal information.[43] Its importance to be a right to be protected has also been regarded as

[38] Jonas S Baumann and Nazreen Ismail, 'The concept of "personal information" in the Protection of Personal Information Act 4 of 2013 – a comparative analysis from a European perspective' (2021) TSAR at 718.

[39] See Rebecca Britton, 'An Employer's Right to Pry: A Study of Workplace Privacy in New Zealand' (2006) 12 Canterbury L Rev 65 quoting Warren & Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review at 196.

[40] Milica R. Kovac-Orlandic, 'Employee's Right to Privacy: Where Is the Bound of the Employer's Right to Monitor Employees' Communications' (2020) 2020 Strani Pravni Zivot 85.

[41] Ibid (note 18) at 624.

[42] Ibid (note 40) 87 quoting Guerin, L. 2011. Employment law: The Essential HR Desk Reference. Berkeley: Nolo 2011 and International Labour Organisation. Conditions of Work Digest: Workers' Privacy Part. 1993.

[43] A. Roos, 'Personal Data Protection in New Zealand: Lessons for South Africa' (2008) 11 Potchefstroom Elec LJ at 66.

a value which gives a reason why it is so difficult to define hence it has been assigned different contradictory meanings.[44] It is a right not only confined to protect an individual from the press publishing unpalatable information but rather in an information technology the gathering, revelation, and utilization of our private data by recognised and unrecognised public and business organisations.[45]

This according to my view relating to the above paragraph is the reason it will be a source of conflict between an employer and an employee in the workplace. We live in an Information Age and therefore, we cannot as human beings be divorced from that reality and by extension includes employees as well. It is apposite to state that workplace privacy in this research in the context of protection of personal information should not be the publication of offensive facts about an employee but what is at stake is prying or monitoring. The concept of personal information will be analysed in the section below and personal data, which is used by POPIA and GDPR, respectively.

4 THE CONCEPTS OF PERSONAL DATA AND PERSONAL INFORMATION

The EU uses the concept of personal data while the drafters of the POPIA opted for personal information. However, despite this the concepts do have the same legal meaning.

The definition of these two concepts is so extensive in such a way that it casts its net wider. The definition can potentially also include all information relating to a data subject. The POPIA has been drafted in line with the EU. Following from this the interpretation by the EU courts will have an influence on how our courts will interpret these concepts which are prevalent in the POPIA and form the theme of the legislative regime.

In support of the above observation the European Court of Justice in *Nowak v Data Protection Commissioner* interpreted personal data as information that is not limited to sensitive or private data, but can include all types of information, both objective and subjective, if it is related to the data subject. [46] This broad definition of the concept by the European Court of Justice and by the POPIA casts its net wider

[44] Ibid (note 1) at 1508.
[45] Ibid (note 1) at 1509.
[46] *Nowak v Data Protection Commissioner* par 34.

and can include in its ambit any information such as surfing on the internet as personal information. Further to this an internet can be an online identifier.[47] Online identifiers as per the Guide to the GDPR can be the IP address or cookies.[48]

The above is supported by the concepts ‘’including, but not limited to’’ in the definitional clause of the POPIA.[49] The concept of personal information according to my view was preferred over personal data because of its wider appeal by the South African Law Reform Commission and adopted by the legislature.[50]

An employee does not relinquish his or her right to privacy in the workplace and that includes when he or she works remotely. Having discussed these two concepts and what the right to privacy entails, what follows is the exposition of remote work and employee privacy in South African law.

5 REMOTE WORK AND EMPLOYEE PRIVACY IN SOUTH AFRICAN LAW

The common law is the foundation of the employment relationship in which control and subordination are its main characteristics as stated in the introduction. The employee is subordinate to the employer. Subordination and control in the employment relationship presupposes a concept of power which by its nature is tilted towards the employer.

The Constitution requires courts and other forums to construe any legislation and evolve the common law or customary law in a way that advances the essence, intention, and objectives of the Bill of Rights.[51] Accordingly the right to privacy must be interpreted in line with the Bill of Rights.

The following cases relating to the right to privacy were decided by CCMA and our courts. But before discussing the cases it is important to state that the paragraph below will give sources of our privacy law and followed by how we have categorized our privacy laws and the Constitutional Court view on this categorisation. In the last few paragraphs implication of POPIA relating to the US test of reasonable expectation

[47] s1 of the POPIA.
[48] Guide to the General Data Protection Regulation (GDPR) 11.
[49] Ibid.
[50] Ibid (note 38) at 729.
[51] s39(2) of the Constitution of the Republic of South Africa, 1996.

of privacy applied by our courts given that it has been drafted in line with EU GDPR is discussed followed by examples of activities in which employers can use as a litmus test whether they have ‘’crossed the line’’ of control.

South Africa belongs to the international community and therefore it was just a matter of time that it followed the trend in developing the protection of an individual’s right to privacy. The source of the right to privacy in South African law is derived from the Constitution, section 14 which is given effect by the POPIA and the common law. However, there are other legislations which have an impact on the right to privacy such as Cybercrimes Act 19 2020, Regulation of Interception of Communication and Provision of Communication-related Information Act 70 of 2002(RICA) and Electronic Communications and Transactions Act 25 of 2002. The jurisprudence of all these sources of the right to privacy overlap. The Cybercrimes Act has an impact on committing crimes on the internet, RICA gives employer’s power to intercept information communicated using their devices while the Electronic and Communications Act may also require parties be provided with information communicated electronically.

In the same way, which is the trend, South African authors have also categorized the right to privacy. The categorisation in other jurisdictions has been dubbed “dignitary privacy” and “data privacy” while in South Africa, the collection, disclosure, and use of our personal information by known and unknown government and corporate entities is classified as encroachments on (including acquisition of information) or interferences with private life, and the revelation or exposure of private information. These can further be categorised “as substantive and informational privacy rights respectively.” [52]

There is also a recognition by the Constitutional Court relating to the notion of “dignitary privacy” when it stated that the right to privacy conceptually emanates from the value of human dignity in the Constitution[53] when it said that the encroachment on

[52] South African Law Reform Commission, Discussion paper 109 Privacy and Data Protection 2004 at 19.
[53] *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd* 2001 (1) SA 545 (CC) par 18.

an individual's privacy violates the individual's related right to human dignity, a right so significant that it pervades almost all other essential rights.[54]

There are however other authors who are of the view that the right to privacy is also associated closely with the right to freedom of expression.[55] My view is that it will be correct to associate it with human dignity given the fact that the POPIA seems tacitly to support this association. There is scant support of the association of the right to privacy to freedom of expression in most literatures dealing with this right hence it has been categorized as “dignitary privacy” and “data privacy”.[56] It is doubtful that given the regulation of the right to privacy by the POPIA courts will associate it with the right to freedom of expression.

It is important to state that there were cases which were deliberated on the US test of expectation of privacy as alluded elsewhere in this research before the promulgation of the POPIA when the Constitutional Court opined in *Bernstein and Others v Bester NO and Others* 1996 (4) BCLR 449 (CC)(*Bernstein*) that as an individual engages in collective relationships and undertakings such as commerce and social communication, the range of private area diminishes proportionally.[57] This echoes the US metaphorical approach that the further one is from home the lesser the protection of the right to privacy.[58]

This legal test of reasonable expectation of privacy was also applied in *Protea Technology Ltd and Another v Wainer and Others* 1997 (9) BCLR 1225 (W) (*Protea)* when a telephone conversation was intercepted, and the court said that the right to privacy can only be protected in instances where “subjective expectation of privacy, which society recognize[d] as objectively reasonable.” It is my view that this principle would have been applicable in the workplace when an employee email would have been intercepted by the employer in his or her duties of control as can be seen from the below paragraph.

---

[54] *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services and (Media Monitoring Africa Trust and others as amici curiae) and a related matter* 2021 (4) BCLR 349 (CC) quoting various judgments handed down by the Constitutional Court at par 28.

[55] Sershiv Reddy, Establishing a test for social media misconduct in the workplace 2018 TSAR at 793.

[56] See below discussions on other jurisdictions.

[57] *Bernstein and Others v Bester NO and Others* 1996 (4) BCLR 449 (CC).

[58] See the discussion on the United States of America below.

The labour court in *Van Wyk v Independent Newspapers Gauteng (Pty) Ltd and others* [2006] 1 BLLR 73 (LC) (*Van Wyk*) also applied the reasonable expectation of privacy a test which was famously called the Katz principle in which an employee's email was read by the employer the content of which was said to be derogatory and a challenge to the employer's authority. The court in this case used the employer's policy that "all material stored on its computers was its property" which had an effect of that an employee has no expectation of privacy.

However, the CCMA in *Smith v Partners in Sexual Health (Non-Profit)* (2011) 32 ILJ 470 (CCMA) seems to hold a different view ostensibly there was no policy formulated in the same way as in *Van Wyk* barring employees using the property of the employer when it said that encroaching into employees email was against her right to privacy and such evidence is inadmissible in the arbitration in which she was charged on misconduct because the information which was found by the employer were not in the public domain.

These cases were decided before the promulgation of the POPIA. It is doubtful as this will stand the test of time and it is not one of the conditions as laid out in the POPIA and given that this is a high threshold, and the power balance tilts to the employer as alluded to in this research. It is my view that decisions which follow the reasonable expectation of privacy will conflict with the conditions as laid down in the POPIA. The decisions will not be good law in line with the ECtHR jurisprudence.

What seems to be a depart from the above cases the Constitutional Court in the case of *Investigating Directorate*: *Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd: In re: Hyundai Motor Distributors (Pty) Ltd v Smit NO* 2000 (10) BCLR 1079 (CC) *(Hyundai*), presented a nuanced approach to the protection of the right to privacy in public spaces. The court seemed to suggest that this right extends beyond "the walls of one's home,"[59] a phrase coined in the US to describe the reasonable expectation of privacy. According to the court, individuals retain a right to be left alone by the State when they are in their offices, cars, or using mobile

[59] See discussion on the United States of America.

telephones, unless certain conditions are met.[60] It is important to note that while this statement refers to the State, the Bill of Rights also applies to private parties.[61]

Hyundai is supported by a Constitutional Court decision in *Gaertner v Minister of Finance* 2014 (1) BCLR 38 (CC) in which it appears to have declined the legal test of expectation of privacy in this case. The court stated that when an individual is not within the confines of their home, they have reduced privacy protection. However, this does not imply that people no longer have a right to privacy when they engage in social interactions or business. Instead, the right to privacy is weakened, not destroyed.[62] This rationale is conceptually relevant when one uses the employer's device such as a laptop or cell phone. What follows is what implications does POPIA has given that it has been drafted in line with EU GDPR.

5.1 Implication of POPIA relating to the US test of reasonable expectation of privacy applied by our courts given that it has been drafted in line with EU GDPR

Accordingly, it is my view that the reasonable expectation of privacy is not the test in terms of South African privacy law. The reasonable expectation of privacy is a high threshold for an employee. This is also in line with the decision of the ECtHR in *Barbulescu v Romania and Niemitz v Germany* discussed under the EU section in which it did not follow this test.

Further to this the reasonable expectation of privacy seems not to be part of the conditions as laid down in the POPIA. The conditions provide a good framework for employers to respect, protect and fulfil the right to privacy of employees. As indicated elsewhere in this research the limitation clause can also serve as a test if a fundamental right has been infringed without justification.

POPIA follows the GDPR and not the US jurisprudence of expectation of privacy which is derived from the Fourth Amendment. There is no general protection of privacy from the legislation at federal level in the US as is the case in South Africa and the EU. It is my view that the approach of the Constitutional Court will be different

[60] *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd: In re: Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others* 2000 (10) BCLR 1079 (CC) par 16.
[61] See s8(2) of the Constitution of the Republic of South Africa, 1996.
[62] *Gaertner and others v Minister of Finance and others* 2014 (1) BCLR 38 (CC) par 49.

given the expansive protection provided by the POPIA particularly relating to data privacy.

The ECtHR in *Barbulescu v Romania* was of the view that reality dictates that an employer cannot expect an employee not to have a private life altogether and in *Niemitz v Germany*, the court said that "it is not always possible, in someone's occupational activities, to disentangle what falls within the professional domain from what lies outside it." It is a principle which the ECtHR emphasised when it said again that employers cannot diminish the extent of the right to privacy to nothing by merely implementing prohibitive measures concerning personal communications. Our courts will be expected to follow the principles as developed by the ECtHR given that our data privacy laws are derived from the GDPR.

South Africa has constitutionalised and legislated the right to privacy, and this elevates it as a fundamental right that needs to be respected and protected. The flow of personal information is no longer country specific but affects individuals worldwide hence the need to harmonise laws to protect the misuse in what has been dubbed the safe-harbour principles or "adequate level of protection."[63] These principles are sometimes referred to as fair information principles.[64]

These principles have been drafted in such a way that an interested party can process such data or information as a "systems of management that seek to balance and regulate the interests of various stakeholders."[65] Accordingly POPIA does not prohibit the processing of personal information, but this must be done in accordance with the eight conditions.[66]

Other replicas of our privacy laws are the CoE Convention, OECD Guidelines and the Directive 95/46/EC.[67] The most recently adopted instrument the GDPR (EU)

[63] Ibid (note 52) at 7.
[64] Anneliese Roos, Privacy in the Facebook era: A South African legal perspective 2012 SALJ at 380.
[65] Gilad Katzav, Compartmentalised data protection in South Africa: The right to privacy in the Protection of Personal Information Act 2022 SALJ at 432.
[66] Chapter 3 of POPIA.
[67] A. Naude & S. Papadopoulos, 'Data Protection in South Africa: The Protection of Personal Information Act 4 of 2013 in Light of Recent International Developments' (2016) 79 THRHR at 214.

2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR) echoes these instruments hence resulting in repealing Directive 95/46/EC.[68]

Given the preceding paragraphs, the South African law on remote work and employee privacy will be shaped by this general framework on data protection. The safe-harbour principles or "adequate level of protection"[69] transcends any differences nations may have regarding data protection such as culture or vantage point on how to address concerns relating to privacy.[70] Other authors called the safe harbour principles or "adequate level of protection" as the "principles" or "conditions."[71] The POPIA chose to use the concept of conditions. These conditions are in line with the limitation clause as espoused in s36 of the Constitution.

5.2 Examples of activities that would be regarded as ''crossing the line'' of control.

Employers should take note that there are instances in which they may be regarded as having ''crossed the line''[72] in matters that are not job related but personal in nature and are being done within the employee's working hours, activities such as sharing an apparently harmless email or providing an individual opinion in an email when there is no universal restriction on this behaviour.

Another notable example is when an employee uses an employer's provided device such as laptop or cell phone by answering an email or call from a relative such as his or her parent which is within his or her working time and has no effect on productivity and other legal obligations and compliance and this one also is personal in nature.[73] The ECtHR acknowledged this and relevant to this example when once again it said that employers cannot diminish the extent of the right to privacy to nothing by merely implementing prohibitive measures concerning personal communications. That is in line with the Guide on Article 8 of the ECtHR when it was alive to the

[68] W. Gregory Voss & Hugues Bouthinon-Dumas, 'EU General Data Protection Regulation Sanctions in Theory and in Practice' (2020) 37 Santa Clara High Tech L J at 4.
[69] Ibid (note 52) at 7.
[70] Ibid note 68.
[71] Ibid note 68.
[72] A phrase used by Karin Mika, 'Privacy in the Workplace: Are Collective Bargaining Agreements a Place to Start Formulating More Uniform Standards' (2012) 49 Willamette L Rev at 252-253.
[73] Example in line with ibid (note 1) at 1507.

“essential aspects” of private life in that there should not be a “discordance between the social reality and the law”.

The employer, however, may not have ‘’crossed the line’’ when one uses the phrase quoted in Karin Mika’s article in Ann C. Hodges’ when she states it is widely accepted that employers have the authority to observe their employees to guarantee that they are participating in fruitful labour and not breaking workplace regulations.

Neither would the employer be ‘’crossing the line’’ when an employee violates workplace rules such as disclosing confidential information or those that have a bearing on the employer liability such as protecting the safety of others be it terrorism or harassment etc.

Another practical example is when an employee’s personal activity affects productivity if most of his working time is on surfing the internet and in that process does not achieve his target than he would have if he were concentrating on the work assigned to him. It is apparent that from these examples the focus is not the ‘’human activity being regulated but the purpose and effect’’ of employer policy that matters as articulated by Prof Neil M. Richards in his article. What this tells us is that the main purpose of protecting private life is to safeguard capriciousness from the state and private actors.

6 THE LEGAL POSITION OF THE RIGHT TO PRIVACY IN OTHER JURISDICTIONS

6.1 United States of America

The right to privacy in the US compared to the European Union countries or Western Europe cannot be said to be the same. The vantage points in terms of which the two ground the basis of privacy differ.[74] This resulted in tension between the two owing to “cultural differences.” The right to privacy in the US is grounded on the ideal of liberty while in continental Europe is on dignity.[75]

There is also the categorisation of what has been termed “data privacy” and “dignitary privacy” in European countries. The former finds its expression in Article 8

[74] James Q. Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) 113 Yale LJ at 1161.
[75] Ibid at 1161.

regulating protection and collection of information and the latter in Article 7 as to "enforce social norms of respectful expression"[76] of Charter of Fundamental Rights of the European Union (2000/C 364/01) (Charter).

The GDPR gives effect to Article 8 of the Charter. Interestingly the European Convention on Human Rights Article 8(1) is a replica of Article 7 of the Charter. Despite being in different provisions they have equal force and meaning per Article 52(3) of the Charter whereby it states that to the extent that this Charter includes rights that match the rights secured by the Convention for the Protection of Human Rights and Fundamental Freedoms, the interpretation and extent of those rights will be identical to those specified in the Convention. Pursuant to this Guide on Article 8 of the European Convention on Human Rights Right (Convention) to respect for private and family life, home, and correspondence (updated on 31 August 2020) serve as a guide for Article 8 of the Charter as well.

The American conception of liberty which focuses on political rights[77] does not, in my view, lead to protection of employee privacy given the decisions of courts in that country. The US does not have legislated data privacy like other European Countries.[78] The US does not have a guaranteed right to privacy but instead it is derived through the court's interpretation of the Fourth Amendment. The interpretation has been coined as the Katz doctrine which requires an individual to establish reasonable expectation of privacy in line with what the community would also regard as "reasonable."[79] This is a high threshold to reach for an employee and therefore the power tilts to the employer.

The American vantage point on liberty is informed by the political consideration such as being free from government intrusion hence it has been metaphorically being dubbed protection from the "walls of one's home".[80] That simply when put into practice

[76] Ibid (note 23) at 992.
[77] Joel R. Reidenberg, 'Resolving Conflicting International Data Privacy Rules in Cyberspace' (2000) 52 Stan L Rev at 1343.
[78] Ibid (note 31) at 1135.
[79] Ibid (note 17) at 604.
[80] Ibid (note 74) at 1194.

means that the “American protections become progressively weaker the further the affected person is from home.”[81]

The metaphorical use of the phrase “walls of one’s home” seems not to be applicable in the digital world relating to employee privacy as worker electronic communication such as email is not forcefully enforced as is the case in continental Europe.[82] One wonders as to how the test of a ‘reasonable expectation of privacy’ emanating from the Fourth Amendment jurisprudence[83] will still hold true given the evolution of the electronic media industry and whether working remotely in places such as home will be falling within the “walls of one’s home” mantra. If this is what is still being followed to the letter, then workers privacy will be nigh impossible.[84] It is however important to note that in his dissent judgment in *Olmstead v United States*, 277 U.S. 438 (1928) Justice Brandeis was of the view that encroachment is not only confined to physically being in one’s home but that can also include through digital means.[85]

It is interesting to contrast the test of ‘reasonable expectation of privacy’ applied by the ECtHR which is discussed below in details in the section dealing with the European conceptualisation of this in *Halford v UK, Copland v UK and Barbulescu v Romania* with the American analogy in terms of which protection should be confined within the walls of one's home.

Another notable point to take note is that the reasonable expectation test has also been associated with the ownership or possession of the property. An employee was using a PC provided by an employer and the court was not persuaded that this principle is applicable, and it opined that an individual cannot have a rational anticipation of privacy in an object in which he/she has no ownership or possessory

[81] Ibid (note 74) at 1194.
[82] Ibid (note 74) at 1194.
[83] Ibid (note 74) at 1194.
[84] Ibid (note 74) at 1195.
[85] Jeremy A. Miller, 'Dignity as a New Framework Replacing the Right to Privacy ' (2007) 30 T Jefferson L Rev at 16.

stake. [86] The employee would also not have a reasonable expectation of privacy in circumstances he has consented or informed in advance that he will be monitored.[87]

This line of reasoning according to my view is at odds with the value of dignity prevalent in Continental law and more aligned to the American conception of liberty. The reasonable expectation of privacy seems to be prevalent in most states statute and is one of the tests used at common law [88] and applied in Electronic Communication Storage Act (ECSA) which in the main regulates privacy alongside and part of Electronic Communications Privacy Act (ECPA).[89] The effect of this test leaves employees at the mercy of the employer rather than the value of dignity. Additionally, this supports the assertion that the US is less concerned with addressing the processing of employee data by employers through regulation.[90] Protection of privacy in the US does not enjoy much support as it should be through legislation at a federal level.[91]

Also, Americans put more emphasis on freedom to contract and this effectively allows employees to make a choice whether they want to work or not. This then shifts the power balance to the employer in which it leaves them at the mercy of the employer.[92] The American view is that this should be left to the market forces because "rights are political rather than social in nature."[93] This line of thinking also leads to putting employee privacy rights in the periphery[94] and this is discernible from employee privacy concerns in cases decided by courts.[95]

Unlike in other countries who are members of the EU, there seems to be a protection of employee privacy by not approaching it in the prism of contractual arrangement as is the case in the US.[96] Privacy has been elevated to be a fundamental

[86] Ira David, 'Privacy Concerns regarding the Monitoring of Instant Messaging in the Workplace: Is It Big Brother or Just Business' (2004) 5 Nev LJ 321 note 12.
[87] In line with US culture of liberty in which an individual has a contractual freedom see ibid (note 74) at 1161.
[88] Ibid (note 74) at 1193.
[89] See summary of cases in (ibid note 86).
[90] Ibid (note 31) at 1116.
[91] Ibid (note 31) at 1123.
[92] Ibid (note 31) at 1138.
[93] Ibid (note 31) at 1137.
[94] Ibid (note 31) at 1138.
[95] See summary of cases in ibid (note 86) at 334-339.
[96] Ibid (note 31) at 1138.

human right which by nature should form part of human dignity in which is given by the community to individuals.[97]

This cultural difference based on the value of liberty and dignity resonates with contrasting the approach on privacy in general as articulated by Joel Reidenberg which is "either liberal, market-based governance or socially-protective, rights-based governance."[98] "Liberal, market based governance" according to my view is associated with the value of liberty in line with American culture while the "socially-protective, rights-based" with continental value of dignity.[99]

Most recently a US based IT company employee, was discharged from work by not following instructions to keep his webcam on. The employee was remotely working for that company in the Netherlands. The employee successfully challenged his dismissal based on this in the local courts and was subsequently awarded €75,000 for wrongful termination.[100] This is testimony that in the US employee privacy laws are not strictly applied compared with EU countries owing to my view to the two different cultural viewpoints on what should inform what constitutes private life.

It is important to state though that President Joe Biden hinted in his state of the union address for the Congress to take heed of the need to have data laws in the US.[101] One hopes that his call is taken into consideration that soon the US will follow suit as a signatory to the GDPR.

6.2 Germany

Privacy laws seems to have its roots in history[102] and as has been stated that the values of dignity and liberty grounded its application in continental Europe and America respectively.[103] Following from this privacy is intuitional "shaped by the prevailing legal and social values of the societies in which we live".[104] Generally, the right to privacy was vertically applied and therefore focusing on protecting an individual

[97] Ibid (note 31) at 1138.
[98] Ibid (note 77) at 1315.
[99] Ibid (note 77) at 1315.
[100] BBC News https://www.bbc.com/news/technology-63203945 Date of access 5 December 2022.
[101] LinkedIn, https://lnkd.in/eDuSyqAH (Date of access 24 March 2023)
[102] Ibid (note 74) at 1165 and infra-note 106.
[103] Ibid (note 74)1161 in which continental Europe views privacy as an aspect of dignity while to Americans it is an aspect of liberty.
[104] Ibid (note 74) at 1160.

against state power, but this traditional view has been changed by the reality that private power does have an influence on an individual in the same way state power does hence its horizontal application to private actors.[105]

However, privacy laws are being informed on the vantage point of either dignity or liberty hence the approach is different in continental Europe and America.[106] Germany is one of the countries that constitutionalised the right to privacy but covering, according to Manfred Weiss & Barbara Geck "freedom of speech, freedom of religion, freedom of conscience, and protection of the family."[107]

There are quite a number of fundamental rights which are protected by the German constitution but the most relevant which is general in its application to this research are the one stated in Article 1 protecting human dignity and Article 2 freedom to determine individual development autonomously .[108] Germany also subscribes to continental law and therefore its privacy policy is informed by the value of dignity which the Federal Constitutional Court seems to have built into the jurisprudence of an individual right to privacy .[109]

To safeguard the intrusion and give meaning to privacy the court has given the individual the power to decide which information can be in the public domain and which must be kept from public scrutiny particularly relating to electronic information which is susceptible to the invasion of one's privacy regardless of the means used for processing.[110] This was only a traditional view of vertical application meaning protecting an individual from the state power but this view has since changed in that courts apply the horizontal application as well between private citizens.[111]

The employee right to privacy cannot be interfered with at the whim of the employer unless authorized by legislation, collective agreement or permission being granted by the works council.[112] Like other jurisdictions, factors which are an exception

[105] Manfred Weiss & Barbara Geck, 'Worker Privacy in Germany' (1995) 17 Comp Lab LJ at 76
[106] Ibid (note 74) at 1161.
[107] Ibid (note 105) at 75.
[108] Ibid.
[109] Ibid (note 74) at 1161.
[110] Ibid (note 105) at 75.
[111] Ibid (note 105) at 76.
[112] Ibid (note 86) at 333.

are when a criminal conduct is an issue or an interest which can be legally justified to interfere with the right to privacy.[113]

In a recent ruling in 2017, the Federal Labour Court in Germany decided that employers cannot use keystroke-tracking software as it violates personal rights.[114] This surveillance software was allegedly used to monitor employee activity closely and ensure that they do not engage in unrelated activities. This decision was made after an employee was dismissed for using the computer for private purposes, which violated the employer's policy. However, this does not mean that employees cannot be monitored under German law. Instead, the weighing of interest is paramount in terms of German labour law, such as compelling rationale that there is criminal activity or an effect on productivity as stated in the previous paragraph.[115]

The verdict by the Federal Labour Court in Germany appears to have emphasized a ruling from 1994 that the creation of the domain of personal life is beyond the control of the employer and is restricted by the obligations of the employment agreement only to the extent that private conduct impacts the workplace and results in its disturbance.[116]

The German Federal Labour Court considers co-determination or worker participation to be a crucial aspect of the employment relationship, stating that its objective is to protect the employees' equitable right to participate in establishing the collective life (*Zusammenleben*) of the workplace.[117] In practice, this implies that there should be a form of interaction at a higher level between the parties involved in the employment relationship. In a separate ruling to emphasise engagements between parties to the employment relationship it further said that the employer's independent installation of concealed cameras to oversee workspaces is prohibited, even if they

[113] Ibid (note 86) at 333.
[114] Judgment dated July 27, 2017, case ref. 2 AZR 681/16.
[115] See quoted German Federal Labour Law cases by Franziska Boehm et al in 'How to measure IT security awareness of employees: a comparison to e-mail surveillance at the workplace' European Journal of Law and Technology Vol 7, No 1 (2016) at 4.
[116] Judgment of June 6, 1994, BAG (Bundesarbeitsgericht) reported in SAE 1995, at 103, 106 as quoted by Matthew W. Finkin, 'Menschenbild: The Conception of the Employee as a Person in Western Law' (2002) 23 Comp Lab L & Pol'y J at 583.
[117] German Federal Labour Court in Matthew W. Finkin, 'Menschenbild: The Conception of the Employee as a Person in Western Law' (2002) 23 Comp Lab L & Pol'y J at 584.

are few and even if notice has been given.[118] This principle is likely to be applicable to remote working as well.

The employer would be “crossing the line” of control if the employer detects private use during their monitoring, for example, by the confidential nature of the subject line or recipient, additional inquiry is prohibited, and the employer must cease reading that specific email immediately.[119]

6.3 France

France is one of the countries that have privacy laws. This can be attested by its promulgation of privacy laws on 6 January 1978 and 31 December 1992.[120] Both these legislations regulate employee personal information and privacy but focusing on distinct aspects. These laws have been interpreted to cover any aspect relating to advancement of technology by the watchdog body responsible for the supervision of these legislations and by courts.[121] Employers are required to inform employees through their representative union about any possible monitoring of their privacy and such data collected must have the blessing of the Commission Nationale de l'Informatique et des Libertes body tasked with that purpose pursuant to France's Law on Data Processing and Liberty.[122]

France like Germany are members of the European Union and as a result their privacy laws should be in line with the continental body. The test that has been used quite often is the proportionality and the legitimate aim of the employer failing which the employer can expect the wrath of the law in the form of damages and with a consequence of such evidence collected not in line with the dictates of the law being rendered inadmissible.[123] Employee privacy rights in France supersede the employer’s productive interest.[124]

---

[118] Ibid at 583.
[119] Peter Hanau, Thomas Hoeren and Dirk Andres, Hanau/Hoeren: Private Internetnutzung durch Arbeitnehmer (Verlag Dr. Otto Schmidt, 2003). p. 54 cited in ibid note 120 at 5.
[120] Enik Pogace, 'Employees' Data Protection in the Workplace and Its Legal Implications: A Comparative Overview of EU's Legal Framework' (2016) 10 Int'l In-House Counsel J at 2.
[121] Ibid.
[122] Ibid (note 86) at 333 and (note 120) at 4.
[123] Ibid (note 120) at 3.
[124] Ibid (note 86) at 333 quoting Jay P. Kesan in Cyber-Working or Cyber Shirking.

6.4 United Kingdom

The domestic law which regulates data protection in the UK is the Data Protection Act 1998 which has been drafted in line with European Data Protection Directive 95/46/EC. This data protection legislation despite it being drafted in line with the spirit and purport of this directive has the force of domestic law in the UK. This legislation has been in force even before Brexit and at the time of the process of leaving the EU some scholars were of the view that it will still be UK data law. The UK leaving of the EU coincided with implementation on 25 May 2018 of what can be described as a recent version of privacy and personal data law to be called GDPR. Other scholars are of the view that the UK privacy and data law will not change because of Brexit. What is important though for this research are the principles of the decisions of the domestic courts and the ECtHR relating to alleged violations. The legal effect of Brexit is beyond the scope of this research.

Article 8 Protection of personal data and Article 7 respect for private for family life has been interpreted to complement each other.[125] There has been uncertainty as to what will be the legal position of the UK relating to the GDPR given the referendum on Brexit on 23 June 2018 in which a slight majority voted in favour of getting out of the EU. The UK was technically bound by the GDPR because they were in force to member states on 25 May 2018.

However, this uncertainty was laid to bed when GDPR was published by the office of the Information Commissioner's Office on 02 August 2018 effectively embracing the EU GDPR and therefore being the law that will regulate personal data in the UK.

The UK seems to have adopted the test of a reasonable expectation of privacy that was coined by the US before Article 8 of the EU regulation can be engaged. The UK Information Commission Office has recently published a guideline on worker monitoring on 3 October 2023.

[125] See Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence (updated on 31 August 2020) and the discussion on United States of America above and Judith Townend, 'Data Protection and the Right to Be Forgotten in Practice: A UK Perspective' (2017) 45 Int'l J Legal Info at 29.

6.5 Has the European Union through its regulations changed the landscape of the right to privacy?

The European Union regulates the protection of natural persons regarding the processing of personal data and on the free movement of such data in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 which came into effect on 25 May 2018.[126] This regulation repealed Directive 95/46/EC (General Data Protection Regulation) which was in force before its repeal on 24 October 1995.[127]

Of particular importance to this research is Article 8 of the Charter of the Fundamental Rights of the European Union which is given effect by some of the provisions of General Data Protection Regulation which encompass codified principles of fair information practices and ECtHR reliance of invoking Article 7 of the Charter which deals with respect for private and family life and has been interpreted by it to protect what has been dubbed “dignitary privacy.”

The body entrusted to implement and interpret this regulation is the ECtHR at a regional level. This jurisdictional competence can be discerned in the cases discussed in this section. These cases serve as an indication on how Article 8 of the regulation has been engaged.

The reasonable expectation of privacy approach coined from the US[128] was mooted in *Halford v UK* and *Copland v UK* by the ECtHR and discarding the practice used before which cast its net wider and thereby potentially had an effect of legal uncertainty.[129] In *Halford* it was about an employee, an Assistant Chief Constable who used the business telephone for private communication and claimed that it was intercepted for ulterior motives and therefore her private life was encroached. The court upheld her complaint in that she had reasonable expectations of privacy because

[126] W. Gregory Voss & Hugues Bouthinon-Dumas, 'EU General Data Protection Regulation Sanctions in Theory and in Practice' (2020) 37 Santa Clara High Tech L J at 4.
[127] Ibid.
[128] Claire E. M. Jervis, 'Barbulescu v Romania: Why There Is No Room for Complacency When It Comes to Privacy Rights in the Workplace' (2018) 47 Indus LJ 442 and see section on United States of America above.
[129] Ibid (note 128) at 443 whereby the court derived the infringement of these rights from the values of autonomy and to a lesser extent dignity.

she was not informed beforehand that she will be monitored.[130] This decision suggests that this test is applicable to correspondence such as telephones and emails.[131]

To counter this the ECtHR was alive to this eventuality when it seems to have endorsed the approach of reasonable expectation of privacy by asking the question of whether the employee has been made aware that he or she will be monitored which logically would engaged Article 8 of the convention which regulates the right to respect for private and family life, home and correspondence.[132] This formulation of the test to right to privacy led employers to include it as a contractual term in which for example employees would be informed that they will be monitored and thereby making reasonable expectation of privacy a nullity.[133]

This led the ECtHR in *Barbulescu v Romania* not to follow this principle because it had a conviction that reality dictates that an employer cannot expect an employee not to have a private life altogether.[134]

7 CONCLUSIONS

The Protection of Personal Information Act (POPIA) has a wide application in South Africa. It is advisable for South Africa to take cues from countries like France and Germany, particularly their emphasis on including all stakeholders in privacy matters. Other European countries have legislation specifically regulating remote work or a Code of Good Practice that guides employment relationships. This Code can also serve as a guide for parties to reach a collective agreement as a form of self-regulation.

The US approach, which emphasizes the expectation of privacy, seems to have been embraced by the UK as a test. However, this approach is incompatible with the right to dignity and should not form part of our privacy law. It is hoped that this test will soon become outdated, as expressed in the state of the nation address by the US president.

[130] H. Tomas Gomez-Arostegui, 'Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations' (2005) 35 Cal W Int'l LJ at 166.
[131] Ibid at 167.
[132] Ibid (note 128) at 443.
[133] Michael Ford, 'Two Conceptions of Worker Privacy' (2002) 31 Indus LJ at 146.
[134] Ibid (note 128) at 445.

While there should be latitude for a “personal sphere” or what another German author referred to as the law of the “Inner Space,”[135] it is important to note that there are limits to employee privacy. Encroachment on the right to privacy is an affront to someone’s dignity. The right to privacy is grounded in protecting individuals’ interests, as derived from Continental law, rather than solely focusing on the American concept of liberty and protection within one’s home.

Whitman posits that privacy law is not exclusively derived from reason or shared encounters and requirements within contemporary communities. Rather, it is influenced by regional societal concerns and aspirations. In the United States, these concerns and aspirations centre around law enforcement, public servants, and the aspiration to safeguard the advantages of freedom. Conversely, on the Continent, the emphasis is on ensuring the societal standing and honour of all individuals.[136]

This perspective resonates with our ideals of protecting employees who are in a weaker position compared to employers in the employment relationship. Consequently, the government has introduced extensive job security rights, such as the right not to be unfairly dismissed. Given the value of dignity that permeates our constitutional order and applies to everyone, it is not surprising that the right to privacy must also be interpreted in conjunction with the right to human dignity, which workers should also enjoy. Therefore, it is up to the employee to determine whether their privacy has been violated, rather than the employer.

Employers should adopt a comprehensive approach that avoids excessive prying into employees’ personal lives. Excessive monitoring can lead to unintended consequences, such as employees being absent or arriving late when they could have addressed personal matters more efficiently through email or other means. Additionally, surveillance or monitoring by an employer can inadvertently infringe on other individuals’ privacy rights, potentially resulting in legal action against the employer.

Considering these factors, it is advisable for South Africa to consider adopting legislation or a Code of Good Practice specifically addressing remote work and

[135] Ibid (note 74) at 1180.
[136] Ibid (note 74) at 1219.

employee privacy. The guidelines can be drafted along the same line as the UK Data protection and monitoring workers. The guidelines cover the following aspects-[137]

- Ensuring that workers are cognizant of the nature, extent, and reasons for monitoring.
- Having a well-defined objective and utilizing the least intrusive methods to accomplish it.
- Having a legal basis for processing workers' data, such as consent or legal obligation.
- Communicating any monitoring to workers in a clear and understandable manner.
- Retaining only pertinent information.
- Conducting a Data Protection Impact Assessment (DPIA) for any monitoring that is likely to result in a high risk to the rights of workers.
- Providing workers with access to personal information collected through monitoring if they make a Subject Access Request (SAR).

[137] UK Data protection and monitoring workers https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment-information/employment-practices-and-data-protection-monitoring workers / Date of access 13 October 2023.

Bibliography

Legislation, draft legislation, and regulations:

Constitution of the Republic of South Africa, 1996.

Charter of Fundamental Rights of the European Union (2000/C 364/01).

Council of Europe's Convention for the Protection of Individuals with regard to the Automatic processing of Personal Data.

Cybercrimes Act 19 2020.

Directive 95/46/EC of the European Parliament of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data.

Electronic Communications and Transactions Act 25 of 2002.

European Convention on Human Rights.

GDPR (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

Guide to the General Data Protection Regulation (GDPR).

Organisation for Economic Cooperation and Development's Guidelines Governing the Protection of Privacy and Trans-border Data Flows of Personal Data.

Protection of Personal Information Act 4 of 2013.

Regulation of Interception of Communication and Provision of Communication-related Information Act 70 of 2002.

International Labour Organisation: Homework Convention, 1996 (No. 177).

Cases:

AmaBhungane Centre for Investigative Journalism NPC and another v Minister of Justice and Correctional Services and others (Media Monitoring Africa Trust and others as amici curiae) and a related matter 2021 (4) BCLR 349 (CC).

Barbulescu v Romania.

Bernstein and Others v Bester NO and Others 1996 (4) BCLR 449 (CC).

Copland v UK.

Gaertner and others v Minister of Finance and others 2014 (1) BCLR 38 (CC).

Halford v UK.

Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd 2001 (1) SA 545 (CC.

Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others: In re: Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others 2000 (10) BCLR 1079 (CC).

Protea Technology Ltd and Another v Wainer and Others 1997 (9) BCLR 1225 (W).

Niemitz v Germany.

Nowak v Data Protection Commissioner.

Olmstead v United States, 277 U.S. 438 (1928).

Smith v Partners in Sexual Health (Non-Profit) (2011) 32 ILJ 470 (CCMA).

Van Wyk v Independent Newspapers Gauteng (Pty) Ltd and others [2006] 1 BLLR 73 (LC).

Book/s:

J Grogan, *Workplace Law* (13th edn, Juta 2020) 23.

Articles:

Ann C. Hodges, Bargaining for Privacy in the Unionized Workplace, 22 Int'l J. of Comp. Lab. L. & Indus. Rel. 147 (2006) p159 quoting a judgment in Colgate-Palmolive Co., 323 NLRB 515 (1997).

A. Naude & S. Papadopoulos, 'Data Protection in South Africa: The Protection of Personal Information Act 4 of 2013 in Light of Recent International Developments' (2016) 79 THRHR 214.

Anneliese Roos, Privacy in the Facebook era: A South African legal perspective (2012) SALJ 380.

A. Roos, 'Personal Data Protection in New Zealand: Lessons for South Africa' (2008) 11 Potchefstroom Elec LJ 66.

Bart Custers & Helena Ursic, 'Worker Privacy in a Digitalized World under European Law' (2018) 39 Comp Lab L & Pol'y J 325.

Ben Bratman, 'Brandeis and Warren's the Right to Privacy and the Birth of the Right to Privacy' (2002) 69 Tenn L Rev 627.

Claire E. M. Jervis, 'Barbulescu v Romania: Why There Is No Room for Complacency When It Comes to Privacy Rights in the Workplace' (2018) 47 Indus LJ 442.

Darcy du Toit The right to equality versus employer 'control' and employee 'subordination': Are some more equal than others? (2016) 37 ILJ.

Da Veiga, A, Vorscer, R., Li, F., Clarke, N., and Furnell, S.M. (2019), "Comparing the protection and use of on-line personal information in South Africa and the United Kingdom in line with data protection requirements", Information and Computer Security, Vol. 28 No. 3, pp. 399-422.

Enik Pogace, 'Employees' Data Protection in the Workplace and Its Legal Implications: A Comparative Overview of EU's Legal Framework' (2016) 10 Int'l In-House Counsel J 2.

Franziska Boehm et al in ‘How to measure IT security awareness of employees: a comparison to e-mail surveillance at the workplace’ European Journal of Law and Technology Vol 7, No 1 (2016).

Gilad Katzav, Compartmentalised data protection in South Africa: The right to privacy in the Protection of Personal Information Act 2022 SALJ 432.

Guy E. Carmi, 'Dignity Versus Liberty: The Two Western Cultures of Free Speech' (2008) 26 BU Int'l LJ 300.

H. Tomas Gomez-Arostegui, 'Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations' (2005) 35 Cal W Int'l LJ 166.

Ira David, 'Privacy Concerns regarding the Monitoring of Instant Messaging in the Workplace: Is It Big Brother or Just Business' (2004) 5 Nev LJ 321.

James Q. Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) 113 Yale LJ 1163.

Joel R. Reidenberg, 'Resolving Conflicting International Data Privacy Rules in Cyberspace' (2000) 52 Stan L Rev 1343.

Jonas S Baumann and Nazreen Ismail, ‘The concept of "personal information" in the Protection of Personal Information Act 4 of 2013 – a comparative analysis from a European perspective’ (2021) TSAR 718.

Karin Mika, 'Privacy in the Workplace: Are Collective Bargaining Agreements a Place to Start Formulating More Uniform Standards' (2012) 49 Willamette L Rev 252-253.

Laura Evans, 'Monitoring Technology in the American Workplace: Would Adopting English Privacy Standards Better Balance Employee Privacy and Productivity' (2007) 95 Calif L Rev 1139.

Manfred Weiss & Barbara Geck, 'Worker Privacy in Germany' (1995) 17 Comp Lab LJ 76.

Michael Ford, 'Two Conceptions of Worker Privacy' (2002) 31 Indus LJ 146.

Matthew T. Bodie, 'The Law of Employee Data: Privacy, Property, Governance' (2022) 97 Ind LJ 723.

Milica R. Kovac-Orlandic, 'Employee's Right to Privacy: Where Is the Bound of the Employer's Right to Monitor Employees' Communications' (2020) 2020 Strani Pravni Zivot 85.

Neil M. Richards, 'Why Data Privacy Law Is (Mostly) Constitutional' (2015) 56 Wm & Mary L Rev 1507.

Rebecca Britton, 'An Employer's Right to Pry: A Study of Workplace Privacy in New Zealand' (2006) 12 Canterbury L Rev 65.

Robert C. Post, 'Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere' (2018) 67 Duke LJ 981.

Saby Ghoshray, 'Employer Surveillance versus Employee Privacy: The New Reality of Social Media and Workplace Privacy' (2013) 40 N Ky L Rev 611.

Sershiv Reddy, Establishing a test for social media misconduct in the workplace (2018) TSAR 793.

Tammy Katsabian, 'The Telework Virus: How COVID-19 Has Affected Telework and Exposed Its Implications for Privacy' (2022) 44 Berkeley J Emp & Lab L 148-149.

W. Gregory Voss & Hugues Bouthinon-Dumas, 'EU General Data Protection Regulation Sanctions in Theory and in Practice' (2020) 37 Santa Clara High Tech L J 4.

Internet sources:

BBC News https://www.bbc.com/news/technology-63203945.

LinkedIn, https://lnkd.in/eDuSyqAH.

UK Data protection and monitoring workers https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment information/employment-practices-and-data-protection-monitoring-workers/

United Nations: https://unstats.un.org/unsd/ccsa/documents/covid19-report-ccsa.

World Health Organization: https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it.

Paper:

South African Law Reform Commission, Discussion paper 109 Privacy and Data Protection 2004.