AI, Machine Learning & Big Data

2020

Second Edition

Contributing Editor:
Matt Berkowitz

glg global legal group

CONTENTS

South Africa

Fatima Ameer-Mia, Christoff Pienaar & Nikita Kekana
Cliffe Dekker Hofmeyr Inc.

Trends

Terminology

"AI" or "artificial intelligence" is a computer or software system that uses algorithms to make it possible for machines to learn from experience, adjust to new inputs and perform or simulate human-like behaviour or tasks.

"Machine learning" is a method of data analysis that automates analytical model building. It is a branch of artificial intelligence based on the idea that systems can learn from data, identify patterns and make decisions with minimal human intervention.

Computer Business Review (online) defines "big data" as large sets of data that are so large and complex that traditional data processing cannot be used to analyse them. The data sets can be both structured or unstructured and, typically, "big data" analysis finds ways to analyse and extract information computationally to reveal patterns, trends and associations, often relating to human behaviour and patterns.

Trends in South Africa

In many industries in South Africa, there has been a drive towards incorporating big data analysis, artificial intelligence and machine learning into businesses and products to streamline operations, analyse user behaviour and determine or predict potential purchasing behaviour. Below we discuss some key trends within South Africa.

FinTech and InsurTech

In the banking industry, financial institutions are increasingly using big data sets (through AI-enabled software) to improve their analysis of clients' credit scores and subsequent risk profiles for loan considerations, to create value-added services and to improve on existing service offerings. AI software is now able to use big data from a variety of online sources linked to a client, including social media accounts, to build risk profiles and better understand which clients may benefit from or be interested in certain products.

Insurance companies have also been using AI and big data analysis to better analyse their clients' behaviours, better predict risk exposure and create insurance models that address concerns that many clients have had with the industry's lack of transparency and large premiums. A South African-based InsurTech start-up uses AI software with photographic recognition to analyse photographs of items which end-users wish to insure and have submitted via the app. The app is able to identify the item from the photograph and offers the end-user insurance for the identified item.

HealthTech

AI is enabling medical professionals to make faster and more accurate diagnoses and to help more patients in remote, far-to-reach locations in South Africa. South Africa's major medical

insurers are experimenting with big data analytical tools and "chatbots" (that utilise machine learning) to create a more client-centric business model that allows its members to connect information about their healthy habits, such as gym workouts and healthy food purchases, in order to get points and receive rewards, such as discounts on flights. In South Africa, there are also a number of entrepreneurial companies using AI and big data to assist the lifestyle management of certain types of diabetes and conduct genetics analytics. A digital health company in South Africa is using a technology platform that uses AI and machine learning to analyse big sets of data of its public and private sector clients, which then allows these clients to implement and manage their healthcare programs.

AgriTech

In the agricultural sector, a few companies are using drones that use artificial intelligence, machine learning and big data analysis to provide imagery to farmers of their crops, and interpret these images and other related data to provide an analysis about the health of the crops.

Other Technology Trends

There are a number of South African AI start-ups which successfully use AI technology and machine learning. For example, one such start-up focuses on developing AI which helps people work more effectively, rather than replacing them with AI systems. As an example, it provides non-coding businesses with the opportunity to develop "Virtual Adviser Apps", which can provide a business' clients with detailed information about the products that that business offers and can also be developed to assist staff in taking decisions particular to their unique business.

Another successful start-up uses artificial intelligence to assist companies within the manufacturing sector to eliminate defects in their factories and improve yield in the production process, and is the first African machine learning specialist company which provides AI solutions for businesses across the globe.

Whilst South Africa is taking big strides in the AI industry, it is not without challenges. In the South African economy, where unemployment is rife, businesses looking to implement AI systems should be mindful of AI replacing human jobs so as not to negatively affect the economy. AI systems are also expensive to implement, and cost is therefore a challenge (and often a barrier) to many businesses.

Ethical AI

A particularly topical trend at present is ethical AI and how we define what a "good outcome" is when it comes to algorithms. The Centre for Artificial Intelligence Research ("CAIR"), which primarily consists of a collaboration of South African universities research groups, was established with the aim of building world-class AI research capacity in South Africa. The CAIR is tasked with, amongst other things, investigating ethical use of AI. In the absence of any policy or regulatory standards regarding ethical AI, it is up to the coders and creators to act ethically and to self-regulate (as such).

Ownership/protection

When a company creates an AI algorithm, who is the owner?

An AI algorithm, or more specifically the written code, encompassing both the program's source code and object code would be categorised as a "computer program" in South Africa and is protected by the law of copyright. The point of departure in the law of copyright is that ownership of original work shall vest in the author, or in the case of joint authorship, in the co-authors of the work. It is therefore critical to identify who the author is. In respect of

a computer program, the Copyright Act 98 of 1978 ("Copyright Act") states that the author is the person who exercised control over the making of the computer program. Where the work is created in the course and scope of employment (whether under a contract of service or apprenticeship), the employer will hold the copyright. Where a computer program has been commissioned, the person commissioning the work would be the author; i.e., where a company has commissioned a developer to create an AI algorithm, the author and therefore owner of the copyright would be the company that commissioned the work, and not the developer (unless stated otherwise in an agreement). See also the section below on copyright.

A more interesting legal question is: who owns the work that an AI machine may create?

In South Africa, the Copyright Act defines an "author" in relation to various works as "the person". The only exception is in respect of a "published edition" which refers to the "publisher" as the author (and does not explicitly refer to a "person"). Considering that all the other definitions refer to "the person", we do not think that it was the drafter's intention to treat the authors of published editions differently to other works and that this is likely just a result of poor drafting. A "person" is not defined in the Copyright Act, and as such we must revert to the rules of statutory interpretation which suggest that a purposive interpretation should follow when a literal interpretation is not possible. The ordinary literal dictionary meaning of a "person" is "a human being regarded as an individual" (*Oxford English Dictionary*). However, both natural and juristic persons are eligible for ownership rights in copyright, so a literal interpretation does not assist us in this instance. Upon a purposive interpretation, we are of the view that the intention of the legislature when drafting the Copyright Act was for legal persons (including both natural and juristic persons) to receive protection under the Act – however, it is unlikely that the legislature anticipated the concept and technology in respect of AI when drafting such provisions, and therefore it is unlikely that the intention of the legislature was for a machine to enjoy copyright protection and ownership.

If the machine is truly autonomous, the work is technically "original" (and not commissioned) as the work would be machine-learned from a series of data inputs. In some instances, the company and/or person feeding the data (inputs) may not know what the output will be – work could therefore be an incidental creation. However, in other instances, the work may be "commissioned" and the copyright vests with the person who commissions such work.

Policy and laws have yet to keep up with the rapidly changing technology landscape. This ownership conundrum is another legal lacuna to which there is no exact answer and would largely depend on the facts and circumstances at hand.

What intellectual property issues may arise regarding ownership?

Ownership issues which may arise include conflicting claims in situations where intellectual property is unregistered. For example, technology may be developed simultaneously but by separate parties or co-developed; and once brought to market, issues around where ownership rights are attached could be of concern.

How are companies protecting their technology and data?

Depending on the type and form of technology, there are various ways to protect one's intellectual proprietary interests in South Africa, including: non-disclosure agreements ("NDAs"); copyright; trade marks; and patent protection.

NDAs

Confidentiality agreements (or NDAs) are almost standard practice in respect of any technology services arrangements and are often concluded as standalone agreements well in advance prior to any technology services agreement being concluded. The purpose of

an NDA is to protect the proprietary and confidential information of the disclosing party. Companies may require developers, employees and third-party suppliers to sign such NDAs prior to having access to such information.

Copyright

Copyright in South Africa is regulated by the Copyright Act and automatically subsists in original works, eligible for protection, created by a qualified person or which were first published in South Africa or another country to which protection is extended. Under the Copyright Act and for a work to be eligible for copyright, it must (i) fall within one of the recognised types of work, (ii) be original, and (iii) be captured in a material form. As stated above, an AI algorithm would be categorised as a "computer program" in South Africa and is protected by the law of copyright.

It is important to note that copyright is territorial in nature. If the work is first published in South Africa, or any one of the owners (authors) is a South African citizen or is domiciled or resident in South Africa (in the case of an individual), or, in the case of a juristic person, is incorporated in South Africa, then the Copyright Act and common law rules afford protection.

However, where a work was first published outside of South Africa or the owners (authors) are not South African citizens, residents or domiciled or incorporated within South Africa, then the work would need to qualify for protection on the basis of the protection being extended to the relevant country by virtue of public international law. South Africa is a signatory to the Berne Convention for the Protection of Literary and Artistic Works of 6 September 1886 ("Berne Convention"). The Berne Convention provides that works must be afforded equal protection in the signatory state as its own copyrighted works. Although a signatory to the Berne Convention, South Africa is, however, not a signatory to the World Intellectual Property Organisation Copyright Treaty of 20 December 1996, which essentially extends the protection of literary and artistic works under the Berne Convention to computer programs. Consequently, copyrights in "internationally created" computer programs are not explicitly recognised in South African law.

Moral rights

Additionally, and separate from an author's copyright, moral rights exist in South Africa to protect certain categories of works. Moral rights include the right to paternity (i.e., the right to claim authorship of the work) and the right to integrity (i.e., the right to object to any distortion or modification of the work where such is derogatory, prejudicial or may cause prejudice to the author). Moral rights are personal rights which attach to the author and exist to protect the integrity and ownership of their work. Moral rights cannot be assigned due to their personal nature, but can be waivered, and should be done so in writing. It is important to bear in mind that a moral right can only subsist in a work if such work enjoys copyright protection in South Africa in the first place.

Trade marks

A trade mark is a word, symbol, phrase or device which identifies the services or goods of one person and distinguishes it from the goods and services of another. It has become popular to give AI software human-like names (e.g., Sophia and Robot Lawyer Lisa), catchy, easy-to-remember names or easily identifiable symbols. To obtain trade mark protection, the mark must: (i) be distinguishable; (ii) not confuse consumers about the relationship between one party and another; and (iii) not otherwise deceive consumers with respect to the qualities of the product.

Trade marks can be registered or unregistered. Unregistered trade marks are protected under common law, in particular the law of delict (tort). Registered trade marks are regulated and

protected by the Trade Marks Act 194 of 1993 ("Trade Marks Act"). It is worth noting that ownership of a registered trade mark is established on a first-to-use basis rather than first-to-file. Registration of a trade mark is not mandatory to establish rights, but a registered trade mark makes proof of ownership easier in the case of infringement. Registration under the Trade Mark Act is *prima facie* proof of ownership and validity. A registered trade mark can be protected forever, provided that it is renewed every 10 years.

Unregistered trade marks are protected under the common law and an applicant would claim for "passing off" under the law of delict for the infringement of its goodwill. The delict of passing off consists of a representation, direct or indirect, by a manufacturer or supplier that his business or goods (or both) are those of a rival manufacturer or supplier. This is often more difficult to prove, as an applicant must show that: (i) the name, get-up or mark used by the applicant has become distinctive of his goods or services; and (ii) the name, get-up or mark used by the respondent is such or is so used as to cause the public to be confused or deceived into believing that the respondent's goods or services emanate from the applicant.

It is important to note that trade mark protection is territorial and that trade marks registered in other jurisdictions are only recognised insofar as they constitute "well-known marks" under the Trade Marks Act.

Well-known marks are protected under the Paris Convention on the Protection of Industrial Property of 20 March 1883 ("Paris Convention") and section 35 of the Trade Marks Act. Whether a mark is "well-known" or not will depend on the knowledge of the trade mark in the relevant sector of the public, including the knowledge which has been obtained as a result of the promotion of the trade mark. If a trade mark is determined to be "well-known", it will receive protection only if the owner is a resident of a nation, domiciled or has real and effective industrial or commercial establishment in a country which is a Paris Convention signatory.

Patents

A patent is a certificate in a prescribed form to the effect that a patent for an invention has been granted in the Republic. Patent protection is granted for a limited period of 20 years. The Patents Act 57 of 1978 ("Patents Act") defines the scope of patentable inventions and explicitly states what cannot be patented. Presently, the Patents Act explicitly excludes a "program for a computer" from the definition of invention and thus from being patentable. It may be in the future that, as in other jurisdictions, the law is developed to accommodate software patents. However, the hardware design that complements the software can be patented as an industrial design.

What are the applicable laws with respect to data ownership, security and information privacy?

Data ownership

Data is arguably one of the most valuable assets in today's world. Data is an intangible asset capable of being commoditised, owned and sold. Ownerships depends on from where it originates and the form it takes. Certain data constitutes personal information and shall be regulated by data protection laws including the Protection of Personal Information Act 4 of 2013 ("POPI").

Information privacy

The right to privacy is enshrined in section 14 of the Constitution of South Africa, 1996 and states that "everyone has the right to privacy, which includes the right not to have the privacy of their communications infringed". In order to give effect to the right to privacy, POPI

was promulgated. POPI is data protection legislation primarily modelled on the European Union general data protection laws. Importantly, it establishes the Information Regulator and confers various powers, duties and functions, including monitoring and enforcing compliance by public and private bodies and handling complaints in respect of contraventions of POPI. It also establishes a comprehensive compliance framework and places cybersecurity obligations on responsible parties to secure the integrity and confidentiality of personal information in its possession or control by taking appropriate, reasonable, technical and organisational measures to prevent unlawful access. Whilst POPI has been promulgated into law, the substantive provisions of POPI are not yet in effect (only the provisions relating to the establishment of the Information Regulator and procedure for making regulations are currently in effect). The commencement date of these provisions of POPI will need to be determined by the President, but this is likely to be later in 2020. Once POPI comes into effect, parties shall have a one-year grace period to comply with it.

Not all data processed in an artificial intelligence or big data context involves personal information and human interaction, but a large spectrum of it does, and this has a direct impact on individuals and their rights with regard to the processing of personal information. Typical AI applications make it possible to collect and analyse large amounts of data in order to identify attitude patterns and predict behaviours of groups and communities. The risks related to the use of data in this context is also to be considered. For example, POPI, as does the GDPR, also requires responsible parties (data controllers) to clearly disclose the purpose for which collected data will be used. The use of AI potentially exposes data subjects to different risks or greater risks than those contemplated initially, and this could be considered as a case of further processing personal information in an unexpected manner. AI produces profiles and decisions that are based not just on data that a data subject has consensually submitted, but on data sometimes obtained without the knowledge or consent of a data subject.

Information security

At present, the current legal framework relating to cybercrime and cybersecurity in South Africa is a hybrid of different pieces of legislation and the common law, which has not kept up with the dynamic nature of technology and international standards. This prompted the drafting of the Cybercrimes Bill [B6-2017] ("Cybercrimes Bill") which will, *inter alia*, consolidate and codify numerous existing offences relating to cybercrimes, as well as create a variety of new offences which do not currently exist in South African law. Before the Cybercrimes Bill becomes law, it will need to be passed by both houses of parliament, undergo a public participation process and receive presidential assent. At the time of writing (March 2020), the Cybercrimes Bill remains with the selection committee in one of the houses of parliament which is processing responses to public submissions made to it.

However, until the Cybercrimes Bill becomes law, most cyber-related crimes, such as hacking and phishing, are regulated under the Electronic Communications and Transactions Act 25 of 2002 ("ECT Act"). It is important to note that once the Cybercrimes Bill is in effect, it will repeal the relevant provisions in the ECT Act relating to cybercrime offences and cybersecurity.

Antitrust/competition laws

Internet access is a critical aspect to enable growth in big data analytics, artificial intelligence and machine learning. Currently in South Africa, a significant portion of internet traffic in South Africa is through mobile data. The cost of mobile data in South Africa has been historically high when compared to other countries. Cable.co.uk ranks South Africa 143rd in the world in terms of mobile data costs. However, this is likely to soon change as the South

African Competition Commission conducted a formal market inquiry into data services and ordered two of South Africa's biggest mobile operators to drastically reduce their data prices and has also been conducting a formal market inquiry into data services. The decrease in mobile data costs will help bolster the amount of data available for big data analytics within South Africa and increase the customer base for apps using AI and machine learning.

As seen above, competition law is well established in South Africa. The South African Competition Commission is very proactive in enforcing the Competition Act 89 of 1998 ("Competition Act") and trying to facilitate market growth and fairness in South Africa. Competition law is well established in South Africa, and the South African Competition Commission is very proactive in enforcing the Competition Act. For instance, according to its annual report for the financial year 2018/2019, the Competition Commission levied administrative penalties to the value of 333 million Rand (approximately €18.24 million).

The Competition Act prohibits certain activities amongst competitors (horizontal relationships) and amongst a firm and its suppliers and/or its customers (vertical relationships).

For horizontal relationships, activities such as price-fixing, collusive tendering and market division between competitors are prohibited. More broadly, any agreement or concerted practice by firms or an association of firms that have the effect of substantially preventing, or lessening, competition in a market are prohibited, unless a party to the agreement, concerted practice, or decision can prove that any technological, efficiency or other pro-competitive gain resulting from it outweighs that effect.

For vertical relationships, any agreement between parties is prohibited if it has the effect of substantially preventing or lessening competition in a market, unless a party to the agreement can prove that any technological, efficiency or other pro-competitive gain resulting from that agreement outweighs that effect. This includes a supplier of goods imposing a minimum resale price to firms purchasing and on-selling their goods and/or services.

What happens when machines collude?

Machine collusion will mainly arise in horizontal relationships and could arise in a number of different contexts.

For instance, two competitors may both utilise software that uses price algorithms to determine the price of a particular type of good or service; e.g., a new camera. If the software is given the capabilities to interact with each other, or, if they have a sophisticated program through which, using machine learning, they can develop these capabilities, then it is theoretically possible that they may "collude" and simultaneously increase the price of the camera in order to ensure that both firms make a greater profit without the risk of losing business to their competitor.

Currently, the Competition Act does not expressly deal with machine collusion. However, the Competition Act does state that a firm is held directly liable for prohibited activities where its employees, staff and directors are involved in prohibited activities on its behalf. Thus, we are of the view that where machines, owned and under the control of and/or instructed by a company, engage in prohibited and anti-competitive activities, our law shall similarly hold the company/companies directly responsible and liable.

What antitrust (competition law) concerns arise from big data?

With the ever-increasing analysis capabilities of big data, firms can successfully utilise data that was previously too large and unrefined to come up with strategies to improve their business model and analyse the market in which they operate in more depth.

This has the potential to have positive effects by increasing the level of competition in a particular industry and allow market disruption with new entrants. Smaller firms and new

entrants can use big data analysis to successfully analyse gaps in the market. Businesses can also, through big data analysis, address consumer dissatisfaction and obtain information previously unknown to both the customer and the business.

For example, in South Africa, one of the newer banks was able to gain significant market strides in the banking sector by successfully identifying a gap in the market; i.e., because customers with lower incomes were not opening bank accounts because the monthly bank fees were too expensive, the bank then came up with a price-per-transaction model that encouraged these customers to open an account.

Companies need to also be conscious of the data analysis and even raw big data that they share with others within the same industry. This is because the Competition Act prohibits the sharing of information between competitors if it has the effect of substantially preventing or lessening competition in a market (unless its technological, efficiency or other pro-competitive gains resulting from such sharing outweighs that effect).

For example, if different companies are all members of an industry body, and at one of these industry body meetings, commercially sensitive information of the competitors (even if it is only large volumes of raw data) is shared, then these companies run the risk of violating anti-competitive laws.

Board of directors/governance

What governance issued do companies need to be aware of, specific to AI and big data?

Companies, more particularly the board of directors of the company, need to ensure effective and secure data management when implementing AI and utilising big data sets. Directors owe certain fiduciary duties to the company and must understand and ensure data is lawfully obtained, stored and used within a specified purpose. Companies will adopt and rely on AI-enabled technology to improve decision-making and management, but it is critical to note that the ultimate responsibility and oversight duties still reside with the board and individual directors. Unless the Companies Act 71 of 2008 ("Companies Act") or common law is developed to provide otherwise, AI and big data will play a supporting function for more effective governance.

The King IV Report on Corporate Governance for South Africa – 2016 ("King IV") is a set of voluntary principles in the area of corporate governance. Companies listed on the Johannesburg Stock Exchange are required to comply with King IV by law. In particular, King IV has a specific focus on the oversight of information and technology management. The board of the company is specifically tasked to make sure it proactively monitors cyber incidents and ensure that it has systems and processes in place from a cybersecurity perspective. Failure by a company to prevent, mitigate, manage or respond to an incident amounts to a breach of directors' duties, both under the common law and the Companies Act.

Under the common law, a breach of fiduciary duties may apply, and the director can be held liable for any losses, damages or costs. Section 76 of the Companies Act sets out standards of directors' conduct, and that a director must always act in good faith, for a proper purpose, in the best interest of the company and with a degree of reasonable care, skill and diligence. Failure to prevent, mitigate, manage or respond to an incident may amount to a breach of directors' duties under the Companies Act.

How does AI and big data affect the due diligence process for boards of directors?

AI has the capability to reduce the workload of a director and make working and decision-making more efficient, quicker and arguably cost-effective. For example, AI-enabled technology can scan, process and organise large data sets in a due diligence exercise and

highlight possible risks more quickly than a human would be able to. The director or professional can then interpret those risks and make a judgment call accordingly. Some AI technologies are capable of highlighting risks and offer solutions based on machine learning, which may remove the need for ultimate judgment from a human entirely. However, as discussed above, a director still retains certain duties to the company and would be ultimately responsible for any decision made by a computer program.

How do AI and big data affect a board's fiduciary duties?

The Companies Act imposes a positive duty on directors to manage the business and affairs of the company. As previously discussed, directors have certain duties which they owe to the company, which include common law duties and duties created under the Companies Act: more specifically, the duty to act in good faith and for a proper purpose in the best interests of the company; and also acting with due care, skill and diligence. Directors may, however, delegate all or any of its management powers and authority to some other person and in those matters involving skills or expertise within the delegatee's competence. However, as in the case of delegating to a human, the ultimate duty remains with the instructing director who cannot shirk his or her fiduciary duty through delegation. Directors will retain the ultimate management function even where a power has been delegated.

AI will certainly permeate the board room, but it is unlikely that South Africa will witness robo-director appointments anytime soon. Only natural persons may serve on the board of directors of a company. Therefore, it is not possible for a robo-director (or AI program) to be appointed to the board.

Regulations/government intervention

Specific laws relating to AI, big data or machine learning in South Africa

AI and machine learning

Unlike other jurisdictions, South African regulators have not yet caught up with the rapid pace of AI technology. South Africa has not yet formalised any policy documents or entered bills to parliament for the regulation of AI. However, the President has appointed members to the Presidential Commission on the Fourth Industrial Revolution ("4IR Commission"), which will assist the government in taking advantage of the opportunities presented by the digital industrial revolution. The task of the 4IR Commission, which will be chaired by the President, is to identify relevant policies, strategies and action plans that will position South Africa as a competitive global player. In late 2019, the 4IR Commission submitted a draft diagnostic report to the President regarding South Africa's 4IR plan and identified available opportunities. The final report is expected to be presented to cabinet in 2020.

Although AI and machine learning are not yet specifically regulated, there are signals that government is building the groundwork for implementation across various industries. For example, in late 2019 the South African regulator responsible for, among other things, the licensing of spectrum surprised the telecommunications industry by publishing a memorandum on the licensing of those parts of the spectrum required to enable 5G. The memorandum invited interested parties to submit their views of the licensing for radio frequency in the ranges of 700MHz and 800MHz, 2.3GHz, 2.6GHz and 3.5GHz by the end of January 2020. Access to 5G technology will allow for industries to explore further AI capabilities and we anticipate interesting new business opportunities shall arise as a result.

Big data

"Big data" as a concept is not specifically regulated, but to the extent that a party wishes

to analyse data sets which include personal information, POPI will be applicable (once commenced). POPI imposes various conditions which must be complied with in respect of the lawful processing of personal information. Personal information can only be processed if, *inter alia*, the data subject consents to the processing, processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party, or processing is necessary for pursuing the legitimate interest of the responsible party. Therefore, a party wishes to use process personal information will need to consider what the implications are from a data protection perspective.

Implementation of AI/big data/machine learning into businesses

What are the key legal issues that companies need to be aware of?

To keep abreast of the trends in their industries, maximise revenue and better understand their consumers, most businesses are increasing their use of AI, big data and machine learning.

When utilising these technologies, one of the most critical legal issues that all businesses should consider is data protection law, which is primarily covered by POPI. As mentioned above, personal information may only be processed for a specific, explicitly defined and lawful purpose (such as where a data subject's consent has been obtained).

Often, businesses wish to utilise big data analysis and AI to further process personal information. An example of this is where a financial provider utilises AI software to analyse which of its customers have mortgage bonds, and then offers such customers its household insurance. This would not be in line with the original purpose for which this information was provided (i.e., so that the customer can take out a home loan); therefore, this further process must be legally justifiable under one of the recognised grounds under POPI.

Businesses are encouraged to review their policies and agreements with customers and their suppliers to ensure that they comply with POPI.

POPI also requires businesses to secure the integrity of personal information in their possession or under their control with appropriate and reasonable technical and organisational measures to prevent the loss of, damage to or unauthorised destruction of personal information, and unlawful access to or processing of personal information. With businesses storing more big data than ever before, a data breach can have devastating consequences and expose a business to significant civil liability as well as administrative penalties. Thus, it is important that businesses ensure that they have in place proper security measures which adhere to international best practice.

Civil liability

What are liability considerations when using AI technology? Where does the liability fall when AI fails?

In South Africa, civil liability can be divided into contractual and delictual (tort) liability. Currently, AI is not recognised as having its own civil liability.

In order for a plaintiff to establish a civil liability claim, such plaintiff must establish that the defendant acted negligently or with intention. An exception to this is strict liability, a common example of which is vicarious liability in employment relationships. In these instances, an employer (often a legal entity) is held liable for its employees' acts (or omissions) that are performed in the course and scope of their employment, which result in delict being committed; e.g., where a construction worker negligently drops a pile of bricks on someone passing the construction site, seriously injuring them.

We are of the view that persons utilising AI technology will similarly remain responsible even in the absence of fault (strict liability) for delicts and their lack of fulfilment of their contractual obligations due to the AI technology.

In South Africa, it is customary for information technology ("IT") contracts that include a service or the licensing of certain software to contain the following warranties that the service provider shall perform:

- their obligations in a professional manner; and
- in accordance with the relevant service levels.

Service levels are targets used to measure or to track the performance of a system and/or service. Service levels in a contract are usually accompanied by service credits. Service credits are deductions from the amount that a client shall pay to a service provider under a contract due to a failure to meet a service level. Thus, if a service level is not met regardless of whether or not AI technology was used, the relevant service credit shall apply and the service provider shall remain contractually liable. Similarly, where a service provider has indemnified a client for a loss due to using its services/system, then it shall remain contractually liable to that indemnity even if AI technology is used.

Sometimes, a service provider may not be the creator or developer of the AI technology. In such instances, where the AI technology fails, it may be possible for a service provider to claim for damages/losses from the developer where its contractual agreement with the developer has warranties or indemnities similar to those in the preceding paragraphs or other liability provisions.

Where the client is a natural person or a small juristic person (consumer), they may also be able to hold both the service provider and developer liable under the Consumer Protection Act 68 of 2008 ("CPA") where the AI technology is considered unsafe, defective or of a poor quality. This is because the producer, importer, distributor and retailer are all deemed to include an implied warranty of quality under the CPA. The CPA also contains a similar right to quality services for a consumer. This is, however, confined to the supplier (i.e., service provider).

What impact does AI have on negligence and malpractice?

It is also likely that in malpractice suits, a person that used AI technology, even where such software is unsupervised, will not readily escape liability as a court is likely to find them negligent (i.e., having not acted in accordance with the reasonable person standard or failing to perform a duty of care or adhere to a professional standard) on the basis that they used the technology without the proper level of care and oversight expected by a reasonable person in their position, or that a reasonable person would not have found the technology appropriate and/or of the acceptable standard for the task that it was used for. In professions such as healthcare and law, whilst AI technology can greatly assist in the generation of faster results, the results would still need to be interpreted by the relevant healthcare practitioner or legal practitioner and cannot be relied on in isolation. Failure to exercise this level of oversight by the relevant practitioner may be a breach of a professional duty, and liability would then attach to the relevant practitioner.

Criminal issues

What if an AI robot or system commits a crime directly?

CR Snyman (2015) Criminal Law, 6th Ed. identifies that most crimes in South Africa have a few essential requirements, namely:

- conduct;
- causation;

- unlawfulness;
- capacity; and
- fault (either intention or negligence).

Where a machine has "committed" a crime such as fraud, under current South African law, that machine shall not itself be found guilty of the crime. This is because current law only recognises conduct that was carried out by human beings as crimes.

Machines also cannot be found guilty of committing a crime, because, like animals and inanimate objects, they are not deemed to have the legal capacity to commit any crime. Where the fault requirement is intention, South African law has not yet developed to recognise a machine, that would likewise not be considered able to act with a direction of its will, as having committed a crime.

Even the Cybercrimes Bill (not yet in effect in South Africa), which seeks to revolutionise the criminal law landscape in South Africa by creating crimes such as cyber fraud and cyber extortion, does not provide for instances where AI (and not a human) is "responsible" for a crime.

Consequently, we are of the view that until South African law is developed to specifically allow for machines to be held directly liable for their crimes, the person who controls and/or instructs the machine would be held responsible for the crime. This view is strengthened by the fact that currently, where an animal is incited by a human to attack another human, it is the human who incited the animal who will be found guilty of committing a crime of assault or murder.

What is not yet clear is how our law shall deal with machines and software that have such sophisticated systems that they are able to independently develop, through machine learning, the capabilities to "commit" crimes without any input from their developers or owners.

What if AI causes others to commit a crime?

It is also possible that AI robots shall cause others to commit crimes.

Renowned author and biochemist Isaac Asimov provides a classic example of this in his book, *The Naked Sun* (1957). A robot unprompted by the perpetrator hands its detachable metallic arm to an enraged but unarmed woman, who in a blind rage strikes and kills a man with the metallic arm.

While we have not yet developed humanoid AI robots to such a level of generalised artificial intelligence and mobility, it is not impossible to imagine instances where AI could enable others to commit crimes. For instance, a piece of AI software could be developed to hack into a website containing financially sensitive information, and then make this information publicly accessible on social media platforms. Persons could then use this information to steal money and unlawfully access other persons' accounts.

For the reasons above, the persons committing the crime and instructing/supervising the machine in its hacking of the website (once the Cybercrimes Bill comes into effect and hacking is a recognised crime) would be held responsible for the crimes.

Discrimination and bias

What laws apply to AI or machine learning systems that produce biased results?

AI is not perfect or impartial. It is possible that biases will exist in the data that AI programs as, in reality, it is a human-built algorithm which will reflect such human bias. For instance, if the training data used in machine learning and/or development in AI programs contains inherent biases this could in turn affect the effectiveness and neutrality of the AI program.

Depending on the context in which such data is used, various anti-discrimination laws may apply, including but not limited to:

- the Constitution, which promotes equality as a central and inalienable right. Unfair discrimination on one of the listed grounds in section 9 is unconstitutional;
- the Promotion of Equality and Prevention of Unfair Discrimination Act 4 of 2000 was promulgated to give effect to section 9 of the Constitution, and to prevent and prohibit unfair discrimination and harassment, promote equality and prevent hate speech;
- the Employment Equity Act 55 of 1998 provides, *inter alia*, that no person may unfairly discriminate, directly or indirectly, against an employee on one or more of the listed grounds; and
- the Competition Act prohibits a dominant firm from discriminating between purchasers of like goods/services in terms of prices charged, if that discrimination leads to an anti-competitive effect. However, conduct involving differential treatment of purchasers is not prohibited if the dominant firm can establish that the differential price makes only reasonable allowance for the difference in costs results from the different method of supply/distribution.

Given South Africa's discriminatory past under apartheid, if South African society is to embrace AI to its full potential, there needs to be trust in the AI programs and the AI solutions produced. An important element of this trust is widespread reliability and a belief in the fairness and authenticity in the results produced using AI and machine learning.

Acknowledgment

The authors would like to thank Lee Shacksnovis, an Associate in the Technology, Media & Telecommunications practice of Cliffe Dekker Hofmeyr, for her contribution to the preparation of this chapter. Lee specialises in commercial, information technology, intellectual property, data protection law and telecommunication law. She has experience in drafting a broad range of information technology and sourcing agreements and regularly advises clients on compliance with privacy laws and data protection regulation in South Africa. Lee has worked in a variety of industries and sectors, both locally and internationally but her interests lie in the financial services and healthcare industry.

Tel: +27 21 481 6453 / Email: lee.shacksnovis@cdhlegal.com

Fatima Ameer-Mia
Tel: +27 11 562 1898 / Email: fatima.ameermia@cdhlegal.com

Fatima Ameer-Mia is a Director in the Technology, Media & Telecommunications practice in Johannesburg. Fatima specialises in commercial, information technology, telecommunications, intellectual property and data protection law. She also has a special interest in the fields of e-commerce, fintech and matters relating to cybercrime and information security. Fatima advises clients, both locally and internationally, on general commercial matters and transactions with a technology related focus – such as software development, licensing, outsourcing, and a wide range of managed services. Her expertise extends to fintech, health-tech, insure-tech and data protection across a diverse range of industry sectors, especially financial services, retail and healthcare.

She regularly advises on data protection and information security, including providing training, seminars, risk assessments and governance frameworks on cybersecurity and data protection laws.

Christoff Pienaar
Tel: +27 21 481 6350 / Email: christoff.pienaar@cdhlegal.com

Christoff Pienaar is a Director and National Head of our Technology, Media & Telecommunications practice. He advises on commercial, information technology and intellectual property law. He specialises in information technology and commercial matters and has particular expertise in payment systems, technology outsourcing, business process outsourcing, systems integration, hardware acquisitions and maintenance, IT consultancy services, managed services, disaster recovery services, software development and software licensing and support transactions.

Christoff also advises on general commercial and intellectual property issues across a diverse range of industry sectors, especially financial services.

Nikita Kekana
Tel: +27 21 481 6334 / Email: nikita.kekana@cdhlegal.com

Nikita Kekana is an Associate in our Technology, Media & Telecommunications practice. Nikita specialises in commercial, information technology, intellectual property and data protection law. Nikita also has a keen interest in artificial intelligence, machine learning and privacy law. Nikita completed her LL.B. at the University of Cape Town in 2016.

Cliffe Dekker Hofmeyr Inc.

11 Buitengracht Street, Cape Town, 8001, South Africa
Tel: +27 21 481 6350 / URL: www.cliffedekkerhofmeyr.com

www.globallegalinsights.com

Other titles in the **Global Legal Insights** series include:

- **Banking Regulation**
- **Blockchain & Cryptocurrency Regulation**
- **Bribery & Corruption**
- **Cartels**
- **Corporate Tax**
- **Employment & Labour Law**
- **Energy**
- **Fintech**
- **Fund Finance**
- **Initial Public Offerings**
- **International Arbitration**
- **Litigation & Dispute Resolution**
- **Merger Control**
- **Mergers & Acquisitions**
- **Pricing & Reimbursement**

Strategic partner