THE PRINCIPLE OF VICARIOUS LIABILITY IN THE CONTEXT OF DATA PROTECTION AND INTERNET USAGE BY EMPLOYEES

INTRODUCION

This opinion piece discusses the WM Morrison Supermarkets plc[1] Appeal decision from the Supreme Court of the United Kingdom wherein the Court pronounced on the principle of vicarious liability to answer the question of whether an employer could be ordered to pay damages for the unlawful theft and usage of personal information of its employees by a fellow employee. The case is of interest in that it touches on various issues which are the subject of much legal discourse in South Africa such as the protection of personal information, more specifically the principles to be observed when dealing with personal information, the use of social media and of equal importance the issue of payment or non-payment of damages by an employer for its employee having breached data protection laws.

EMPLOYEES AND SOCIAL MEDIA USE IN SOUTH AFRICA

The far-reaching consequences of social media use by employees in South Africa have become public knowledge on account of a few often discussed disputes such as *Fredericks,*[2] *Sedick,*[3] *Mvemve*[4] *and the Arendse*[5] case. A number of organisations have taken legal advice on various aspects of social media use and its effects on the workplace, as they have become aware of the potential risks to employers, the need for a balancing of rights, the trend of including specific provisions in employment contracts, social media policies, codes of conduct and the importance of having a social media strategy.[6]

In the *Fredericks*,[7] *Sedick,*[8] *Mvemve*[9] and *Arendse*[10] disputes mentioned above, and which were heard in the Commission for Conciliation, Mediation and Arbitration (the CCMA), the CCMA handed down rulings confirming that employees had been dismissed fairly after having made certain postings on social media.[11] It is established law in terms of Section 28 of the Arbitration Act[12] that arbitration awards in alternative dispute resolution forums such as the

---

[1] WM Morrison Supermarkets plc v Various Claimants [2020] UKSC 12 on appeal from [2018] EWCA Civ 2339.
[2] *Fredericks v Jo Barkett Fashions* [2011] JOL 27923 (CCMA).
[3] *Sedick v Krisray (Pty) Ltd* (2011) 8 BALR 879 (CCMA).
[4] *Media Workers Association of SA obo Mvemve v Kathorus Community Radio* (2010) 31 ILJ 2217 (CCMA).
[5] *National Union of Food, Beverage, Wine, Spirits and Allied Workers Union obo Arendse / Consumer Brands Business Worcester, a Division of Pioneer Foods (Pty) Ltd* 2014 7 BALR 716 (CCMA).
[6] Cowan-Harper Attorneys Presentation: "Social Media in the Context of Employment Law" accessed at https://www.labourguide.co.za/workshop/1375-social-media-handout-cowen-harper-attorneys/file on 11/4/20.
[7] *Ibid.*
[8] *Ibid.*
[9] *Ibid.*
[10] *Ibid.*
[11] *Ibid.*
[12] Act 42 of 1965.

CCMA are valid and binding.[13] These cases are therefore persuasive enough to deter employees from misconducting themselves on their personal social media profiles as this may result in dismissal from employment.

CASE DISCUSSION – UNLAWFUL PROCESSING OF PERSONAL INFORMATION

It is trite that in the adjudication of disputes within South African courts and other fora, adjudicators are permitted to derive assistance from foreign law.[14] Briefly, the facts of the WM Morrison Supermarkets case entail that one Mr Skelton, who was employed as a senior auditor of the Appellant processed the payroll data which essentially was comprised of the personal information (names, address, gender, date of birth, phone numbers, national insurance number, bank sorting code, bank account number and salary of each employee).[15] The judgment was handed down on 1st April 2020.

Mr Skelton firstly searched for software to help him disguise the identity of the computer from which he would conduct the unlawful acts;[16] he copied the personal information from his work computer onto a flash disk;[17] he had purchased an 'untraceable' phone; he created a fake email account in an attempt to frame a fellow employee for his actions;[18] and then made an unlawful disclosure (a day preceding the day on which the Appellant's financial results were due to be announced) in terms whereof he posted the personal information onto a publicly accessible file-sharing website using the phone and further proceeded to pretend to be a concerned member of the public by informing newspaper outlets that he had found the information online.[19]

The legal instrument which the Court considered as it relates to the processing of personal information in the UK is the Data Protection Act (the "DPA").[20] Territorially, this is the piece of legislation applicable in the UK, unlike the widely known General Data Protection Regulation (GDPR) put in place to deal with the processing of personal information in Europe.[21] The principles for the lawful processing of personal information in the DPA are contained in Schedule 1 thereof.[22] The Court in its judgment concerned itself with the discussion of the principle of vicarious liability to answer the pertinent question of whether the Appellant could be ordered to make payment of damages, however, it is just as important to make mention of the principles, or otherwise known in the South African legal discourse as the 'conditions' for the lawful processing of personal information.[23] It is worth noting that UK legal instruments make reference to personal data, whereas in South Africa reference is made to personal information.

---

[13] Please see *Johnson v CCMA and Others* (C450/2004) [2005] ZALC 77 at para 10.
[14] *State v Makwanyane* 1995 (6) BCLR 694.
[15] Para 4.
[16] Para 5.
[17] Para 6.
[18] *Ibid.*
[19] Para 8.
[20] Data Protection Act, 1998.
[21] About the DPA accessed at https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/about-the-dpa-2018/ on 11/4/20.
[22] Data Protection Act, 1998 accessed at http://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf on 14/4/20.
[23] Protection of Personal Information Act, 4 of 2013 (The POPIA).

CONDITIONS/PRINCIPLES FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

The data protection principles contained in Schedule 1 of the DPA state that personal data must be: processed fairly and lawfully; obtained only for one or more specified and lawful purposes, should not be further processed in any manner incompatible with such purpose; adequate, relevant and not excessive in relation to the purpose for which it was processed; accurate, up-to-date; kept for no longer than is necessary to achieve the purpose; kept in accordance with the rights of data subjects under the Act; in accordance with appropriate technical and organizational measures against the unauthorized and unlawful processing against accidental loss, destruction or damage; secured against transference to a territory outside the European Economic Area unless the foreign territory ensures adequate levels of protection.[24] These principles are similar and/or identical to the conditions contained in the POPIA.[25]

The long title of the POPIA specifically outlines that part of the purpose of the Act is to introduce certain conditions so as to establish minimum requirements for the processing of personal information. Section 2 of the Act relating to its purpose also sets the purpose of the Act as being the establishment of conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information.[26] It is submitted that considering the wording of the DPA and the GDPR regarding the principles for lawful processing of information, and the similar wording with corresponding interpretation in the POPIA, the Morrison case discussed in this opinion is of use to the South African workplace.

The conditions as set out in the POPIA are accountability;[27] processing limitation (this entails principles such as lawfulness of processing, minimality, consent, justification and objection, collection directly from data subjects);[28] purpose specification (this entails collection of personal information for a specific purpose, as well as retention and restriction of records);[29] further processing limitation;[30] information quality;[31] openness;[32] security safeguards;[33] and data subject participation.[34]

A *prima facie* view of the conditions in the POPIA and the principles as set out in the DPA reveals the importance for employers within the South African jurisdiction to heed their purpose and to actively take steps towards compliance with data protection laws as vicarious liability can be imputed in the event of a lack of compliance. The Morrison case is an example of an employee acting *ultra vires*, although the Court *a quo* was of a different view.[35]

---

[24] *Ibid.*
[25] Please see Chapter 3 of the Protection of Personal Information Act, 4 of 2013.
[26] Section 2 of the POPIA.
[27] Section 8 of the POPIA.
[28] Sections 9, 10, 11 & 12 of the POPIA.
[29] Sections 13 & 14 of the POPIA.
[30] Section 15 of the POPIA.
[31] Section 16 of the POPIA.
[32] Sections 17 & 18 of the POPIA.
[33] Section 19, 20, 21 & 22 of the POPIA.
[34] Section 23, 24 & 25 of the POPIA.
[35] *Ibid* at para 11.

It is clear, however, that the primary responsibility to observe data protection laws and put measures in place to ensure compliance with them rests with the employer. It is held as a matter of principle that public interest and the rule of law require finality.[36] It follows therefore that the Respondents, in seeking reparation for damage suffered, would pursue the employer rather than the employee as the former would be best position to make payment(s) of damages.

THE PRINCIPLE OF VICARIOUS LIABILITY

Any discussion of the principle of vicarious liability in South African casuistry is misplaced if no mention is made of the cases of *Rabie*,[37] *K*,[38] and *F*[39] wherein the Courts developed the test which consists of two main questions: firstly, whether the employee committed the wrongful acts solely in his own interests or those of the employer (the subjective question); and secondly whether there is a sufficiently close link between the employee's conduct and the business of his employment (the objective question)[40]

In the aforementioned *Booysens* case, the Court drew a clear distinction between what the Court considererd as *factors* in *K* and *F*, and what the Court considered as *requirements* and the weight to be accorded to each factor which ought to be determined on a case-by-case basis (as in *Booysens* matter). The Court concluded that the test for vicarious liability is a flexible one and will lead to different factors being accorded different weights by different courts. Scoping through the lens of South African case law, the decision of the Court in Morrison can be viewed and found to have been applied in a flexible manner.

In seeking to escape liability, the Appellant had made the argument that the DPA impliedly excludes vicarious liability for an employer.[41] The Appellant sought to place its reliance on the wording used in the DPA that states that *"[an] individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage*". The Appellant therefore drew on the definition of a data controller (referred to as a 'responsible party' in the POPIA),[42] and made the argument that *it* was the data controller, and not Mr Skelton to convince the Court that the Appellant had complied with the DPA and therefore was not responsible for the actions of Mr Skelton. The Court did not find this argument persuasive and found it to be inconsistent with the imposition of strict liability.[43] It can be drawn from this that while the outcome of the appeal was in favour of the Appellant, employers need to remain cognizant of the possible imposition of strict liability on them should they fail to observe the conditions or principles of lawful processing of personal information.

---

[36] Molaudzi v S [2015] ZACC 20 at para 16.
[37] Minister of Police v Rabie 1986 (1) SA 117.
[38] *K v Minister of Safety and Security* (CCT52/04) [2005] ZACC 8; 2005 (6) SA 419 (CC); 2005 (9) BCLR 835 (CC) ; [2005] 8 BLLR 749 (CC) (13 June 2005)
[39] *F v Minister of Safety and Security and Another* (CCT 30/11) [2011] ZACC 37; 2012 (1) SA 536 (CC); 2012 (3) BCLR 244 (CC); (2012) 33 ILJ 93 (CC); 2013 (2) SACR 20 (CC) (15 December 2011)
[40] Please see *Booysen v Minister of Safety and Security* (CCT25/17) [2018] ZACC 18; 2018 (9) BCLR 1029 (CC); 2018 (6) SA 1 (CC); 2018 (2) SACR 607 (CC) (27 June 2018) at para 11.
[41] *Ibid* at para 52.
[42] Section 1 of the Protection of Personal Information Act, 4 of 2013.
[43] Para 53.

In their article on the practical application of strict liability Millard and Bascerano[44] hold the view that the POPIA creates a form of strict liability. This view is correct considering the civil suit remedy available to an aggrieved data subject against a responsible party.[45] To buttress this view, the authors state that by ascribing accountability to the employer, the POPIA creates a form of strict liability. Accountability is the very first of the 8 (eight) conditions for lawful processing of personal information in the POPIA.[46] This condition requires that "*the responsible party must ensure that the conditions, as well as all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself*."[47]

While the Court in the Morrison case made no mention of an accountability principle, and neither does the DPA, it is clear that strict liability is a very real consequence for any employer in the event that its employees breach data protection laws. The aforementioned provision relating to civil remedies in terms of POPIA states that "*a data subject or, at the request of the data subject, the Regulator, may institute a civil action for damages in a court having jurisdiction against a responsible party for breach of any provision of the Act … whether or not there is intent or negligence on the part of the responsible party.*" In consideration of the fact that a civil suit may also be instituted by the custodian of the POPIA itself (the Information Regulator), POPIA must be a sufficient deterrent to any organization from being lax in observing data protection laws and ensuring strict compliance by its employees.

CONCLUSION

The Court in Morrison found that Mr Skelton himself was indeed a data controller, however, it found the DPA to be silent about the position of an employer of a data controller (otherwise a responsible party).[48] The Court drew the conclusion that there cannot be an inconsistency between the duties imposed by the DPA, or for breaches arising under the common law.[49] The Court found that Mr Skelton's disclosure of the personal information of Morrison employees on the internet did not form part of his functions or field activities.[50] The Court also held that the mere fact that Mr Skelton's employment gave him an opportunity to commit the wrongful act would not be sufficient to warrant the imposition of vicarious liability.

The Morrison example is one that gives a detailed discussion on the principle of vicarious liability *vis-à-vis* the observation of data protection legislation similar to that of South Africa. Employers and employees are encouraged to observe all the conditions for the lawful processing of personal information contained in the POPIA as all its provisions are soon to come into full force and effect. While this particular case excluded the employer's liability, it is important to note that strict liability is an actual possibility for responsible parties in South Africa and that each case will be determined on its specific facts. The common form of sanction for unlawful internet use comes from decided cases on the use of social media in South Africa, however, it is to be expected that such cases should be read in light of the POPIA as it is the most important data protection law with consequences for employers and employees.

---

[44] Millard D and Bascerano EG "Employers' Statutory Vicarious Liability in Terms of the Protection of Personal Information Act" PER / PELJ 2016(19) - DOI http://dx.doi.org/10.17159/1727-3781/2016/v19i0a555.
[45] Please see Section 99 of the Protection of Personal Information Act, 4 of 2013.
[46] Please see
[47] Section 8 of the POPIA.
[48] Para 54.
[49] *Ibid.*
[50] Para 31.

Vilimile Gumede (BA Law) UP
Candidate Attorney at Snail Attorneys @ Law
E-mail: vgumede@snailattorneys.com
Skype Name: vili.gumede

Masego Morige (BCom Law) MGI
Paralegal at Snail Attorneys @ Law
E-mail: masego@snailattlorneys.com
Skype Name: MasegoMorige