THE LEGAL ISSUES REGARDING THE USE OF ARTIFICIAL INTELLIGENCE TO SCREEN SOCIAL MEDIA PROFILES FOR THE HIRING OF PROSPECTIVE EMPLOYEES

Sershiv Reddy
LLB LLM
Lecturer, University of Johannesburg

SUMMARY

The fourth industrial revolution has introduced advancement in technologies that have affected many commercial sectors in South Africa, and the employment sector is no exception. One of these advancements is the creation of artificial intelligence technologies that can assist humans to make everyday tasks quicker and more efficient. It has become common for organisations to screen social media profiles in order to gain information about a prospective employee. With the aid of artificial intelligence, employers can use such systems to easily sift through social media profiles and access the data it needs. Although these technological creations have many successful outcomes, artificial intelligence systems can also have drawbacks, such as inadvertently discriminating against certain groups of people when data is collected, processed and stored. Issues surrounding privacy breaches are also raised where artificial intelligent systems seek to access personal information from social media profiles. Prospective employees will need to be informed that their social media profiles are being screened and the artificial intelligence system needs to be programmed properly to ensure that data is correctly and fairly processed and collected.

1 INTRODUCTION

The past few decades have seen an information revolution where electronic and Internet-connected devices have led to a social media revolution.[1] Although the law may have in some instances adapted to new technologies, the rapid advancements in technologies necessitate a response from policymakers.[2] The fourth industrial revolution may have the effect of blurring the distinction between the physical and digital world. This revolution is a

1 Potgieter *Social Media and Employment Law* (2014) 5.

2 Calo "Robotics and the Lessons of Cyberlaw" 2015 *California Law Review* 513 562. The author concludes that robotics will affect our lives in a profound way, and it is up to us to provide a legal reaction that is balanced and cognisant of the impact of these new technologies.

fast-emerging shift from the previous ones and involves smart systems and automated machines that include emerging technological breakthroughs such as artificial intelligence (AI), blockchain technology, advanced robotics, the Internet of Things, and autonomous vehicles that create a fusion of technologies across physical, digital and biological worlds.[3]

Calo argues that issues surrounding robotics and AI raise the question as to how the legal fraternity will deal with these new technological advancements because these developments will surely affect the law disciplines.[4] The fourth industrial revolution will no doubt require technological and legislative reform to address the changes it brings. The change in technology has created new risks such as safety issues, privacy concerns and data risks.[5] The aim of the law should be to encourage innovation and growth and to be wary of over-regulating the industry; at the same time, the law needs to protect other important rights of individuals from harm.

Although the fourth industrial revolution seeks to encourage innovations and ideas, it also poses certain risks to the employment sector. According to a report published by the World Economic Forum in 2018, the advancement of technology and issues impacting socio-economic factors have decreased the work-lifespan of many employees because their skills will be outdated and only those employees who can work with AI are likely to benefit from these advancements.[6] Forbes argues that as technology continues to advance, AI can revolutionise the way that companies hire and fire employees.[7] The legal issue is whether AI technologies should be used to gather data on individuals for the purposes of hiring employees. This is because a great concern with AI is that it can be biased in collecting and processing information, leading to a lack of fairness and accountability.[8] Hauser argues that machine-to-machine communications will bring about regulatory issues and it may be necessary for laws to be updated in order to adapt to these legal hurdles.[9] One of the main concerns with the monitoring, collection and processing of personal information of another is breach of privacy.

---

3 Schwab *The Fourth Industrial Revolution* (2017) 1–17.

4 Calo 2015 *California Law Review* 513 550.

5 Tschider "Regulating the Internet of Things: Discrimination, Privacy and Cybersecurity in the Artificial Intelligence Age" 2018 *Denver Law Review* 87 89.

6 Schwab "Towards a Reskilling Revolution: A Future of Jobs for All" 2018 http://www3.weforum.org/docs/WEF_FOW_Reskilling_Revolution.pdf (accessed 2019-03-29) 3.

7 Rogers "The Key Role Evolving AI Will Play in Tech Hiring and Firing" (12 June 2018) https://www.forbes.com/sites/forbestechcouncil/2018/06/12/the-key-role-evolving-ai-will-play-in-tech-hiring-and-firing/#614fc4b4b32b (accessed 2019-03-29).

8 Katyal "Private Accountability in the Age of Artificial Intelligence" 2019 *University of California Law Review* 54 58.

9 Hauser "Industry 4.0: Digital Business, Autonomous Systems and the Legal Challenges" (2014) *Business Law Magazine* https://www.businesslaw-magazine.com/wp-content/uploads/sites/4/2015/04/BLM_Seite-26-29.pdf 26 28.

2 PRIVACY

At common law, Mcquoid-Mason argues that invasion of privacy is addressed through the *actio injuriarum* and depends on whether a reasonable person of ordinary sensibilities would regard the invasion of privacy as unlawful.[10] Privacy entails seclusion from the public by an individual and may be infringed by the unauthorised act of an outsider on the individual or her personal affairs.[11] Bilchitz avers that the right to privacy seeks to protect the freedom of the individual against the arbitrary exercise of coercive power by the State and further provides the individual with a sense of personal security.[12] This means that people have the right to be free from government intrusions in order to have a sense of safety from interference from outsiders.

Besides privacy being protected at common law, the right is also enshrined in section 14 of the Constitution:[13]

> "Everyone has the right to privacy, which includes the right not to have–
> (*a*) their person or home searched;
> (*b*) their property searched;
> (*c*) their possessions seized; or
> (*d*) the privacy of their communications infringed."

A contravention of section 14 of the Constitution may be regarded as an unlawful invasion of privacy, unless the breach is justified in terms of section 36[14] of the Constitution.[15] In *Berstein v Bester*,[16] the court took cognisance of the fact that privacy has its boundaries and is not absolute:

> "Privacy is acknowledged in the truly personal realm, but as a person moves into communal relations and activities such as business and social interaction, the scope of personal space shrinks accordingly."[17]

Burns supports this argument and provides that the scope of privacy will vary, depending on whether it is truly a personal space that has been infringed or whether it involves communal relations.[18]

---

10 Mcquoid-Mason "Invasion of Privacy: Common Law v Constitutional Delict – Does it Make a Difference?" 2000 *Acta Juridica* 227 229–223.

11 Neethling, Potgieter and Visser *Law of Delict* (2014) 371.

12 Bilchitz "Privacy, Surveillance and the Duties of Corporations" 2016 *TSAR* 45.

13 The Constitution of the Republic of South Africa, 1996.

14 The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including–
(a) the nature of the right;
(b) the importance of the purpose of the limitation;
(c) the nature and extent of the limitation;
(d) the relation between the limitation and its purpose; and
(e) less restrictive means to achieve the purpose.

15 Mcquoid-Mason 2000 *Acta Juridica* 227 246.

16 1996 (2) SA 751 (CC).

17 Par 67.

As privacy is not absolute, it may be limited in certain circumstances. Privacy must be balanced with other competing interests and rights such as freedom of speech and access to information.[19] Burns argues that in South Africa, it is well established in our law that once information has entered the public domain, there can be no legitimate expectation of privacy in relation to such information.[20]

Bilchitz argues that technology has become a standard feature in our daily lives both socially and commercially and because of this continuous usage, such technology exists in both private and public spaces, which in turn may lead our communications to be monitored and tracked.[21] Although individuals may make use of the Internet and social media in their private homes where privacy is highly protected, the consequence of technology has allowed this intimate space to become potentially publicly accessible.[22] Thus despite privacy being highly protected in our private homes, this right may lose its protection once information has been published to the public.

Goddard opines that the use of social media raises the fundamental question as to what information uploaded onto these platforms is considered to fall within and outside the public domain.[23] The idea of protecting online privacy stems from the protection of personal or sensitive information, which if divulged to the public may cause harm to the user. This is why several websites have created privacy settings that allow users to control access to information and limit other users from viewing their posts.[24] It must be understood, therefore, that where a user reveals personal information to a limited group of people, the user has only consented to the publication of that information to that selected group and not to everyone on the Internet.[25] With this in mind, entities such as insurers may use different methods to obtain social media information, but are often limited in such access by privacy settings, including being blocked from viewing a policyholder's location, pictures and updates.[26]

In *Bernstein v Bester*,[27] the court stated that any information pertaining to participation in a public sphere cannot be subject to a reasonable expectation of privacy.[28] Bilchitz argues that with respect to privacy and the monitoring of personal communications, the key test is whether the

---

18 Burns *Communications Law* (2015) 231.

19 Swales "Protection of Personal Information: South Africa's Answer to the Global Phenomenon in the Context of Unsolicited Electronic Messages (Spam)" 2016 *SA Merc LJ* 49 59.

20 Burns *Communications Law* 604.

21 Bilchitz 2016 *TSAR* 45.

22 Bilchitz 2016 *TSAR* 45 52.

23 Goddard "Sharing Privately: The Effect Publication on Social Media Has on Expectations of Privacy" 2017 *Journal of Media Law* 45 52.

24 McGuinness and Simon "Information Disclosure, Privacy Behaviours, and Attitudes Regarding Employer Surveillance of Social Networking Sites" 2018 *International Federation of Library Associations and Institutions* 203 205.

25 Roos "Privacy in the Facebook Era: A South African Legal Perspective" 2012 *SALJ* 375 399.

26 Cole and McCullogh "The Use of Social Media by Insurers and Potential Legal and Regulatory Concerns" 2012 *Journal of Insurance Regulation* 181 186.

27 *Supra*.

28 Par 85.

individual has a reasonable expectation of privacy.[29] Bilchitz further opines the following in determining an individual's reasonable expectation of privacy:

> "In testing the reasonableness of an expectation, however, I would suggest that some of the factors that are expressly contained within the general limitations clause could well be relevant, including – in particular – a proportionality enquiry. That would require determining whether there was any legitimate purpose for interfering with a subjective expectation of privacy, the relationship between the interfering means adopted and the purpose, whether there is an alternative that interferes less with the subjective expectation yet still achieves the purpose and a balancing of the interests of the individual in privacy and the company in question."[30]

On the basis of the above, one needs to determine whether a person has a reasonable expectation of privacy in respect of the information sought by another. A reasonable expectation of privacy may become a bit more difficult when information is readily available on social media. In the United States, most of the courts have ruled that users lose their reasonable expectation of privacy where they post communications on social media platforms.[31] Issues concerning social media receive a separate and further analysis below.

3 SOCIAL MEDIA

Social media has been in existence for some time now and is no longer considered a new innovation. It is common for employers and employees to use social media in their personal capacities, as well as for business purposes. It is not uncommon for employers to use social media as a means to do background checks on potential employees to decide whether a person would be suitable for the position. Facebook, Twitter, and Instagram are common social media sites used by recruiters and some studies have found that 70 per cent or more of recruiters search prospective employees' social media profiles to screen applicants.[32] Other sources have further indicated that three in five recruiters have turned down a candidate owing to content on social media and 57 per cent of recruiters say that they find content on social media that makes candidates unsuitable for the required job.[33] Social media is therefore a powerful tool that recruiters and employers can use to find prospective candidates.

Social media leaves behind a digital footprint that can be tracked and followed.[34] Mund argues that normal daily in-person conversations traditionally constituted private speech, but such conversations now

---

29 Bilchitz 2016 *TSAR* 45 64.

30 Bilchitz 2016 *TSAR* 45 65.

31 Mund "Social Media Searches and the Reasonable Expectation of Privacy" 2017 *Yale Journal of Law & Technology* 238 249.

32 Zhang, Van Iddekinge, Arnold, Roth, Lievens, Lanivich and Jordan "What's on Job Seekers' Social Media Sites? A Content Analysis and Effects of Structure on Recruiter Judgments and Predictive Validity" 2020 *Journal of Applied Psychology* 1530.

33 Ranosa "How Recruiters Check for Red Flags on Social Media" (29 October 2019) https://www.hcamag.com/au/specialisation/hr-technology/how-recruiters-check-for-red-flags-on-social-media/189899 (accessed 2020-04-01).

34 See generally McPeak "The Facebook Digital Footprint: Paving Fair and Consistent Pathways to Civil Discovery of Social Media Data" 2013 *Wake Forest Law Review* 887.

transpire over social media, leaving digital footprints and evidence as to a person's behaviour, and that such information is not entirely private.[35] The problem is that people wish to share information on social media and at the same time are led to expect that this information may be shared privately because they are likely to share more if they know that their information will remain secure.[36] Authors have argued that social media users feel safe to share information on social networks because they feel it is a controlled environment where information is shared to a specific audience who they can sometimes choose through privacy settings. However, this privacy is sometimes misconceived owing to the visibility of their profiles to the general public.[37] The consequence is that online users may think their profiles and publications are only visible to their contact list, when in fact they may be visible to the public. Although privacy rights exist, these arguably diminish on an online public platform, and they also depend on the reasonable expectation of privacy. This is because private information is no longer a secret owing to the public effect of social media publications.[38] People sign up on different social media platforms and consent to the processing of their private data and personal information. Sharing information publicly on social networks is commonplace and one of the main reasons for its creation.[39]

Although the main purposes of social media are to facilitate communication and allow for the uploading of instant communications, this is done on a purely voluntary basis by a user.[40] This means that people may choose what to upload on their profiles and no one forces them do so. Grimmelmann argues that people tend to blame social media for private information uploaded onto these websites. Yet, social media does not compel its users to compromise their privacy; rather, it offers users a means to communicate, and exposing private information is a personal choice.[41] People may disclose personal information on their profiles and this act of disclosure is referred to as a user's "visibility" to others, which may be controlled through privacy settings on social networks.[42] A user's profile is therefore visible to everyone else on social media unless they have controlled their visibility through the privacy settings.[43]

One may argue that creating a profile on social media is similar to appearing in a public place because the Internet is regarded as such. However, the privacy settings will determine whether a person has chosen to

---

35 Mund 2017 *Yale Journal of Law & Technology* 238 239.

36 Goddard 2017 *Journal of Media Law* 45 50.

37 McGuinness and Simon 2018 *International Federation of Library Associations and Institutions* 203 203–204. The authors argue that the failure to have adequate privacy settings on social media profiles exposes users to certain risks such as allowing unwanted viewers to obtain information that has been uploaded on their social media profiles.

38 Potgieter *Social Media and Employment Law* 36. The author argues that information, which was once a secret, can now be uploaded on social media and information regarding companies can become transparent to the world.

39 McGuinness and Simon 2018 *International Federation of Library Associations and Institutions* 203 205.

40 Goddard 2017 *Journal of Media Law* 45 46.

41 Grimmelmann "Saving Facebook" 2009 *Iowa Law Review* 1137 1140.

42 Roos 2012 *SALJ* 375 386.

43 *Isparta v Richter* 2013 (6) SA 529 (GNP) par 6.

disclose personal information to a specific group of people.[44] Roos argues that social media poses certain threats to the right to privacy:

(1) when users divulge personal information on their social media profiles;
(2) when the social network operators receive information from users or third parties and process this information; and
(3) when third parties gain access to a user's personal information.[45]

Although social media websites were created to foster communication and relationships between people across borders, it has also given rise to new legal issues that were not originally anticipated, especially in instances where users argue that their postings are private.[46]

The unintended consequence of social media platforms is that personal information is readily available, and this allows both private and public bodies to collect personal data with ease.[47] Social media postings have been argued to reflect people's intelligence and personality, including their dark-side traits. However, the relevant question is whether it is legal and ethical to process this data for hiring purposes.[48] Information in the public domain and particularly on the Internet may be obtained by anyone with Internet access. This is because social media profiles have readily available information in one place; a comprehensive profile will contain personal information pertaining to a person's name, birthday, political and religious views, contact information, gender, relationship status, educational and employment history, and pictures.[49]

Although companies do not have direct access to prospective employees' social media profiles, if their profile lacks privacy settings, the employer may be able to access that profile and all its contents. Where an employee's social media settings are private, there is no way an employer may lawfully access the employee's profile. The accessing of a user's social media will not be held to be an invasion of privacy where the person fails to make use of the privacy options on these sites. However, where a person does restrict access through privacy settings, comments published online may fall into a zone of privacy upon which another should not intrude.[50] In *Sedick v Krisray*,[51] it was held that because the Internet is generally part of the public domain, social media is by its nature also part of the public domain, but members are able to exercise options to restrict access to their personal pages and the content of those pages.[52]

---

44 Roos 2012 *SALJ* 375 386.

45 *Ibid*.

46 Langan "Likes and Retweets Can't Save Your Job: Public Employee Privacy, Free Speech and Social Media" 2018 *University of St Thomas Law Journal* 228 229–230.

47 Mund 2017 *Yale Journal of Law & Technology* 238 241.

48 Dattner, Chamorro-Premuzic, Buchband and Schettler "The Legal and Ethical Implications of Using AI in Hiring" (25 April 2019) *Harvard Business Review* https://hbr.org/2019/04/the-legal-and-ethical-implications-of-using-ai-in-hiring (accessed 2020-04-01).

49 Grimmelmann 2009 *Iowa Law Review* 1137 1149.

50 *National Union of Food, Beverage, Wine, Spirits and Allied Workers Union obo Arendse* v *Consumer Brands Business Worcester, a Division of Pioneer Foods (Pty) Ltd* 2014 (7) BALR 716 (CCMA) par 16.

51 (2011) 8 BALR 879 (CCMA).

52 Par 50.

4 PROCESSING PERSONAL INFORMATION

Once an organisation is legally allowed to collect information about another individual, it must ensure that the collection of such information is done in the correct manner. When an employer enters data on a system pertaining to an individual, it must ensure it is collected, processed and stored in the correct manner in order to keep the integrity of the information and maintain its confidentiality.[53] It is submitted that employees will trust their employers when they know their data remains safe and is kept and used in a responsible manner. Where data is carelessly processed and leaked, employees may have legal recourse against employers for breaches of privacy. Data processing therefore has important legal ramifications in the employment arena and transgressions are unlikely to be taken lightly by employees, especially in a digital world where information can be transferred and communicated instantly. Sensitive and private information may be spread with ease and breaches of privacy occur more easily than in the past because of technology. As is mentioned later in this article, AI requires the collection of big data to function and the risk of disclosing sensitive or personal information is great.[54] The protection of personal information therefore becomes crucial.

The importance of protecting personal information cannot be overstated. Swales states that the "protection of personal information is becoming a basic necessity as more and more people conduct their lives in an ever-increasing digital manner".[55] Historically, privacy concerns centered on the State and its power to constrain the private lives of its citizens, but now there has been a shift that has led to other bodies collecting large amounts of personal information relating to individuals.[56] Roos aptly notes that privacy concerns were raised when technology advanced since computers were able to misuse personal information by storing vast amounts of personal information relatively easy, cheaply and for almost indefinite periods.[57] Etsebeth highlights legal considerations relating to information security in regard to:

(i) the way in which information is created, processed, stored, transmitted, used and communicated;
(ii) who has access to this information;
(iii) the reasons and purposes of collecting the information;
(iv) the duration of such access; and
(v) who has the authority to change access and how.[58]

---

53 Tschider 2018 *Denver Law Review* 87 116.

54 Tschider 2018 *Denver Law Review* 87 117. The author submits that these data breaches may relate to sexual preferences, personal finances and health conditions – information that an individual may only want to share with a family member or friend and not anyone else.

55 Swales 2016 *SA Merc LJ* 49.

56 Bilchitz 2016 *TSAR* 45.

57 Roos 2012 *SALJ* 375 377.

58 Etsebeth "Governance in the Information Age: Implications for the Law" 2005 *TSAR* 274 276.

The collection of data by computers poses a threat to privacy in instances where there is unauthorised collection of personal data and the disclosure of such data.[59] As a result of privacy issues relating to the collection and storage of personal information, data protection principles should apply when personal information is processed, collected and stored by other bodies.[60] What these arguments indicate is that online personal information may be collected and processed, as long as certain steps have been taken and brought to the attention of the individual whose data is in issue. At the same time, however, an individual can only make a decision once he or she has been properly informed as to what information is being collected and the purpose for such collection.

Where persons give voluntary consent and lawful access to their personal and private information, they also voluntarily assume the risk attached to the exposure of that information.[61] This indicates that where a person voluntarily reveals information to another party, the former party impliedly waives his or her right to privacy and cannot reasonably expect to limit the recipient's usage of that information since permission has been granted.[62] It has been argued, however, that although an individual has the right to consent to information being released or monitored, the reality of such consent may be affected by certain power relations.[63] Prospective employees may thus have no choice but to accept the agreed terms of allowing employers to collect their information via social media because without acceptance, an employee may not be hired for the job. Roos argues that the social media user must have full knowledge and appreciation of the nature and extent of the possible harm that may arise when consent is granted because a person cannot validly consent to the disclosure of personal information if she or he is not informed of what it will be used for or who will have access to it.[64]

5 POPIA

The Protection of Personal Information Act[65] (POPIA) regulates the "processing" of "personal information" by certain bodies. The Act recognises the importance of the right to privacy and provides that it includes a right to protection against the unlawful collection, retention, dissemination and use of personal information; at the same time, it acknowledges that privacy is subject to justifiable limitations that are aimed at protecting other important interests and rights such as the access to information.[66]

The Act will apply to social media communications because of the type of information that is uploaded onto these websites. "Personal information" is given a broad meaning in the Act and includes the personal opinions, views

59 Burns *Communications Law* 235.
60 Roos 2012 *SALJ* 375 387.
61 Mund 2017 *Yale Journal of Law & Technology* 238 246.
62 Mund 2017 *Yale Journal of Law & Technology* 238 250.
63 Bilchitz 2016 *TSAR* 45 58.
64 Roos 2012 *SALJ* 375 399.
65 4 of 2013.
66 See the Preamble of the Act, read with ss 2(*a*)(i)–(ii).

or preferences of a person, which are often posted on social networks.[67] "Processing" is defined as:

> "any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including–
> (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
> (b) dissemination by means of transmission, distribution or making available in any other form; or
> (c) merging, linking, as well as restriction, degradation, erasure or destruction of information."[68]

As a result of this wide definition, the use of any of a prospective employee's personal information from social media by an employer or recruiter will amount to information being processed, even if it is a once-off activity. The applicability of the Act to recruiters or employers also relies on other important definitions such as "private body",[69] "public body"[70] and a "responsible party".[71] Furthermore, section 3 of POPIA applies to the processing of personal information that is entered in a record by or for a

---

67 See s 1 definitions, which defines "personal information" as information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to–
(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
(b) information relating to the education or the medical, financial, criminal or employment history of the person;
(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
(d) the biometric information of the person;
(e) the personal opinions, views or preferences of the person;
(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
(g) the views or opinions of another individual about the person; and
(h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

68 S 1 of POPIA.

69 "Private body" means–
(a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity;
(b) a partnership which carries or has carried on any trade, business or profession; or
(c) any former or existing juristic person, but excludes a public body.

70 "Public body" means–
(a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or
(b) any other functionary or institution when–
(i) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or
(ii) exercising a public power or performing a public function in terms of any legislation.

71 "Responsible party" means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

responsible party by making use of automated means[72] or non-automated means and where it is processed by non-automated means, it forms part of a filing system or is intended to form part thereof.[73]

The Act emphasises the lawful processing of information[74] and much relies on consent being given by the person whose information is being processed. Consent envisages any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.[75] Consent must be obtained from a person in order to process his or her information, although the processing may occur if it is necessary for pursuing the legitimate interests of the responsible party.[76]

Although personal information should be collected directly from a person, the Act allows a responsible party to dispense with this requirement where the information concerned is found in a public record or has deliberately been made public by the person.[77] This is where social media becomes so important. On social media platforms, public profiles contain information about an individual and may be used by the employer because it is in the public domain. As alluded to earlier, relaxed privacy settings therefore provide an opportunity in allowing employers to collect information from social media profiles of prospective employees. Although it has been established that employers can use social media information to consider hiring prospective employees, there may be some bias attached to these processes. This bias or discrimination may materialise where employers rely on technology to search and filter relevant candidates for the interview process.

6 ARTIFICIAL INTELLIGENCE AND SCREENING EMPLOYEES

Most current legislation was drafted before the fourth industrial revolution, and this may warrant significant legislative reform to enable the law to keep up with technological advancements. Prospective employees may not be aware of the amount of data that others possess about them and are also not aware of how such data is used by AI systems.[78] Organisations use AI

---

72 S 3(4) of POPIA provides that "automated means", for the purposes of the section, means any equipment capable of operating automatically in response to instructions given for the purpose of processing information.

73 S 3(1)(*a*) of POPIA. S 3(1)(*b*) provides further that in order for the Act to apply, the responsible party should be:

(i) domiciled in the Republic; or

(ii) not domiciled in the Republic but makes use of automated or non-automated means in the Republic, unless those means are used only to forward personal information through the Republic.

74 S 4 of POPIA sets out certain conditions that need to be met by the responsible party for the lawful processing of information, read with s 9, which provides that personal information must be processed in a reasonable manner that does not infringe upon the right to privacy.

75 S 1 of POPIA. Also see s 11, which sets out when consent is necessary.

76 See s 11(1)(*a*)–(*f*) of POPIA.

77 S 12(2)(*a*) of POPIA.

78 Yanisky-Ravid and Hallisey "Equality and Privacy by Design: A New Model of Artificial Intelligence Data Transparency via Auditing, Certification, and Safe Harbour Regimes" 2019 *Fordham Urban Law Journal* 428 455.

systems and big data to decide which applicants to interview or hire in their companies, but this can raise certain concerns.[79]

Data has been described as the "lifeblood" of AI because it relies on a constant feed of data to analyse and process its systems.[80] Data and AI are able to determine personal attributes of people with accuracy based on their social media profiles, where personal information is accurate and identifiable.[81] Artificial intelligence relies on the processing of information or data given to its system, hardware or software and operates through codes or algorithms.[82] Katyal submits that big data and AI seek to fulfil the modern-day promises of ease, efficiency and optimisation.[83] It is true that AI can significantly reduce the legal costs and time of work and is therefore appealing to the commercial sector. Hauser proposes that one of the biggest issues with the fourth industrial revolution is the ability to generate, process and use large amounts of data for commercial purposes.[84]

This means that AI may provide accurate and high-end services in different fields without the need for human intervention. Although these "machines" may work at a greater speed of processing, there may always be a need for human supervision and guidance. There is no doubt that the fourth industrial revolution can positively change the world, but conversely it may also create certain negative legal consequences. Yu proposes that in order for an automated AI system to be fair, it should rely on translation (building legal rules and outcomes), approximation (approximating decisions and providing updates and feedback into the system) and self-determination (independent autonomous decisions in which the system will make decisions that, in its view, are correct).[85] Translation and approximation are created and rely on human decisions, whereas self-determination allows for autonomous determinations, which can occur without human involvement.[86]

AI has changed the way in which data is collected and processed by using and collecting large amounts of data, which has not previously been possible.[87] The scary possibility of AI is that it has the potential to anticipate our behaviour and predict our intentions.[88] This means that through algorithms coded on AI, the intelligence will use specific data to predict intentions and outcomes of employees in the workplace by analysing their

---

79 Prince and Schwarcz "Proxy Discrimination in the Age of Artificial Intelligence and Big Data" 2020 *Iowa Law Review* 1257 1259.

80 Weaver "Artificial Intelligence and Governing the Life Cycle of Personal Data" 2018 *Richmond Journal of Law & Technology* 1 2.

81 Dattner *et al* 2019 *Harvard Business Review*.

82 Hildebrandt "Law as Computation in the Era of Artificial Legal Intelligence: Speaking Law to the Power of Statistics" 2018 *University of Toronto Law Journal* 12 26.

83 Katyal 2019 *University of California Law Review* 54 56.

84 Hauser https://www.businesslaw-magazine.com/wp-content/uploads/sites/4/2015/04/BLM_Seite-26-29.pdf 26 27.

85 Yu "Artificial Intelligence, the Law-Machine Interface and Fair Use Automation" 2020 *Alabama Law Review* 188 206–213.

86 Yu 2020 *Alabama Law Review* 188 206.

87 Tschider 2018 *Denver Law Review* 87 96. The author submits that AI and machine learning allow for a variety of capabilities, ranging from self-driving cars to fully functional automated robots.

88 Hildebrandt 2018 *University of Toronto Law Journal* 12 27.

behavioural patterns. Although AI systems can predict outcomes, they also have the ability to create new content.[89] AI programs can find patterns or preferences that others did not perceive, including the data subject him- or herself.[90]

Machine learning will affect the legal field in new ways, especially where it relates to data processing and disclosure of information.[91] Machine learning involves algorithms that are trained to learn from a body of data based on past human behaviour and practices and which then develop for future use.[92] Machine learning is where AI is exposed to data and the system identifies patterns after performing different tasks; as long as it is fed enough data, the system will continue to develop and learn.[93] It is submitted that issues could arise from these practices, especially where employers may programme a system not to hire a particular person for one job function and the system thereafter learns that this particular person is unsuitable for any other job function.

An AI system that has been created to predict who will be a successful employee can only do so if it has been programmed and trained in a certain way, as well as by using historical hiring data; relying on such data may create the risks of historical disparities in employment.[94] This will create bias and discrimination against people in the same category as the individual who is now not considered for any future role in the company. Raub argues that a lack of responsibility and accountability in relation to artificial intelligence and algorithms may lead to certain pitfalls in employment relating to discrimination in terms of unequal opportunities.[95] Despite issues with using AI automated systems, this does not mean that one should refrain from using these systems; rather, one should properly make use of its operation and be active in providing updates or corrections when issues arise.[96]

Using AI, data, social media, and machine learning, employers have greater access to candidates' private lives and personal attributes.[97] It has been submitted that machine learning has the potential to measure and process certain characteristics from social media profiles and be more fruitful than the traditional limited human processing and bias.[98] A machine-learning system, however, may be inaccurate where the data it is given is too narrow and may therefore be unable to make accurate predictions.[99] Underrepresented data could lead to discrimination where under-inclusive information about certain groups of people has been collected and processed.[100] Similarly, data that is overrepresented to a machine-learning

89 Yanisky-Ravid and Hallisey 2019 *Fordham Urban Law Journal* 428 441.
90 Weaver 2018 *Richmond Journal of Law & Technology* 1 47.
91 Hildebrandt 2018 *University of Toronto Law Journal* 12 27.
92 Katyal 2019 *University of California Law Review* 54 68–69.
93 Yanisky-Ravid and Hallisey 2019 *Fordham Urban Law Journal* 428 440.
94 Yanisky-Ravid and Hallisey 2019 *Fordham Urban Law Journal* 428 443.
95 Raub "Bots, Bias and Big Data Artificial Intelligence, Algorithmic Bias and Disparate Impact Liability in Hiring Practices" 2018 *Arkansas Law Review* 529 530.
96 Yu 2020 *Alabama Law Review* 188 203–204.
97 Dattner *et al* 2019 *Harvard Business Review*.
98 Zhang *et al* 2020 *Journal of Applied Psychology* 1530 1544.
99 Katyal 2019 *University of California Law Review* 54 70.
100 Yanisky-Ravid and Hallisey 2019 *Fordham Urban Law Journal* 428 449.

algorithm may also unfairly scrutinise a particular group and create bias towards that group.[101] The potential effect is that an AI system distinguishes between "safe" people and those to avoid when filtering data and could place candidates in certain categories such as good or bad employees.[102] Hence, AI systems have become powerful filtering tools, sorting and categorising persons in many areas, and their influence and dominance will surely continue to grow in significant and unpredictable ways.

It is therefore imperative that accurate data be coded in these machines so that discrimination may be avoided. Other than biased processing of information, data that is generated and stored may relate to personal information (including owner identity, health and biometric data) and this information is susceptible to cyber-attacks or breaches of privacy.[103] Employers making use of AI systems will therefore need to take into consideration various legal implications if they fail to properly code their algorithms, as well as safeguard the interests of its data subjects.

Forbes argues that unemployment rates are high and there is a risk that employers cannot fill positions or that they fill positions with the wrong employees, both of which may drain the company of its resources. AI could empower recruiters and employers to make smarter hiring decisions.[104] Conversely, however, algorithms used by AI may lead to certain negative consequences, especially where it collects private data from social networks.[105] AI tools have given corporations an unprecedented power to make decisions based on data collected, thereby giving insights into candidates for job positions.[106]

Since the significant impact of AI on technology, companies have begun to use its services for hiring employees.[107] AI therefore has the potential to gather personal data about prospective employees and process this to an employer's satisfaction in screening a candidate for a specific job. As can be seen from earlier discussions, AI may generate thorough information relating to private details found on social networks and provide detailed feedback and backgrounds on employees for hiring purposes. The idea behind using AI technologies is that a large number of resumés may be uploaded to an employer's database and AI may quickly process these applications and forward top candidates to the employer.[108] AI tools have the ability to disrupt the recruitment and assessment process, which leads to issues regarding

---

101 Katyal 2019 *University of California Law Review* 54 74.

102 Yanisky-Ravid and Hallisey 2019 *Fordham Urban Law Journal* 428 445.

103 Tschider 2018 *Denver Law Review* 87 93–94.

104 Rogers https://www.forbes.com/sites/forbestechcouncil/2018/06/12/the-key-role-evolving-ai-will-play-in-tech-hiring-and-firing/#614fc4b4b32b. The author suggests that AI can generate detailed assessments on potential candidates by using a wide variety of data and linking the data received with the job specifications. This arguably makes AI more efficient and effective than human recruiters.

105 Raub 2018 *Arkansas Law Review* 529 530.

106 Dattner *et al* 2019 *Harvard Business Review*.

107 Raub 2018 *Arkansas Law Review* 529 537.

108 Dastin "Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women" (10 October 2018) *Reuters* https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G (accessed 2020-04-01).

their accuracy, ethical, legal, and privacy implications.[109] Katyal importantly reveals that although AI may create the impression of autonomy, its actions are actually dependent upon the code that humans write for it.[110]

In traditional recruitment, one would usually advertise a job, receive applications, shortlist prospective candidates, arrange interviews, and finally employ the individual.[111] It is not uncommon for recruiters to use social media as a means to screen prospective employees because the information found on these networks gives companies an insight into the candidate that they would never find during an interview nor glean from a curriculum vitae.[112] Authors have submitted that recruiters use various platforms to screen prospective employees and using social media platforms in the recruitment process has increased in popularity.[113] In a recent online article, BusinessTech published details about South African employers screening social media posts of possible job candidates and explained what the employers were looking for.[114] The article explains that recruiters often face the danger and difficulty that candidates misrepresent their professional, criminal and academic backgrounds in order to get an available employment position and this undermines the recruitment process. Employers therefore seek to use social media to check certain posts and it has been revealed that many social media users were found to have posted "negative content" that would be seen as unprofessional, as these posts involve discriminatory comments, defamatory content, sexual images or potential drug abuse. Employers therefore engage in these background checks to ensure responsible hiring decisions that will mitigate financial and reputational harm to their organisations.

LinkedIn is an example of a social media website. It is considered a social network site where professionals may connect in the workplace and recruiters may find suitable candidates for employment positions.[115] These types of social media platforms allow users to upload information regarding their qualifications, work experience, and skills, which significantly increases the probability of employers finding a required match for a job opportunity.[116] Not all social media, however, is created for the professional purpose of employment opportunities.

---

109 Dattner *et al* 2019 *Harvard Business Review*.

110 Katyal 2019 *University of California Law Review* 54 62.

111 Ruparel, Dhir, Tandon, Kaur and Islam "The Influence of Online Professional Social Media in Human Resource Management: A Systematic Literature Review" 2020 *Technology in Society* 1.

112 Potgieter *Social Media and Employment Law* 38.

113 Ruparel *et al* 2020 *Technology in Society* 1.

114 BusinessTech "South African Employers Are Screening Your Social Media Posts: Here's What They're Looking Out For" (23 March 2021) https://businesstech.co.za/news/internet/477804/south-african-employers-are-screening-your-social-media-posts-heres-what-theyre-looking-out-for/ (accessed 2021-03-24).

115 Potgieter *Social Media and Employment Law* 14. On LinkedIn, a user can create and upload a profile and a curriculum vitae, which others can view. Personal information is contained on the user's page, such as employment history, relevant skills, degrees and work experience.

116 Ruparel *et al* 2020 *Technology in Society* 2.

Social media gives AI a perfect platform from which to collect and process information regarding employees as all the information is already kept in one place. AI can use its algorithms to screen employees on LinkedIn and select suitable candidates for employers. AI thus replaces those recruiters who would normally search and sift through all the online profiles. There are risks attached to screening social media profiles, including bias or discrimination, because the information is intended on being private and may not be relevant to the workplace.[117] Two negative implications can arise from using AI algorithms; first, incorrect data could be collected in the processing of data, leading to inaccuracies when providing feedback; secondly, the AI could be programmed or coded in such a way that it discriminates or creates some form of bias when processing data (for example, it could process that men are more likely to get promoted than women and consequently exclude all females from the process).[118] In other words, although an AI system may be programmed in a particular way, it may fail to accomplish its set goals and prove to be affirmatively harmful towards others.[119] Arguably, a candidate's personal affairs should not affect his or her job qualifications, skills and ability to fill the position.[120]

In order to programme an AI system to find prospective employees, the system is given a database of the CVs of past candidates (both successful and unsuccessful) and this data allows machine learning to determine a formula to screen future candidates.[121] Scholars have argued that cognitive ability and intelligence testing are a reliable means of predicting job success in occupations, but these assessments may also be discriminatory if they adversely impact certain protected groups, such as those defined by gender, race, age, or national origin.[122] This is because AI systems are based on combining past data and providing their own definition of success, which may not be objective and may create bias or discrimination.[123] In order for employers to use AI tools successfully in recruiting or firing employees, the employer must prove that the assessment process is job-related and predictive of success for that specific job.[124] There have been occasions where AI algorithms and face-recognition systems have been found to be discriminatory or show bias towards others.[125] For example, Amazon's AI technology was found to be discriminatory because it had taught itself that male candidates were preferable to female ones; it was therefore not

---

117 Potgieter *Social Media and Employment Law* 38. The author argues that the interview process should remain objective and the private and social information of a candidate may affect this process.

118 Katyal 2019 *University of California Law Review* 54 68.

119 Gravett "The Dark Side of Artificial Intelligence: Challenges for the Legal System" 2020 *Southern African Public Law* 1 17.

120 Potgieter *Social Media and Employment Law* 38.

121 Brownlie "Encoding Inequality: The Case for Greater Regulation of Artificial Intelligence and Automated Decision-Making in New Zealand" 2020 *Victoria University of Wellington Law Review* 1 3.

122 Dattner *et al* 2019 *Harvard Business Review*.

123 Brownlie 2020 *Victoria University of Wellington Law Review* 1 5.

124 Dattner *et al* 2019 *Harvard Business Review*.

125 Humble and Altun "Artificial Intelligence and the Threat to Human Rights" 2020 *Journal of Internet Law* 12 13.

gender-neutral in processing the data it received.[126] Depending on how AI systems are set up, they can discriminate against individuals and screen people they do not like or build lists of individuals based on unfair criteria; AI systems therefore need to be programmed in a proper and fair manner.[127]

7 RECOMMENDATIONS AND CONCLUSION

Artificial intelligence is only possible through human creation and development. It is therefore necessary to supplement AI with good training and human intelligence because this will define the parameters (both acceptable and unacceptable boundaries) of the AI as it performs its necessary functions.[128] Bad, incorrect or missing data can lead to wrong decisions and incorrect conclusions reached by the AI system.[129]

Trial or mock runs could also help identify issues within the system. It is clear that organisations wish to protect their images and reputations by searching and hiring the best suitable candidate for the job. While prospective employees also have their right to privacy online, this privacy may diminish online. It is imperative that there is a legal balance in the operation of AI to ensure that technology can enhance the commercial field while respecting and protecting the rights of individuals. Finding this balance, however, may prove difficult, as there will be arguments for and against the proper application of AI. The obvious way to regulate AI is to control the way it is programmed and coded, as this will set the parameters of its data processing and ultimately involve a fair and permissible collection of employees' information. Fairness, however, gives rise to technical challenges in creating decision-making algorithms for AI systems.[130] Programmers of AI systems should seek to create an interface that feeds data pertaining specifically to the job in question and which does not contain biased or irrelevant characteristics based on gender, race, or sexual orientation.[131]

Prospective candidates must also in any event be made aware of monitoring and processing or interception of their information in the workplace. This may be done during the pre-contractual stage or by updating employees on a regular basis through communication such as email.[132] This would ensure that employees are informed at all times and that consent has been given to the lawful processing of their information. In

---

126 Dastin https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

127 Gravett 2020 *Southern African Public Law* 1 16.

128 Hildebrandt 2018 *University of Toronto Law Journal* 12 33–34. The author believes that artificial intelligence may be successfully regulated through a disciplined public administration process so that it aligns with the rule of law. However, the author states that there is no exact procedure to follow to ensure that artificial intelligence embraces the rule of law.

129 Yanisky-Ravid and Hallisey 2019 *Fordham Urban Law Journal* 428 449.

130 Tschider 2018 *Denver Law Review* 87 100.

131 Yanisky-Ravid and Hallisey 2019 *Fordham Urban Law Journal* 428 445.

132 This can be done when applying for a position; for example, when the job is advertised it can be indicated in the advertisement that recruiters or organisations will screen social media profiles of those people being considered for an interview.

some instances, giving notice of privacy breaches is outdated, misleading or difficult to find and the individual is sometimes not given a choice to withhold consent.[133] Transparency requires those in charge of the design and process of an AI system to declare how such systems make a decision, so that the data subject can make an informed decision and understand how the decision was made by the AI system.[134]

The problem facing potential employees who are being considered for a position at a company is how will they be protected from unlawful processing of their data? Tschider submits that a personal data store may be the way forward to process an individual's data lawfully – a system where data is collected from a variety of devices and origins for an individual and allows the user or data subject to make decisions regarding their data.[135] This means the employee can divulge the relevant information and restrict access to other users and also set limitations as to what data may be accessed. The AI will then have all the information in this data store to process, making the process more accurate and individualistic because it has only collected data on that specific employee through that system. This hopes to resolve the issue of discriminatory or biased processing of information. Other authors have argued that a "transparency model" approach should be used in which data users up and down the data supply chain ensure that the data remains in compliance with existing laws.[136] This would mean that AI systems will have to comply with the provisions of POPIA, which it should have to do in any event, as a failure to comply with this legislation would render the collection and processing of data by a company unlawful.

AI needs to be supportive of employer and employee rights. A supportive role by AI will enhance the monitoring system and ultimately lead to fair practices in the workplace. In order to achieve this, the algorithms used in programming must be fair, which is not easy to achieve. Automating the hiring process and replacing human intervention must accordingly be done with caution.[137] Informed employees will have a better understanding of their rights and responsibilities in the workplace pertaining to the use of social media and the monitoring of their personal information. Trust between employer and employee is one of the most important factors influencing a successful employment relationship and the employer must therefore find a balance between monitoring employees and breaching their trust.[138] Although AI may enhance some administrative functions in the workplace, it must be used in the correct manner. Prospective employees should also be made aware of how their information is being collected and processed.

---

133 Tschider 2018 *Denver Law Review* 87 110.

134 Humble and Altun 2020 *Journal of Internet Law* 12 15–16. The authors submit that individuals should be informed before the processing, during the processing and after the decision is made in order to provide complete transparency to the process.

135 Tschider 2018 *Denver Law Review* 87 139.

136 Yanisky-Ravid and Hallisey 2019 *Fordham Urban Law Journal* 428 473. The authors also propose that, based on this model, the data should be audited to ensure that the source, use and contents of the data have been conducted in a lawful manner.

137 Dastin https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

138 Potgieter *Social Media and Employment Law* 35. Excessive monitoring of employees will lead to a breakdown in trust and may lead to more damage in the workplace.

Some scholars have proposed that it must be disclosed to the individual that his or her personal data will become part of a dataset for the purposes of an AI system.[139] Lastly, regular updates or auditing of the AI system should ensure that it is constantly checked for bugs or ways in which the system could be improved.

[139] Humble and Altun 2020 *Journal of Internet Law* 12 15.