

https://dspace.org/

The current South African legal position on artificial intelligence: what can we learn from the United States and Europe?

Lisinski, Ryszard Paolo

2018

https://hdl.handle.net/10539/27163

Lisinski, Ryszard Paolo, (2018) The current South African legal position on artificial intelligence: what can we learn from the United States and Europe?, University of the Witwatersrand, Johannesburg, https://hdl.handle.net/10539/27163

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

THE CURRENT SOUTH AFRICAN LEGAL POSITION ON ARTIFICIAL INTELLIGENCE: WHAT CAN WE LEARN FROM THE UNITED STATES AND EUROPE?

RESEARCH REPORT

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

By

RYSZARD PAOLO LISINSKI
0317120E

SUPERVISOR: MS VERINE ETSEBETH

28 February 2018

ABSTRACT

As a general rule, law lags behind technology. The exponential growth that is occurring worldwide in the field of artificial intelligence is testing the current regulatory landscape and raising novel legal and ethical issues that have never been contemplated before. Once these issues have been identified and understood, there is no doubt that the current regulatory regime in South Africa will have to adapt to cater for the new status quo.

The United States and the European Union have embraced this technological change and although regulatory progress is slow, the framework has been put in place to understand and meet all of the challenges that come with it. The inroads made thus far serve as an excellent reference point for the South African government to assist it in facilitating a proactive regulatory approach to the AI revolution.

With this in mind, a number of research questions will be set out, acting as the backbone of an analysis conducted on the current regulatory regime in South Africa, the United States, and the European Union. Thereafter, the three jurisdictions will be compared, the lessons learned will be extracted and a conclusion reached on the proposed way forward for South Africa.

TABLE OF CONTENTS

ABSTRACT.....i
LIST OF DIAGRAMS.....iv
LIST OF ABBREVIATIONS.....v
I. INTRODUCTION.....1
II. PURPOSE OF RESEARCH.....3
III. RESEARCH OBJECTIVES.....4
IV. RESEARCH METHODOLOGY.....4
V. SCOPE.....4
VI. LAW TO DATE.....4
VII. LIMITATIONS.....5
VIII. REFERENCING TECHNIQUE.....5
IX. ETHICAL REQUIREMENTS.....5
X. OUTCOMES.....5
XI. OUTLINE.....5
XII. RESEARCH QUESTIONS.....5
XIII. LEGAL POSITION - SOUTH AFRICA.....6
(a) Legal Status of AI.....6
(b) Automated Transactions.....7
(i) Electronic Communications and Transactions Act ("ECTA").....7
(ii) Are automated transactions concluded in these circumstances valid?.....8
(c) Liability Regime.....9
(i) Civil liability.....9
(aa) Automated Transactions - ECTA.....9
(bb) Defective AI - Consumer Protection Act ("CPA").....10
(cc) Medicines and Related Substances Act ("MRSA").....11
(dd) Part 101 of the Civil Aviation Regulations ("PART 101").....11
(ii) Criminal liability and Mens Rea.....12
(d) Privacy.....12
(i) POPI.....13
(e) Intellectual Property.....14
(i) Copyright.....14

(ii) Patents 15
(iii) Ownership of IP created by AI? 15
XIV. LEGAL POSITION – US 16
(a) Legal Status of AI in the US 16
(b) Automated Transactions in the US 17
(c) US Liability Regime 18
(i) Civil 18
(aa) Contract Law 18
(bb) Tort Law 19
(cc) UETA 19
(ii) Criminal 20
(d) Privacy in the US 20
(i) Drones 21
(ii) Autonomous Cars 22
(e) Intellectual Property in the US 22
(i) Copyright 22
(ii) Patents 23
(iii) Ownership 24
XV. LEGAL POSITION – EU 24
(a) Legal Status of AI in the EU 25
(b) Automated Transactions in the EU 25
(c) EU Liability Regime 26
(i) Civil 26
(ii) Criminal 27
(d) Privacy in the EU 28
(e) Intellectual Property in the EU 29
(i) Copyright 29
(ii) Patents 30
(iii) Ownership 30
XVI. FINDINGS 31
XVII. CONCLUSION AND THE PROPOSED WAY FORWARD FOR SA 32
BIBLIOGRAPHY 34

LIST OF DIAGRAMS

Diagram 1 Illustration of the progression of AI over the last five decades.

Diagram 2 Illustration of the interaction between AI, ML, and DL.

LIST OF ABBREVIATIONS

AI	Artificial Intelligence.
COPP	California Online Privacy Protection Act, 2003.
CPA	Consumer Protection Act, No. 68 of 2008.
DL	Deep Learning.
ECTA	Electronic Communications and Transactions Act, No. 25 of 2002.
E-Sign	Electronic Signatures in Global and National Commerce Act, 2000.
EU	European Union.
FAA	Federal Aviation Administration.
GDPR	General Data Protection Regulation 2016/679 [2016] OJ L119/1.
IP	Intellectual Property.
ML	Machine Learning.
MRSA	Medicines and Related Substances Act, No. 101 of 1965.
PART 101	Part 101 of the Civil Aviation Regulations, 2015.
POPI	Protection of Personal Information Act, No. 4 of 2013.
UETA	Uniform Electronic Transactions Act, 1999.
USPA	U.S. Patent Act, 35 U.S.C.
US	United States.

I. INTRODUCTION

A short while ago, the world was faced with a regulatory conundrum when the internet revolutionised our daily lives and in particular, the way business is conducted.[1] Since then, we have learned to deal with the unique cyber law issues that arose as a result of this novel form of technology, and we have found ways to regulate them. In the same vein, it is likely that the equally challenging legal issues that flow from the prolific rise of Artificial Intelligence ("AI") will similarly be understood and regulated over time.

Given that AI is very broad in its application, it is immensely challenging to define concisely. In very basic terms, AI is a computer system or software that mimics human thought processes and behaviour with the aim of assisting and in some instances replacing humans in certain business and social environments.[2] The rapid progression of AI and particularly AI software, over the last five decades, is depicted in the diagram below.

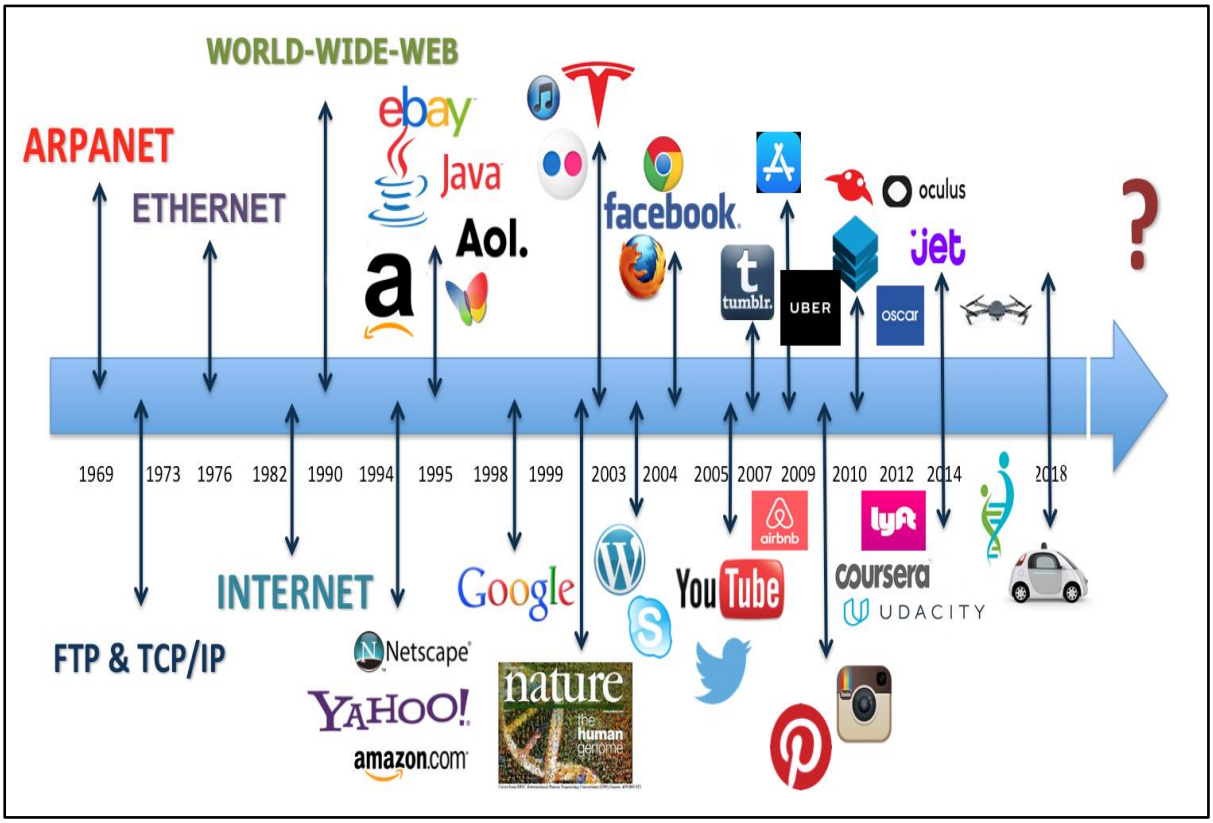


Diagram 1. Illustration of the progression of AI over the last five decades.[3]

[1] R Calo 'Robots in American Law' (2016) University of Washington School of Law Research Paper No. 2016-04, 3.
[2] R Kouatly et al. 'Lebanon Chapter' in A Bensoussan et al. (1st Ed) *Comparative Handbook: Robotic Technologies* Law (2016) 216.
[3] 'Technology 2018', <http://www.aurametrix.com/blog>.

AI is widely used for everyday tasks such as browsing the internet and communicating via social media.[4] Whilst doing so, consumers use AI software designed to interpret data and to "learn" from experience.[5] This subcategory of AI is commonly referred to as Machine Learning ("ML").[6] Real world examples of ML are Facebook Newsfeeds that use data collected to predict what articles you will like and Google Maps applications that use traffic information to guide you home via the most efficient route.[7]

In addition, AI manifests itself in sophisticated machines such as drones, robots and smart cars, which are being developed, tested, and sold at a rapid rate.[8] The more technologically advanced versions of these machines employ the cutting edged concept of Deep Learning ("DL"), which is essentially the use of algorithms to mimic the multi-layered neural network of the human brain in order to allow AI software to train itself to solve complex real-world problems.[9] The interaction between AI, ML and DL is illustrated in the diagram below.

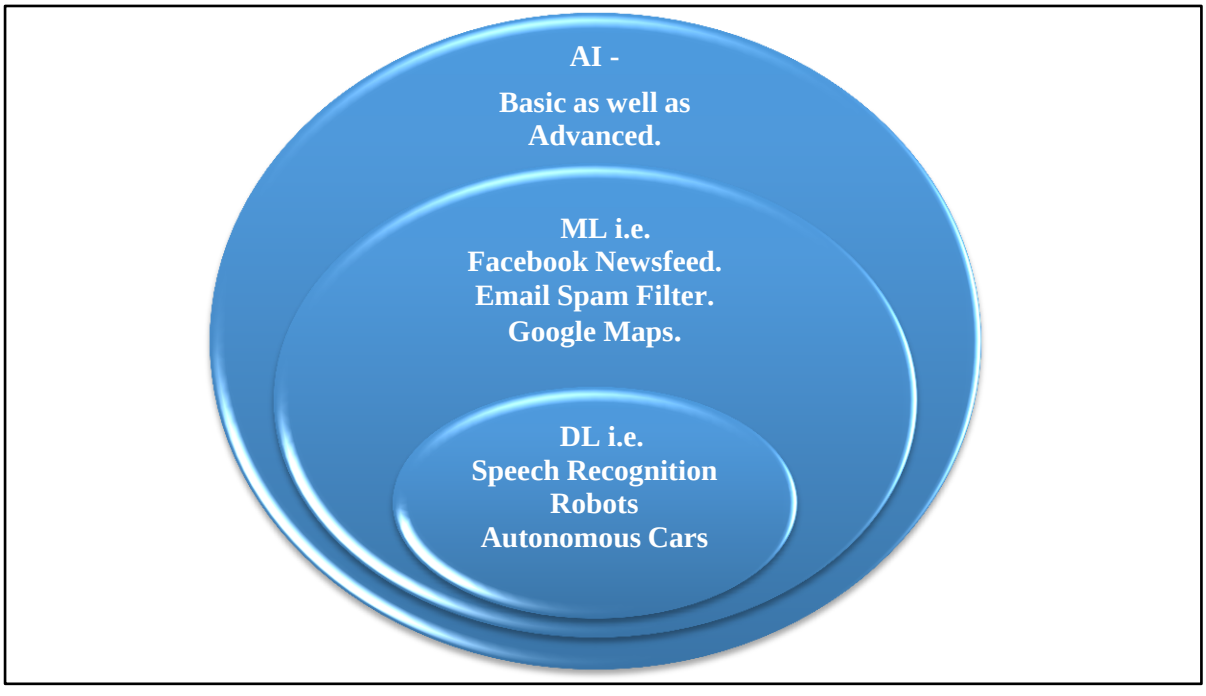


Diagram 2. Illustration of the interaction between AI, ML, and DL.[10]

[4] P Stone et al. 'Artificial Intelligence and life in 2030' (2016) One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel *Stanford University* 12, <http://ai100.stanford.edu/2016-report>.
[5] Ibid.
[6] Note 4 above, 14.
[7] Ibid.
[8] R Gilbert 'United States Chapter' in A Bensoussan et al. (1st Ed) *Comparative Handbook: Robotic Technologies* Law (2016) 335.
[9] Note 4 above, 14-15.
[10] Diagram created by the author using a similar illustration in J Jacobs 'Artificial Intelligence, Explained' Global X (17 July 2017), < https://www.globalxfunds.com/artificial-intelligence-explained/>.

A real-world hypothetical example of DL in action is an autonomous car that is programmed to drive on a public road.[11] Whilst driving, it gradually collects as much real-world data as possible to assist it in predicting the behaviour of other road users and to equip it to deal with complex future situations.[12]

As is usually the case with novel and innovative technology that advances at the rate that AI does, the corresponding legal framework is unable to keep up.[13] This apparent disconnect generates a number of intellectual property, liability and privacy issues which affect many spheres of modern society.[14]

In South Africa, there is currently no legislation which deals directly with AI and the legal issues associated with it.[15] Nevertheless, certain current and prospective legislation may be read to apply to the numerous legal issues that will potentially arise.[16] The various issues that require regulation, as well as the legislation that currently pertains to them to a limited extent in South Africa, will be examined.

In addition, the legislative framework already in place in jurisdictions leading the charge in this field, namely the United States of America ("US") and the European Union ("the EU"), will be considered in detail in order to highlight any gaps in South African jurisprudence. Thereafter, the initiatives already underway to develop and augment the existing body of jurisprudence in these jurisdictions will be canvassed in order to extract valuable lessons to assist legislators in determining the way forward for South Africa.

II. PURPOSE OF RESEARCH

The primary purpose of this research is to analyse the current regulatory regime pertaining to AI in South Africa and to compare and contrast this position with that of the US and the EU. The author is not aware of any similar study on this subject, from a legal perspective, which has ever been undertaken in South Africa.

[11] Note 8 above, 348-349.
[12] Note 8 above, 349-350.
[13] J P De Almeida Lenardon 'The Regulation of Artificial Intelligence' (2017) Tilburg Institute for Law, Technology and Society *Tilburg University* 11, < http://arno.uvt.nl/show.cgi?fid=142832>.
[14] Ibid.
[15] J Giles & A Emma-Iwuoha 'South Africa Chapter' in A Bensoussan et al. (1st Ed) *Comparative Handbook: Robotic Technologies* Law (2016) 265.
[16] Ibid.

III. RESEARCH OBJECTIVES

The specific objectives of this research report are as follows:

- to evaluate the current regulatory regime in South Africa, the US and the EU in the context of the research questions posed;
- to extrapolate any lessons that can be learned from the US and the EU; and
- to hypothesise a way forward for AI regulation in South Africa.

IV. RESEARCH METHODOLOGY

In light of the fact that this is a legal study, a desktop approach was adopted, and the following sources were consulted:

- electronic databases such as Google Scholar, Sabinet, SACat, SA ePublications, Westlaw, the Wits Electronic Database and WorldCat;
- national and international statutes;
- national and international case law;
- national and international standards and codes; and
- accredited peer-reviewed articles.

V. SCOPE

The overarching focus of this research report is on the South African perspective. In order to facilitate a critical legal analysis, the legal positions in the US and the EU were evaluated in detail. These jurisdictions were chosen as comparisons for three primary reasons:

1) they consist of many different independent states (in the case of the US) and member countries (in the case of the EU), the amalgamation of which allows for a holistic assessment for educational purposes;
2) the relatively widespread adoption of AI in both jurisdictions; and
3) the substantial progress both jurisdictions have made in the regulation of AI thus far.

VI. LAW TO DATE

This research report considered relevant literature up to and including 21 January 2018.

VII. LIMITATIONS

Given the complexity of this topic, the technical aspects pertaining to AI and how it functions as well as the in-depth themes of NanoBot technology and Virtual Reality have been excluded. Being a novel subject area, minimal research has been conducted in South Africa on this topic. Consequently, the reader will observe a general lack of case law and South African peer-reviewed articles.

VIII. REFERENCING TECHNIQUE

The South African Journal of Human Rights House Style was implemented.

IX. ETHICAL REQUIREMENTS

No tests or experiments were conducted or performed on humans or animals.

X. OUTCOMES

To compile a comprehensive analysis of this topic in order to provide assistance to South African legal practitioners, legislators, and government officials attempting to navigate this novel area of the law.

XI. OUTLINE

A number of research questions will be set out, acting as the backbone of the analysis conducted in South Africa, the US and the EU. Thereafter, the three jurisdictions will be compared, the lessons learned will be extracted and a conclusion reached on the proposed way forward for South Africa.

XII. RESEARCH QUESTIONS

Given the increasingly wide spectrum of application of AI, the issues that currently require regulation and will ultimately require some form of regulation in the future, are vast.

The most pressing of these legal issues have been condensed into the following research questions:

a) What is the legal status of AI?
b) Are automated transactions concluded by AI outside of the parameters of its programming valid?
c) What is the current liability regime, both civilly and criminally, in respect of defective and malfunctioning AI?
d) Can AI legally collect, store and process personal information?
e) Is intellectual property created autonomously by AI protectable and to whom does it belong?

Each of these research questions will be examined in light of existing legislation in all three of the highlighted jurisdictions in order to identify the differences between them and extract any valuable lessons that may be learned from the US and the EU.

XIII. LEGAL POSITION - SOUTH AFRICA

(a) Legal Status of AI

Currently, AI does not enjoy a separate legal status in South Africa.[17] However, this may have to change in the near future as AI software becomes more and more autonomous and through machine learning, starts making independent decisions outside of the scope of those initially programmed.

This change could potentially be facilitated by extending the principle laid out by Corbett CJ in *Financial Mail v Sage Holdings,*[18] namely that courts tend to view natural and artificial (legal) persons as enjoying the same personality rights in circumstances where it is appropriate to do so.[19] In this particular case, the extension of privacy rights to a company.

It follows then that if personality rights (analogous to those conferred on companies) can be extended to "artificial" persons, creating a separate form of legal status for AI may be possible in certain specified circumstances in the future.[20]

[17] Note 15 above.
[18] 1993 (2) SA 451 (A),
[19] Ibid, para 25.
[20] Note 15 above.

An excellent example of the efficacy of this idea is the granting of citizenship to the AI robot "Sophia" in Saudi Arabia on 25 October 2017.[21] This radical innovation certainly denotes the possibility of AI being viewed as a separate being, capable of having rights previously ring-fenced exclusively for natural persons.[22]

(b) Automated Transactions

Much of modern business is conducted online via email and Skype.[23] As a result, electronic agreements concluded in the context of an electronic transaction have become extremely prevalent.[24] South African law has caught up with these technological advances and fortunately, contracts concluded autonomously by an electronic agent are recognised and regulated.[25]

An automated transaction in this context is an agreement formed where either of the parties to an agreement uses an artificially intelligent electronic agent to autonomously fulfil one of the functions of the conclusion of an agreement.[26] A good example of this is the automated transactions that occur on websites such as Amazon or the South African equivalent, Takealot, for the purchase, sale, and delivery of goods.

(i) Electronic Communications and Transactions Act[27] ("ECTA")

Section 20 of the ECTA sets out various parameters for the valid conclusion of an automated transaction. An automated transaction is defined as "any electronic transaction conducted or performed, in whole or in part, by means of data messages in which the conduct or data messages of one or both of the parties are not reviewed by a natural person in the ordinary course of such natural person's business or employment."[28]

---

[21] G Katznelson 'AI Citizen Sophia and Legal Status' *Harvard Law Blog* (9 November 2017), <http://blogs.harvard.edu/billofhealth/2017/11/09/ai-citizen-sophia-and-legal-status/>.
[22] Ibid.
[23] A Christie 'Smart Contract 2.0: The need for "Smart Lawyers" *Polity* (2017), <http://www.polity.org.za/article/smart-contract-20-the-need-for-smart-lawyers-2017-09-26>.
[24] W Erlank & L Ramokanate 'Allocating the risk of software failures in automated message systems (autonomous electronic agents)' (2016) *SA Merc LJ* 204-205.
[25] Ibid.
[26] Ibid.
[27] No. 25 of 2002.
[28] ECTA, Section 1.

This definition is broad enough to include all agreements concluded electronically where one of the parties is an electronic agent and a transaction is completed subject to specified parameters. Essentially, these parameters can be summarised as follows:

- an agreement is reached when an electronic agent performs one of the functions necessary for the conclusion of a contract in South African Law;[29]
- one of the parties to the contract must be an electronic agent[30] (this includes scenarios where all of the parties to an agreement are electronic agents);
- if a party elects to use an electronic agent, they are bound by the terms of the agreement reached regardless of whether or not they reviewed the terms of that agreement;[31]
- if a natural person is a party to the agreement, they cannot be bound by its terms unless all of such terms were capable of review by that natural person prior to the conclusion of the agreement;[32] and
- a valid agreement is not concluded if a natural person made a material error in the creation of a data message provided that: (i) the natural person was not afforded an opportunity to rectify this error; (ii) the natural person notified the other party of this material error as soon as practically possible; (iii) the natural person takes reasonable steps to return any performance received, alternatively destroy such performance; and (iv) the natural person has not received any benefit from a third party arising from the conclusion of the agreement.[33]

(ii) Are automated transactions concluded in these circumstances valid?

It is clear from the above that a valid contract may be concluded electronically where AI represents one or both of the parties. Whilst this is encouraging, this does not expressly deal with the distinct possibility of AI learning from experience through ML and DL and altering the terms of the electronic contract outside the parameters of its programming.

In these particular circumstances, it is not clear whether the electronic agent would bind the party it represents by its actions or whether that party could avoid the consequences of the

[29] ECTA, Section 20(a).
[30] ECTA, Section 20(b).
[31] ECTA, Section 20(c).
[32] ECTA, Section 20(d).
[33] ECTA, Section 20(e).

contract by asserting some form of mistake or lack of authority on the part of the electronic agent.

A potential solution to this problem could be found in the concept of legal personality mentioned above. If the AI concerned is afforded legal capacity outside of the law of agency to conclude a contract, this form of electronic agreement concluded independently would be valid.

(c) Liability Regime

(i) Civil liability

Whilst all of the legal issues highlighted are of critical importance, the most obvious question that will no doubt be at the forefront of a consumer's mind is the liability regime pertaining to AI in the event of a malfunction and/or damage caused.

In the absence of a separate legal personality regime for AI, these issues are generally product-centric and are governed by the specific consumer protection and product legislation set out below.[34] Notably, this legislation does not detract from the remedies available under the law of contract (such as breach of warranty) and the law of delict (such as patrimonial and non-patrimonial loss).[35]

(aa) Automated Transactions - ECTA

Section 20(c) of ECTA creates a rebuttable presumption that the parties to an automated transaction are bound by its terms irrespective of whether or not they have reviewed the contents of the contract.[36]

Section 25(c) of ECTA goes on to place the liability for the consequences of an automated transaction squarely on the shoulders of the programmer of the electronic agent, alternatively the person for whom the electronic agent was programmed.[37] This remedy is subject to the caveat that the programmer may escape liability if it can be shown that the electronic agent deviated from its programming when concluding the contract.[38]

---

[34] Note 15 above.
[35] Ibid.
[36] Note 24 above, 213.
[37] Ibid
[38] Ibid.

In addition, a certain amount of leeway is afforded to programmers and suppliers of software given that it is accepted in general that software is not a perfect product and will no doubt require some form of remedial work to correct any bugs and errors that occur.[39] It is commonly accepted in this day and age that these bugs and errors will be addressed over time by the programmer and/or supplier through updates and patches.[40]

(bb) Defective AI - Consumer Protection Act[41] ("CPA")

In terms of Section 61 of the CPA, suppliers of goods are presumed to be liable for any harm suffered by an affected party as a result of any failures and defects.[42] This presumption is not based on fault and a consumer is entitled to hold the producer/importer/distributor/retailer ("the supplier") jointly and severally liable for both physical and economic harm.[43]

Despite the above, there are numerous defences available to the supplier of an AI product. These defences are *inter alia* as follows:

- the consumer is not a juristic person that falls within the thresholds set out in the CPA;[44]
- the defect was not present at the time of the supply of the product;[45]
- the error is wholly attributable to the consumer failing to follow instructions provided with the product;[46] and
- the claim has prescribed through the effluxion of time as set out more fully in the Prescription Act 68 of 1969.[47]

[39] Note 24 above, 213.
[40] *Saphena Computing Ltd v Allied Collection Agencies Ltd* [1995] FSR 616 at 652.
[41] No. 68 of 2008.
[42] Note 15 above. See further - J Giles 'Product Liability for Damage caused by Goods' *Michalsons*, <https://www.michalsons.com/blog/product-liability-for-damage-caused-by-goods/4584>.
[43] CPA, Section 61(5).
[44] R2 000 000 as set by the Minister of Trade and Industry in Government Gazette No 34181, dated 1 April 2011.
[45] CPA, Section 61(4)(b)(i).
[46] CPA, Section 61(4)(b)(ii).
[47] CPA, Section 61(4)(d) and Section 11 of the Prescription Act, which sets out the periods of prescription pertaining to particular debts.

(cc) Medicines and Related Substances Act[48] ("MRSA")

Certain medical devices are regulated in terms of the MRSA. Many of such devices use AI to perform autonomous tasks which would otherwise be performed by the medical professional/staff member concerned.[49]

The Medicines and Related Substances Amendment Act[50] provides a new definition for medical devices, which widens it to include "any instrument, apparatus, implement, machine, appliance, implant, reagent for in vitro use, software, material or other similar or related article…".[51] This broad definition can be read to include modern forms of medical AI, which would have to be registered in terms of the MRSA and would be subject to the punitive provisions contained therein,[52] in the event that an AI medical device does not comply with the requirements set out therein.[53]

(dd) Part 101 of the Civil Aviation Regulations[54] ("PART 101")

Drones are defined in PART 101 as Remotely Piloted Aircraft Systems ("RPAS").[55] Regulation 101.01.1(2) of Part 101 states that RPAS may be operated for commercial, corporate, non-profit and private operations. In addition, Regulation 101.01.1(3)(c) of Part 101 states that the Civil Aviation Regulations do not apply to a model aircraft or a toy aircraft. Part 101 goes on to provide a whole list of rules for the operation of RPAS which are crucial for their regulation and safe operation.[56]

Specific drones may be classified as artificially intelligent given that they undertake tasks autonomously, for example, surveillance drones and drones that monitor crops and weather conditions.[57] In these circumstances, such artificially intelligent drones would have to comply with Part 101 and would be subject to the punitive sanctions contained therein in the event of a breach.

[48] No. 101 of 1965.
[49] Note 15 above, 273.
[50] No. 14 of 2015.
[51] Ibid, Section 1(g).
[52] MRSA, Section 30.
[53] Note 15 above, 274.
[54] Of 2015.
[55] Regulation 1, PART 101.
[56] Note 15 above, 276.
[57] Note 15 above, 277.

(ii) Criminal liability and Mens Rea

Whereas establishing civil liability and calculating economic loss is relatively straight-forward in light of the provisions of ECTA and the CPA, working out where criminal responsibility lies when AI commits a crime, is a far more complicated endeavour.

To prove most crimes, one of the prerequisites is culpability or *Mens Rea*.[58] *Mens Rea* pertains to the mental state of the accused at the time of the commission of the crime[59] and requires either an element of negligence or intention to be proved.[60] Simply put, negligence requires that the accused ought to have reasonably foreseen the outcome and intention denotes that the accused intended to commit the crime.[61]

Naturally, if the AI was explicitly programmed to commit a crime, this puzzle is easily solved however when ML and DL cause AI to evolve to such a level that it is capable of making its own decisions, the current regulatory regime in South Africa does not provide specific guidance for this potential outcome.

If South African courts eventually confer some form of legal personality upon AI, perhaps it may be possible to charge AI directly for a crime committed by it. Assuming this hurdle is somehow cleared, the next challenging issues to solve will be how to prove the elements of negligence and intention and subsequently, the form of punishment that would be suitable for AI.

(d) Privacy

The legality of the collection of private information processed by and stored by AI systems and machines has not been expressly dealt with by South African legislation that is currently in force. Nevertheless, the Protection of Personal Information Act[62] ("POPI") will apply to this issue directly once it comes into force on a date which is still uncertain.

[58] S N Kwanje 'Distinguishing between intention and negligence in South African Criminal Law' (2016) *North-West University* 9, <https://repository.nwu.ac.za/bitstream/handle/10394/24910/Kwanje_SN.pdf?sequence=1&isAllowed=y.>.
[59] J Burchell *Principles of Criminal Law* 3 ed (2005) 459.
[60] Note 58 above, 2.
[61] Ibid.
[62] No. 4 of 2013.

(i) POPI

In order for AI to lawfully gather and store personal information, the provisions of POPI will have to be followed and will become mandatory when the commencement date for POPI is finally announced.[63] The responsible party, namely the person who decides what data is collected, stored and processed will have to:

- attain the consent of the person from whom the data is collected and notify such person when the data is being collected;[64]
- confirm that all data processed in relation to children is lawfully authorised in terms of section 35 of POPI;
- ensure that there is a valid lawful purpose for processing the data collected and inform the person from whom the data is collected precisely what this purpose is;[65]
- limit any further processing of data to the purpose for which it was initially collected;[66]
- be transparent as far as possible in relation to the actions taken by AI when collecting and processing data;[67]
- verify that the data collected is correct;[68]
- make sure that the data collected is adequately secured;[69] and
- permit the owner of the data collected to access such data to correct it if necessary.[70]

Once the commencement date of POPI is announced, the responsible party concerned will then have a grace period of a year to comply with the provisions of POPI,[71] which period may be extended for a further maximum period of three years.[72]

It is not clear from the provisions of POPI whether or not AI that collects information on its own volition as a result of ML and DL will be explicitly regulated by POPI. Currently, the duty of care would have to fall on the owner of the AI. However, if a separate legal

[63] Note 15 above, 277. See further - J Giles 'Protection of Personal Information Act Summary – POPIA' *Michalsons*, <https://www.michalsons.com/focus-areas/privacy-and-data-protection/protection-of-personal-information-act-popia>.
[64] POPI, Sections 11 and 18.
[65] POPI, Sections 9, 10 and 13.
[66] POPI, Section 15.
[67] POPI, Section 18.
[68] POPI, Section 16.
[69] POPI, Section 19.
[70] POPI, Sections 23 and 24.
[71] POPI, Section 114(1).
[72] POPI, Section 114(2).

personality regime is ultimately created for specific forms of AI, the AI itself will become the responsible party.

(e) Intellectual Property

AI is capable of producing material that would traditionally be afforded protection by the intellectual property rights of a particular country if a human being created such content.[73] Regrettably, the current regulatory regime in South Africa does not cater specifically for material created independently by AI.

To ascertain in what manner, if any, the current legislation applies to content created independently by AI, the relevant subcategories of intellectual property ("IP") and its potential applicability to content created by AI will be dealt with more fully below. Thereafter, the ownership of content created independently by AI will be dealt with expressly in light of the current IP legislation in South Africa.

(i) Copyright

The protection afforded by copyright is inherent and does not require registration.[74] In terms of Section 2 of the Copyright Act[75] ("the Copyright Act"), it applies to many classes of work such as literary works, musical works, and films. In the unanimous judgment of Streicher JA in the matter of *Haupt t/a Softcopy v Brewers Marketing Intelligence (Pty) Ltd and Others*,[76] the literary works contemplated by this section were found to include databases,[77] which are commonly created by the AI algorithms used by Google and other similar AI software programmes on a daily basis.

In light of the above, South African copyright protection could theoretically be applied to content created independently by AI provided that it is original and was created in South Africa.[78] Whether or not this Copyright could be enforced is a matter of ownership and will be dealt with below.

---

[73] N Porto & D Preiskel 'United Kingdom Chapter' in A Bensoussan et al. (1st Ed) *Comparative Handbook: Robotic Technologies* Law (2016) 319.
[74] Note 15 above, 268.
[75] No. 98 of 1878.
[76] 2006 (4) SA 458 (SCA)
[77] Ibid, para 39.
[78] Note 15 above, 268.

(ii) Patents

Patents are exclusive rights assigned for a limited period to an inventor.[79] To qualify to be patented, the subject of the invention must:[80]

- be novel;
- of practical use; and
- inventive.[81]

If all of these requirements are met, the invention may qualify to be registered in the South African Patents Office.[82] The issue that arises is again one of ownership of the invention as this would traditionally vest with the "inventor" provided that the rights to this invention have not been sold or assigned.[83]

Given that the term "inventor" is not defined in the Patents Act,[84] it is unclear whether the Patents Office would accept a Patent application where the inventor is listed as a particular form of AI. In the current technologically undeveloped governmental system in South Africa, this form of deviation from the norm is unlikely to be accepted.

(iii) Ownership[85] of IP created by AI?

If the owner of AI elects to programme it to create material or products capable of being protected by intellectual property laws, this material or product could be seen as a derivative offshoot of the programming and belonging to the owner.[86] However, if the AI concerned learns from its environment and creates the same material or product entirely independently of its programming, it is not altogether clear where ownership vests.[87]

If some form of legal status is ultimately created for AI, there may potentially be a time where the AI itself can claim some form of ownership over the intellectual property created by it. In the interim, however, the current legal regime does not contemplate or address this issue.[88]

---

[79] Note 15 above, 269.
[80] Ibid.
[81] Section 25(1) of the Patents Act No. 57 of 1978.
[82] Note 15 above, 269.
[83] Note 15 above, 270.
[84] No. 57 of 1978.
[85] For the purposes of this report, ownership of IP is considered at a very basic legal level, namely the right to deal with the IP as desired within the limits of the law. See further - *Regal v African Superslate (Pty) Ltd* 1963 1 All SA 203 (A).
[86] Note 81 above.
[87] Ibid.
[88] Ibid.

Practically the only interpretation that makes sense in these circumstances, where intellectual property is created by AI outside the scope of the initial programming, is that the intellectual property must be owned by the natural or legal person who programmed or owns the AI.

XIV. LEGAL POSITION – US

AI technology traditionally developed by the US for the military is now being produced and sold to the general population.[89] An excellent example of a company taking advantage of this evolution is Amazon, who has declared that they are in a position to use autonomous drones for delivery of parcels when the various regulations are enacted to allow them to do so.[90]

Another good example is the motor industry where producers such a Tesla are fast-tracking the development and testing of autonomous vehicles, which will very shortly be available on the open market.[91]

There is no doubt that the US is not only an avid consumer of AI but is also a leading innovator in the field.[92] With this in mind, the current legislative landscape in the US,[93] as well as the various initiatives adopted in this jurisdiction thus far, will be considered in detail in relation to the research questions posed.

(a) Legal Status of AI in the US

Regrettably, judges in the US still view robots as mere programmable tools despite the blurred line that is forming between person and device.[94] The lack of a separate legal personality regime for AI and particularly robots in the US challenges the judiciary's ability to competently deal with the issues that will likely be faced in everyday life in the near future.[95]

The tendency in US law is to attribute liability to a person as opposed to AI itself to avoid dealing with the complicated ethical and legal questions that AI creates.[96] This approach may work in instances where the person responsible for monitoring AI does not do

[89] Note 8 above.
[90] Ibid.
[91] Ibid.
[92] Ibid.
[93] This analysis will be focussed on federal legislation and in certain specific instances, noteworthy legislation of individual states.
[94] Note 1 above, 36.
[95] Ibid.
[96] Ibid.

so correctly, for example, a pilot failing to monitor an autopilot system.[97] However, this approach will be much harder to justify in the instance where AI reaches a level of experience through ML and DL where it acts entirely independently of its programming.

Fortunately, the US government has acknowledged this issue and is taking positive steps to address the regulatory gaps that have appeared.[98] The approach adopted involves the manipulation of current legislation as far as possible to cater for the changes AI will pose to industries such as automation and aviation.[99] In particular, the US Department of Transportation has adopted a hybrid of this approach by creating safe avenues for testing of autonomous cars to identify potential issues and deal with these issues prior to allowing autonomous vehicles to flood the world market.[100]

(b) Automated Transactions in the US

Automated transactions concluded by electronic agents are governed by section 14 of the Uniform Electronic Transactions Act[101] ("UETA")[102] (which is similar but more limited in scope than section 20 of the South African ECTA) and the Electronic Signatures in Global and National Commerce Act[103] ("E-Sign").

Section 14 of UETA rubber stamps the conclusion of an automated transaction where one of the parties is an electronic agent. Section 101(h) of E-Sign builds on this provision and states that an electronic contract can be enforced if one of the parties is an electronic agent provided that its actions are attributable to "a person to be bound."

When read together, the wording of these acts does not contemplate a situation where the AI itself enters into a contract independently of its programming. This is partly because the

[97] Akin to the scenario in *Brouse v United States* United States District Court, N.D. Ohio, E.D. 83 F. Supp. 373 (N.D. Ohio 1949).
[98] C Cath et al. 'Artificial Intelligence and the "Good Society": the US, EU, and UK approach' (2017) *Sci Eng Ethics* 4, <https://doi.org/10.1007/s11948-017-9901-7>.
[99] Ibid.
[100] Executive Office of the President National Science and Technology Council Committee on Technology. '*Preparing for the future of artificial intelligence'* (2016) Washington, DC, USA 1, <https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf>.
[101] Of 1999.
[102] Adopted by 47 of the 50 US States. Notably, the Uniform Computer Transactions Act of 1999 also governs automated transactions, however, given that it has only been adopted by Maryland and Virginia, it was not discussed in this section.
[103] Of 2000.

legislators at the time viewed electronic agents as tools and did not yet appreciate the fact that they may eventually evolve to a point where they could act entirely autonomously.[104]

As is the case in South Africa, this scenario would necessitate some form of legal personality being attributed to the AI in order that it may validly enter into a contract and be bound independently (of a natural or juristic person) to the terms thereof.

(c) US Liability Regime

(i) Civil

In the US, the primary realm of civil liability for AI is also product-centric. In the absence of universal consumer protection legislation, AI product defects will be dealt with under contract or tort law (the American equivalent of delict in South Africa),[105] depending on the circumstances of each situation.

Contract law applies when there is a pre-existing contractual relationship between the parties and Tort law applies in the event of an incident or accident. In addition, UETA contains a specific provision which regulates the liability that arises out of a mistake or error in an automated transaction.

(aa) Contract Law

Provided that a contractual relationship exists between the supplier and the consumer, breaches of contract as a result of malfunctioning AI may give rise to a claim for contractual damages. A good example of this is a breach of an express warranty set out in a contract when an AI product does not perform as represented.[106]

Aside from the express warranties codified in contracts, certain implied warranties apply to AI products in terms of the US commercial codes.[107] These implied warranties include, *inter alia*, the following:[108]

- the product is of a commercially acceptable quality;
- it is suitable for the purpose for which it is marketed and intended; and

[104] S Kis 'Contracts and Electronic Agents' (2004) *LLM Theses and Essays* 11, <http://digitalcommons.law.uga.edu/stu_llm/25> .
[105] Note 8 above.
[106] Note 8 above, 338.
[107] Ibid.
[108] Ibid.

- the supplier has the right to transfer ownership of the product to the consumer.

(bb) Tort Law

When analysing tort law in the US, it is important to note that each state has different laws which govern product liability. Nevertheless, the two main tort principles that may be extracted are "strict liability" and "negligence.[109]

Strict liability is only applicable to products that are intrinsically dangerous. To prove strict liability, a consumer will have to prove that: the AI product was defective when it left the factory; it reached the consumer without having been altered; and that it was the proximate cause of damages/injuries suffered by the consumer.[110] This form of liability would be applicable in the case of specific AI medical devices where reliability is paramount for the maintenance of human life.[111]

Negligence, on the other hand, pertains to all other products which are not by their nature, dangerous.[112] In these instances, the consumer would have to prove that: the manufacturer was duty bound to exercise care when creating the product; this reasonable care was not exercised; and that the negligence of the manufacturer was the proximate cause of the consumer's damages/injuries.[113] This may be very difficult to establish in relation to AI that is found to have strayed drastically from the manufacturer's programming as a result of ML and DL.

(cc) UETA

Section 10(2) of UETA sets out the conditions in terms of which a natural person may escape the provisions of an automated transaction[114] in the event of a mistake or error. These terms and conditions mirror those set out in section 20(e) of ECTA.

One notable difference between the two, however, is the additional "security procedure" defence available to a natural person in this scenario in terms of section 10(1) of UETA. In essence, this defence is available when a security procedure to detect changes and errors was agreed to between the parties and such security procedure was not followed by one of the

[109] Note 8 above, 338.
[110] Ibid.
[111] Note 8 above, 337.
[112] Ibid.
[113] Ibid.
[114] J A Estrella Faria 'e-Commerce and international legal harmonization: Time to go beyond functional equivalence' (2004) SA Merc LJ 552.

parties.[115] In this instance, the innocent party may avoid the consequences of the automated transaction.

(ii) Criminal

Criminal law in the US, in a similar vein to South African criminal law, places great emphasis on the mental element of *Mens Rea* when assigning criminal liability.[116] As with South African Law, negligence or intention is very difficult to establish when AI acts outside the scope of its programming. Assuming that a criminal liability regime is ultimately created for AI, legislators would still have to fashion an appropriate method of punishment to be metered out.[117]

Practically, it is evident that capital punishment cannot be considered given that the main punitive element of this form of punishment for humans is a deprivation of time and life,[118] two elements that do not affect AI.

A potential solution to this issue could be a form of community service whereby the AI concerned performs remedial work in a community of the victim's choice for a pre-determined period.[119]

(d) Privacy in the US

Currently, personal data is protected generally in the US in terms of the United States Privacy Act.[120] The approach adopted is a sectoral one with different statutes applying to the public and private sectors.[121] These laws consist of a conglomeration of federal and state legislation and vary in application from industry to industry, applying individually to different categories of information.[122]

In these circumstances, the approach adopted in respect of the collection of private information processed by and stored by AI systems and machines varies considerably from

[115] UETA, Section 10(1).
[116] Note 4 above, 47.
[117] G Hallevy '"I, Robot – I, Criminal" – When Science Fiction Becomes Reality: Legal Liability of AI Robots committing Criminal Offences' (2010) 22 *Syracuse Science & Technology Law* Reporter 29.
[118] Ibid, 31.
[119] Ibid, 33.
[120] Of 1974, 5 U.S.C.
[121] P M Schwartz 'The EU-US Privacy Collision: A turn to institutions and procedures' (2013) 126 *Harvard Law Review* 1974.
[122] M A Weiss & K Archick 'U.S.-EU Data Privacy: From Safe Harbour to Privacy Shield' (2016) 7-5700 *Congressional Research Service Report* 3, <https://fas.org/sgp/crs/misc/R44257.pdf>.

state to state. Nonetheless, on the whole, most states have some form of privacy legislation which would govern this field.[123]

An example of this is the California Online Privacy Protection Act[124] ("COPP"), which requires commercial websites (that more than likely use AI to collect personal information) to post their privacy policies on such websites.[125] This policy must also describe the manner in which the data will be handled and the principles contained therein.[126]

Generally, state-specific legislation is loosely based on common worldwide data protection principles and in light of the variation in its content and applicability, will be best examined more fully in the context of specific AI industries such as drones and autonomous cars.

(i) Drones

The Federal Aviation Administration ("the FAA") requires owners of drones weighing between 0.55 and 55 pounds to register them online.[127] This system allocates a unique identification number to each registered owner of a drone and ensures that these owners do not slip through the system,[128] thereby remaining accountable for any issues that may arise in contravention of the FAA Modernization and Reform Act.[129]

Given that most small drones operate in limited spaces and at an extremely low altitude, they are perfect vessels for invading personal space and collecting and processing personal information.[130]

There is currently no specific federal legislation that regulates the collection and processing of personal information by drones. However, the pending Drone Aircraft Privacy and Transparency Act[131] requires that certain disclosures are made as part of the drone flight approval plan, namely the private data that is likely to be collected as well as the manner in which is intended to be processed.[132]

[123] Note 8 above, 347.
[124] Of 2003.
[125] COPP, Chapter 22 – 22575(a).
[126] COPP, Chapter 22 – 22575(b).
[127] Note 8 above, 346.
[128] Ibid.
[129] Of 2012, H.R. 658.
[130] Note 8 above, 346.
[131] Of 2017, H.R. 1526
[132] Note 8 above, 347.

In addition, in terms of section 1708.8 of the Civil Code of California, it is illegal for a drone to photograph a person if such photographs are taken whilst trespassing in an area that would traditionally be considered private.[133]

(ii) Autonomous Cars

Considering that smart cars have the capacity to collect an enormous amount of personal data, it is unsurprising that various US automakers have codified a number of principles for the valid collection and processing thereof.[134] The principles, as set out in the codification document entitled "Consumer Privacy Protection Principles for Vehicle Technologies and Services," can be summarised as follows:[135]

- maintain transparency when collecting, processing and distributing data;
- offer choices in respect of such collection, processing, and distribution;
- preserve the context of data at all times;
- collect data only for valid reasons and keep it only as long as necessary;
- maintain data security;
- ensure data accuracy and permit the owner of the data collected to access such data to correct it if necessary; and
- take reasonable steps to ensure that all of these principles are followed.

(e) Intellectual Property in the US

US IP law similarly caters for copyright and patent protection in respect of AI. In order to avoid unnecessary repetition, these IP principles will only be discussed briefly in relation to content created independently by AI and subsequently, applied to the notion of ownership.

(i) Copyright

In the US, copyright is not inherent and must be registered in the US Copyright Office to enjoy the protection of the Copyright Act.[136] In addition and to qualify for registration, the

[133] Note 8 above, 347.
[134] Ibid.
[135] Alliance of Automobile Manufacturers, Inc. 'Consumer Privacy Protection Principles – Privacy Principles for Vehicle Technologies and Services' (12 November 2014), < https://autoalliance.org/connectedcars/automotive-privacy-2/principles/>.
[136] Note 8 above, 342.

work must have been created by a human.[137] In *Naruto v Slater*,[138] the issue of whether a monkey was entitled to copyright in respect of a selfie taken by him was dealt with. The district court found that the limited scope of current copyright laws in the US only afforded this right to humans and not to animals.[139]

If this principle is extended, any work created autonomously by AI without the input of a human programmer cannot be registered in the US Copyright Office and enjoy any form of Copyright protection. If the US copyright laws are not changed in the near future, this close-minded approach to copyright is likely to continue. Nevertheless, if a separate legal personality is created for AI and authorship is capable of being assigned to it, it is not inconceivable that such IP may eventually be copyrighted.

(ii) Patents

Patents are separated into three categories in US law, namely design, utility and plant patents.[140] Design relates to appearance; utility pertains to functionality and plant patents refer to the discovery of a new species of plant.[141] In terms of the U.S. Patent Act[142] (USPA), an invention under these categories would have to satisfy the following four requirements to qualify to be patented:

- it must be new or novel;[143]
- it must be useful;[144]
- it must fall into one of the categories set out by the statute, namely processes, machines, articles of manufacture, and compositions of matter;[145] and
- it cannot be obvious, i.e., it must consist of an inventive step which is not apparent to an ordinary member of the field.[146]

As with South African law, once the requirements for a patent have been satisfied, the issue of defining the "inventor" of the invention in the context of AI inventions rears its head and presents a legal conundrum for the Patents Office.[147]

---

[137] Section 306 of The Compendium of U.S. Copyright Office Practices (29 September 2017), < https://www.copyright.gov/comp3/docs/compendium.pdf>.
[138] No. 15-cv-4324, 2016 WL 362231 (N.D. Cal. Jan. 28, 2016).
[139] Ibid.
[140] Note 8 above, 339 - 340.
[141] Ibid.
[142] 35 U.S.C.
[143] USPA, Section 101.
[144] Ibid.
[145] Ibid.
[146] USPA, Section 103.

An inventor is defined in section 100(f) of the USPA as "the individual or, if a joint invention, the individuals collectively who invented or discovered the subject matter of the invention." This section has been interpreted by the US Supreme Court in *Diamond v Chakrabarty*[148] as applying to anything created by humans. This restricted interpretation has not yet been extended to content created by AI and accordingly, it cannot be patented under the current regulatory regime.[149]

(iii) Ownership

Regrettably, as is the case with most current legislation, the limited definitions in US copyright and patent legislation do not contemplate a scenario where AI itself creates IP without human instruction or intervention.[150] In light of these constrictions, there is no doubt that the law will have to be developed in this area and some form of resolution reached on the capacity of AI to own IP created by it as opposed to such IP potentially remaining in the public sphere for the benefit of all.

XV. LEGAL POSITION – EU

The European Commission has recently identified AI and artificially intelligent objects as crucial for the future development of society and the European economy.[151] Given that the EU consists of 28 member countries, the approach to certain aspects of AI regulation varies from country to country.

Nevertheless, the EU jurisdiction as a whole serves as a very useful yardstick to gauge the current state of AI regulation across these various countries and to extract valuable lessons for the future regulation of AI in South Africa. For the sake of brevity, the general legal position pertaining to each research question in the EU will be dealt with first, and if notable, the approach in individual countries will be included thereafter.

---

[147] F A DeCosta & A G Carrano 'Intellectual Property Protection for Artificial Intelligence' (2017) *Westlaw Journal of Intellectual Property* 2.
[148] 447 U.S. 303 (1980).
[149] Ibid.
[150] Note 8 above.
[151] G Ballas & T J Konstantakopoulos 'Greece Chapter' in A Bensoussan et al. (1st Ed) *Comparative Handbook: Robotic Technologies* Law (2016) 133.

(a) Legal Status of AI in the EU

As is the case in South Africa and the US, AI and AI machines are not afforded any form of separate legal personality in the EU.[152] This thinking stems from the outdated perception that historically pervaded the minds of scholars in most EU countries, i.e., that AI and AI machines are mere tools and that as such, the responsibility for such tools will always lie with human beings.[153]

Fortuitously, as ML and DL allow AI to increase its decision-making capacities and to ultimately make autonomous decisions, this limited mindset of the past will slowly transform.[154] The French scholar Alain Bensoussan, being the first to suggest a form of legal persona for AI,[155] has a very elegant viewpoint on the subject. In short, he believes that the more autonomous AI becomes, the stronger the argument in favour of applying human legal standards to such AI.[156]

In January 2017, the EU parliament's Committee on Legal Affairs approved a report that tables many recommendations pertaining to the development of the EU civil law rules on robotics.[157] This report calls on the commission to explore the legal solution of establishing a separate legal status for robots.[158] Given that robots are driven by AI software, this is a significant positive step forward in creating a separate legal status to cater for the liability issues that AI will create.

(b) Automated Transactions in the EU

The legal framework regulating automated transactions and electronic agents in the EU is less developed than in the US and South Africa. The overarching piece of regulation governing this aspect is the Directive on Electronic Commerce[159] ("the Directive"), which creates the

[152] Note 73 above, 314.
[153] Ibid.
[154] A Bensoussan & J Bensoussan 'France Chapter' in A Bensoussan et al. (1st Ed) *Comparative Handbook: Robotic Technologies* Law (2016) 70.
[155] S Fanti 'Switzerland Chapter' in A Bensoussan et al. (1st Ed) *Comparative Handbook: Robotic Technologies* Law (2016) 297.
[156] Note 154 above.
[157] M Delvaux 'European Parliament Report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2013(INL))' (27 January 2017) A8-0005/2017.
[158] Ibid, 18.
[159] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000, O.J.L 178/1, 17.7.2000.

framework for the conclusion of electronic contracts in the EU and encourages member states to eliminate all legal impediments to their use.[160]

Notably, the Directive does not refer to or define an electronic agent.[161] Nevertheless, the Proposal text of the Directive[162] does provide some guidance on this issue. It states that the member states of the EU must not prevent the use of "electronic agents" to conclude an electronic contract.

Remarkably, the Directive has not been widely transposed into national legislation by the member states despite being required to do so by January 17, 2002.[163] Nonetheless, individual member states[164] have enacted horizontal provisions which recognise the validity of contracts concluded by electronic means and by electronic agents.[165]

As is the case with the US and South Africa, the European community as a whole still views electronic agents as mere tools for the conclusion of electronic contracts that cannot be interpreted to be subject to rights and obligations and should only be seen as agents of a human principal.[166] Accordingly, it is likely that any contract concluded by AI entirely outside of the parameters of its programming will not be considered valid in the EU.

(c) EU Liability Regime

The legislation that applies to AI in the EU differs considerably between the various member states. Consequently, this section will be limited to the principles that overlap and the proposed standard set of rules which have been suggested for the EU thus far.

(i) Civil

Generally, as in both the US and South Africa, the liability regime in respect of AI in the EU is product based.[167] Potential product liability claims may arise out of a breach of contractual provisions, in terms of the tort law of negligence and alternatively, in terms of the strict liability regime imposed by consumer protection legislation.[168] The principles relating to

[160] Note 157 above, 18.
[161] S M Kierkegaard 'E-contract formation: U.S. and EU perspectives' (2007) 3 L. Com & Tech. 12 para 41, <http://www.lctjournal.washington.edu/Vol3/a012Kierkegaard.html>.
[162] Note 159 above, Annex 1 586.
[163] Note 159 above, Article 22(1).
[164] Including Belgium, Germany, Spain, Luxembourg & Finland.
[165] Note 104 above, 20.
[166] Note 104 above, 22.
[167] Note 73 above.
[168] Note 73 above, 315.

contractual and tort claims have already been dealt with comprehensively under US law and will not be dealt with in detail again as they do not differ drastically from the same principles in the EU.

The approach favoured currently and implemented in national legislation by a number of the EU members, is the strict liability regime encapsulated in the EU Product Liability Directive.[169] In terms of Article 1 of this directive, the "producer" of the AI product is held liable for any defects provided that the claimant can prove that the defect existed.[170] The main advantage for the consumer in this scenario is that there is no requirement to prove fault on the part of the manufacturer/supplier of the product (which is not the case with claims under contract and delict).[171]

(ii) Criminal

European criminal law is a hybrid system consisting of a combination of standardised Union law and national law that has been influenced by the directives issued under Union law.[172] The universal principle for the purposes of this section is that a criminal act in European Law also requires a subjective or mental element such as *Mens Rea* for a perpetrator to be held liable.[173] In this instance, *Mens Rea* refers to the fault elements of a crime, namely intention, recklessness, and negligence.[174]

As in South Africa and the US, attributing any of the fault elements required for a criminal act to AI will be challenging at best. In addition, even if these fault elements are somehow established and attributed to AI through the avenue of a separate legal personality regime, sentencing will present a further legal conundrum.

Article 5(4) of the Treaty on European Union[175] requires that EU union members apply the principle of proportionality to any actions taken, such as sentencing.[176] In this light, an appropriate solution may be the establishment of some form of sliding scale of punishment proportional to the level of autonomy of the AI and of a sufficiently punitive nature that it

[169] 85/374/EEC of 25 July 1985.
[170] Ibid.
[171] Note 73 above, 315.
[172] J H Blomsma '*Mens Rea* and defences in European criminal law' (2012) 54 *School of Human Rights Research Series* 5.
[173] Ibid, 43.
[174] Ibid.
[175] Treaty on European Union, 13 December 2007, 2008/C 115/01.
[176] E Herlin-Karnell 'What Principles Drive (or Should Drive) European Criminal Law?' (2010) 11 *German Law Journal* 1125.

discourages future transgressions.[177] Alternatively, legislators could make it mandatory for producers of AI to build in a "Kill-switch" to neutralise the AI and prevent the harm from occurring in the first place.[178]

(d) Privacy in the EU

In the EU, the collection, storage, and processing of personal information is governed by the General Data Protection Regulation[179] ("GDPR"), which was adopted on 27 April 2016.[180] The GDPR is enforceable as from 25 May 2018 and replaces the Data Protection Directive of 1995.[181]

The principles set out in the GDPR are very similar to those set out in POPI and will not be canvassed in great detail. Essentially, to validly collect, store and process data. AI will have to:

- garner the consent of the individual concerned,[182] which could potentially be done by way of an electronic approval containing the terms and conditions of the processing;
- ensure that there is a lawful basis for the processing of the data;[183] and
- ensure that such data is appropriately secured.[184]

Two interesting developments of the GDPR are: the introduction of a right to erasure, where a data subject (the person to whom the data relates) retains the right to cause the controller of the data (the AI in this case) to erase his/her/its data immediately;[185] and the introduction of regulations pertaining to Automated individual decision making, including profiling.[186]

The latter provision will prohibit the use of a number of AI algorithms, including recommendation algorithms such as the one used by Facebook and other social media platforms, that suggest further relevant content to users based on their preferences.[187] In its

[177] Note 175 above.
[178] J D Caytas 'European Perspectives on an Emergent Law of Robotics' (2017) *Columbia Journal of European Law* 2.
[179] 2016/679 [2016] OJ L119/1. See further - European Commission 'What does the General Data Protection Regulation (GDPR) Govern,' <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en>.
[180] B Goodman & S Flaxman 'European Union regulations on algorithmic decision-making and a "right to explanation"' (2016) 8 *AI Magazine* 1.
[181] Ibid.
[182] GDPR, Article 6(1)(a).
[183] GDPR, Article 6.
[184] GDPR, Article 32(1).
[185] GDPR, Article 17.
[186] GDPR, Article 22.
[187] Note 180 above.

current form, this article of the GDPR may necessitate a reinvention of the standard AI algorithms currently used.[188]

(e) Intellectual Property in the EU

As a part of its effort to create a unified system of law to standardise the approach taken in all of its member states, the EU issued a number of directives to regulate IP law.[189] The germane aspects of the principles extracted from these directives will be canvassed below in relation to both copyright and patent law.

(i) Copyright

The conditions necessary to qualify for Copyright protection in the EU are set out in the Berne Convention for the Protection of Literary and Artistic Works.[190] In short, there are two requirements, namely that the work must be original and that the subject matter of the work must be protectable (article 2).[191]

When these two conditions are applied to content created by AI, the subject matter requirement is easily dispensed with by consulting the predetermined list of protected works. Either the work falls into a protectable category, or it does not. The originality requirement, on the other hand, is slightly trickier to resolve.

In the three directives issued by the EU [192] that provide some guidance on the originality requirement, it is clear that the IP created by AI must be the "authors own intellectual creation" to meet the requirement of originality. This interpretation was confirmed in the matter of *Infopaq v Danske Dagblades Forening.*[193]

With this in mind, it will be difficult to attribute an expression of personal creativity to AI. This concept denotes that a form of consciousness is required in order for the work to qualify for originality,[194] the efficacy of which has not yet been considered but could be part of the framework for the assessment of copyright in the near future.

---

[188] Note 180 above.
[189] E Zirnstein 'Harmonization and Unification of Intellectual Property Laws in the EU' (2005) *Slovenia* 296, < http://www.fm-kp.si/zalozba/ISBN/961-6486-71-3/293-306.pdf>.
[190] As amended on September 28, 1979
[191] WIPO Intellectual Property Handbook: Policy, Law, and Use (2004) at para 5.171
[192] Articles 1(3) of the Software Directive 91/250/EC, 3(1) of the Database Directive 96/9/EC and Article 6 of the Term Directive 2006/116/EC.
[193] [19 July 2009] ECR I-6569 at para 37.
[194] H M Bohler 'EU copyright protection of works created by artificial intelligence systems' (2017) *University of Bergen*, <http://bora.uib.no/bitstream/handle/1956/16479/JUS399_V17_183.pdf?sequence=1&isAllowed=y>.

(ii) Patents

In terms of Article 52(1), as read with Articles 54(1) and 56(1) of the Convention on the grant of European Patents,[195] an invention must fulfil the following requirements to qualify for patent protection:

- the invention must be novel;
- it must not be in the public domain;
- it must consist of an inventive step which is not apparent to an ordinary member of the field; and
- it must be capable of industrial application.

Generally, patentable inventions were always thought of as being as a result of human thought processes.[196] This limited view is primarily as a result of being grounded in an era where inventions were only capable of being created by humans.[197] Even though the term "inventor" is not explicitly defined in any of the patent directives issued by the EU, currently it is thought of as referring exclusively to a natural person.[198]

In light of the above, it is clear that the present regulatory regime in the EU does not cater for the registration of a patent in respect of an invention created autonomously by AI. As AI continues to evolve, identifying the "inventor" will increase in difficulty exponentially and will potentially necessitate some form of separate legal personality regime to categorise what was traditionally thought of as only being attributable to humans.[199]

(iii) Ownership

In their current form, EU copyright and patent laws cannot be interpreted to vest ownership for work or inventions in AI itself.[200] This may change in the near future as the European Commission considers the viability of a separate legal status for AI machines such as robots.[201] If this is found to be a competent solution, this would precipitate a substantial overhaul of the current regulatory regime.

[195] Of 1973.
[196] E Fraser 'Computers as inventors – legal and policy implications of artificial intelligence on patent law' (2016) 13 *Scripted* 13, 324.
[197] Ibid.
[198] Ibid, 329.
[199] Ibid.
[200] Note 194 above, 28.
[201] Note 157 above, 18.

XVI. FINDINGS

At a cursory glance, the current regulatory regime pertaining to AI seems to be equally underdeveloped in all three jurisdictions. Whereas specific regulations (such as product liability legislation) can be manipulated to fit the required mould, this comparison has shown that legislation worldwide is woefully ill-equipped to deal with the regulatory issues that are lurking over the horizon.

With the above in mind, the lessons that may be extracted from the highlighted jurisdictions are threefold. The first lesson concerns national government's involvement in the future regulation of AI. In both the US and the EU, the relevant governing bodies have adopted an active approach to the AI revolution.[202] Committees have been formed and reports have been written setting out the framework for future regulation.[203]

In the US, the White House has approached the issue from all angles. It has recommended a "light touch" when developing regulation for AI and has encouraged experimentation to flush out issues in a safe testing environment.[204] The EU, on the other hand, has focussed its efforts on the regulation of autonomous vehicles, drones, and medical-care robots.[205] In addition, the EU has considered the impact that this form of AI will have on the economy at length, particularly in the context of the workforce.[206]

The second lesson to be learned is the importance of research and development. Both the US and the EU invest heavily in these two areas.[207] This form of investment is crucial for the development of the South African legislature and to educate legal practitioners and the judiciary to enable them to deal with the unique legal issues that AI poses.

The final lesson to be learned is the importance of early adoption. Both the US and the EU incentivise the private sector to innovate in the AI field through state-funded tax deductions and policy benefits.[208] As a result, they have access to cheaper and up to date technology, they use this technology to improve the lives of their citizens and they learn to deal with the novel issues that new technology brings before other jurisdictions.

[202] Note 100 above, 1.
[203] Ibid, 2.
[204] Note 100 above, 17.
[205] Note 157 above, 18.
[206] Note 157 above, 8-9.
[207] Note 100 above, 19.
[208] Note 100 above, 5.

The perfect example of this is the realm of automated cars. Both international jurisdictions have facilitated the growth of this area and are consequently light years ahead of South Africa in this field, both from a technological perspective and a legislative perspective.

In the US, certain states such as California, Florida, Michigan, and Nevada have implemented legislation allowing for the testing of autonomous vehicles on public roads provided that an experienced driver is situate behind the wheel at all times.[209] The District of Columbia has also implemented such legislation but has not limited the use of autonomous cars to testing.[210]

Additionally, in the EU, various member countries have allowed testing on their roads and interestingly, this has facilitated the legal operation and testing of driverless buses under very strict conditions in Switzerland and Greece.[211]

Whilst the approaches differ, the nett result is that the efforts put in by both the US and the EU will more than likely pay off in the long term. The South African government would do well to learn from these initiatives and to allocate sufficient resources to emulate them.

XVII. CONCLUSION AND THE PROPOSED WAY FORWARD FOR SA

Undeniably, the law will always be two steps behind AI. The ever-changing nature of this technological landscape would require endless resources to regulate expediently. With this in mind, there is no doubt that our current regulatory regime in South Africa does not adequately cater for the novel legal issues that AI raises.

Nevertheless, a balance must be struck between over-regulation, which may stunt and hamper the growth of the AI industry in South Africa, and under-regulation, which could lead to unmanageable societal risks such as cyber terrorism.[212]

As a means of facilitating this mammoth task, a substantial amount of research will have to be conducted and the existing laws in place will have to be examined by experts in the field with the aim of drawing up an action plan to assist the South African government in dealing with the uncertainty of AI.

At the very least, this action plan should contemplate a manner of tackling the regulation that will be required in respect of the following legal issues extracted from the comparison conducted in this report:

---

[209] Note 8 above, 349.
[210] Ibid.
[211] Note 151 above, 165 & Note 155 above, 305.
[212] Note 13 above, 39.

- separate legal status for AI;
- ownership of IP created independently by AI;
- criminal liability of autonomous AI;
- appropriate criminal punishment for AI; and
- the inevitable assimilation of autonomous cars into everyday South African life.

Moreover, this action plan should make provision for the formation of some form of regulatory body to oversee the development and implementation of AI legislation as well as the allocation of resources to educate legal professionals, government officials and the judiciary, thereby fostering understanding and creating expertise in this field.

BIBLIOGRAPHY

Articles

1. B Goodman & S Flaxman 'European Union regulations on algorithmic decision-making and a "right to explanation"' (2016) 8 *AI Magazine.*
2. E Fraser 'Computers as inventors – legal and policy implications of artificial intelligence on patent law' (2016) 13 *Scripted*.
3. E Herlin-Karnell 'What Principles Drive (or Should Drive) European Criminal Law?' (2010) 11 *German Law Journal.*
4. F A DeCosta & A G Carrano 'Intellectual Property Protection for Artificial Intelligence' (2017) *Westlaw Journal of Intellectual Property.*
5. G Hallevy ′"I, Robot – I, Criminal" – When Science Fiction Becomes Reality: Legal Liability of AI Robots committing Criminal Offences' (2010) 22 *Syracuse Science & Technology Law* Reporter.
6. J A Estrella Faria 'e-Commerce and international legal harmonization: Time to go beyond functional equivalence' (2004) SA Merc LJ.
7. J D Caytas 'European Perspectives on an Emergent Law of Robotics' (2017) *Columbia Journal of European Law.*
8. J H Blomsma '*Mens Rea* and defences in European criminal law' (2012) 54 *School of Human Rights Research Series.*
9. P M Schwartz 'The EU-US Privacy Collision: A turn to institutions and procedures' (2013) 126 *Harvard Law Review*.
10. W Erlank & L Ramokanate 'Allocating the risk of software failures in automated message systems (autonomous electronic agents)' (2016) *SA Merc LJ.*

Books

1. A Bensoussan & J Bensoussan 'France Chapter' in A Bensoussan et al. (1st Ed) *Comparative Handbook: Robotic Technologies* Law (2016).
2. G Ballas & T J Konstantakopoulos 'Greece Chapter' in A Bensoussan et al. (1st Ed) *Comparative Handbook: Robotic Technologies* Law (2016).
3. J Burchell *Principles of Criminal Law* 3 ed (2005).
4. J Giles & A Emma-Iwuoha 'South Africa Chapter' in A Bensoussan et al. (1st Ed) *Comparative Handbook: Robotic Technologies* Law (2016).

5. N Porto & D Preiskel 'United Kingdom Chapter' in A Bensoussan et al. (1st Ed) *Comparative Handbook: Robotic Technologies* Law (2016).
6. R Gilbert 'United States Chapter' in A Bensoussan et al. (1st Ed) *Comparative Handbook: Robotic Technologies* Law (2016).
7. R Kouatly et al. 'Lebanon Chapter' in A Bensoussan et al. (1st Ed) *Comparative Handbook: Robotic Technologies* Law (2016).
8. S Fanti 'Switzerland Chapter' in A Bensoussan et al. (1st Ed) *Comparative Handbook: Robotic Technologies* Law (2016).
9. WIPO Intellectual Property Handbook: Policy, Law, and Use (2004).

Case Law

1. *Brouse v United States* United States District Court, N.D. Ohio, E.D. 83 F. Supp. 373 (N.D. Ohio 1949).
2. *Diamond v Chakrabarty* 447 U.S. 303 (1980).
3. *Financial Mail (Pty) Ltd and Others v Sage Holdings Ltd and another* 1993 (2) SA 451 (A).
4. *Haupt t/a Softcopy v Brewers Marketing Intelligence (Pty) Ltd and Others* 2006 (4) SA 458 (SCA).
5. *Infopaq v Danske Dagblades Forening* [19 July 2009] ECR I-6569.
6. *Naruto v Slater* No. 15-cv-4324, 2016 WL 362231 (N.D. Cal. Jan. 28, 2016).
7. *Regal v African Superslate (Pty) Ltd* 1963 1 All SA 203 (A).
8. *Saphena Computing Ltd v Allied Collection Agencies Ltd* [1995] FSR 616.

Internet Articles

1. A Christie 'Smart Contract 2.0: The need for "Smart Lawyers" *Polity* (2017), <http://www.polity.org.za/article/smart-contract-20-the-need-for-smart-lawyers-2017-09-26>, last accessed on 21 January 2018.
2. C Cath et al. 'Artificial Intelligence and the "Good Society": the US, EU, and UK approach' (2017) *Sci Eng Ethics,* 4, <https://doi.org/10.1007/s11948-017-9901-7>, last accessed on 21 January 2018.
3. European Commission 'What does the General Data Protection Regulation (GDPR) Govern,' <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en>, last accessed on 21 January 2018.

4. Executive Office of the President National Science and Technology Council Committee on Technology. '*Preparing for the future of artificial intelligence'* (2016) Washington, DC, USA, <https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf>, last accessed on 21 January 2018.
5. E Zirnstein 'Harmonization and Unification of Intellectual Property Laws in the EU' (2005) *Slovenia,* < http://www.fm-kp.si/zalozba/ISBN/961-6486-71-3/293-306.pdf>, last accessed on 21 January 2018.
6. G Katznelson 'AI Citizen Sophia and Legal Status' *Harvard Law Blog* (9 November 2017), <http://blogs.harvard.edu/billofhealth/2017/11/09/ai-citizen-sophia-and-legal-status/>, last accessed on 21 January 2018.
7. H M Bohler 'EU copyright protection of works created by artificial intelligence systems' (2017) *University of Bergen,* <http://bora.uib.no/bitstream/handle/1956/16479/JUS399_V17_183.pdf?sequence=1&isAllowed=y>, last accessed on 21 January 2018.
8. J Giles 'Product Liability for Damage caused by Goods' *Michalsons,* <https://www.michalsons.com/blog/product-liability-for-damage-caused-by-goods/4584>.
9. J Giles 'Protection of Personal Information Act Summary – POPIA' *Michalsons,* <https://www.michalsons.com/focus-areas/privacy-and-data-protection/protection-of-personal-information-act-popia>, last accessed on 21 January 2018.
10. J Jacobs 'Artificial Intelligence, Explained' Global X (17 July 2017), < https://www.globalxfunds.com/artificial-intelligence-explained/>, last accessed on 21 January 2018.

    J P De Almeida Lenardon 'The Regulation of Artificial Intelligence' (2017) Tilburg Institute for Law, Technology, and Society *Tilburg University,* < http://arno.uvt.nl/show.cgi?fid=142832>, last accessed on 21 January 2018.
11. M A Weiss & K Archick 'U.S.-EU Data Privacy: From Safe Harbour to Privacy Shield' (2016) 7-5700 *Congressional Research Service Report,* <https://fas.org/sgp/crs/misc/R44257.pdf>, last accessed on 21 January 2018.
12. P Stone et al. 'Artificial Intelligence and life in 2030' (2016) One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel *Stanford University,* http://ai100.stanford.edu/2016-report, last accessed on 21 January 2018.

13. S Kis 'Contracts and Electronic Agents' (2004) *LLM Theses and Essays*, <http://digitalcommons.law.uga.edu/stu_llm/25>, last accessed on 21 January 2018.
14. S M Kierkegaard 'E-contract formation: U.S. and EU perspectives' (2007) 3 L. Com & Tech., <http://www.lctjournal.washington.edu/Vol3/a012Kierkegaard.html>, last accessed on 21 January 2018.
15. S N Kwanje 'Distinguishing between intention and negligence in South African Criminal Law' (2016) *North-West University*, <https://repository.nwu.ac.za/bitstream/handle/10394/24910/Kwanje_SN.pdf?sequence=1&isAllowed=y.>, last accessed on 21 January 2018.
16. 'Technology 2018', <http://www.aurametrix.com/blog>, last accessed on 21 January 2018.

Legislation

1. Berne Convention for the Protection of Literary and Artistic Works, as amended on 28 September 1979.
2. California Online Privacy Protection Act, 2003.
3. Civil Aviation Regulations, 2015.
4. Consumer Protection Act, No. 68 of 2008.
5. Convention on the grant of European Patents, 1973.
6. Copyright Act, No. 98 of 1978.
7. Database Directive 96/9/EC.
8. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000, O.J.L 178/1, 17.7.2000.
9. Drone Aircraft Privacy and Transparency Act, 2017 H.R. 1526.
10. Electronic Communications and Transactions Act, No. 25 of 2002.
11. Electronic Signatures in Global and National Commerce Act, 2000.
12. EU Product Liability Directive 85/374/EEC of 25 July 1985.
13. FAA Modernization and Reform Act, 2012 H.R. 658.
14. General Data Protection Regulation 2016/679 [2016] OJ L119/1.
15. Government Gazette No 34181, 1 April 2011.
16. Medicines and Related Substances Act, No. 101 of 1965.
17. Medicines and Related Substances Amendment Act, No. 14 of 2015.
18. Patents Act, No. 57 of 1978.
19. Privacy Act, 1974 5 U.S.C.

20. Protection of Personal Information Act, No. 4 of 2013.
21. Software Directive 91/250/EC.
22. Term Directive 2006/116/EC.
23. The Civil Code of California, 1872, as amended.
24. Treaty on European Union, 13 December 2007, 2008/C 115/01.
25. U.S. Patent Act, 35 U.S.C.
26. Uniform Electronic Transactions Act, 1999.

Miscellaneous

1. Alliance of Automobile Manufacturers, Inc. 'Consumer Privacy Protection Principles – Privacy Principles for Vehicle Technologies and Services' (12 November 2014), < https://autoalliance.org/connectedcars/automotive-privacy-2/principles/>, last accessed on 21 January 2018.
2. The Compendium of U.S. Copyright Office Practices (29 September 2017), <https://www.copyright.gov/comp3/docs/compendium.pdf>, last accessed on 21 January 2018.
3. M Delvaux 'European Parliament Report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2013(INL))' (27 January 2017) A8-0005/2017.
4. R Calo 'Robots in American Law' (2016) University of Washington School of Law Research Paper No. 2016-04.